A HISTORY OF U.S. COMMUNICATIONS SECURITY (U)
(The David G. Boak Lectures)

HANDLING INSTRUCTIONS

1. This publication consists of covers and numbered pages 1 to 101 inclusive. Verify presence of each page upon receipt.

2. Formal authorization for access to SECRET material is required for personnel to have access to this publication.

3. This publication will not be released outside government channels without approval of the Director, National Security Agency.

4. Extracts from this publication may be made for classroom or individual instruction purposes only. Such extracts will be classified SECRET NOFORN and accounted for locally until destroyed.

5. This publication will not be carried in aircraft for use therein.

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

Revised July 1973

SECRET

ORIGINAL 1
Reverse (Page 2) Blank

INTRODUCTION

This publication consists of a series of lectures prepared and given to interns and other employees by Mr. David G. Boak in 1966. Mr. Boak is uniquely qualified to discuss the history of U.S. COMSEC because he has participated significantly in most aspects of its modern development over the past twenty years.

The purpose of these lectures was to present in an informal yet informative manner the fundamental concepts of Communications Security and to provide an insight into the strenghts and weaknesses of selected manual systems, electro-mechanical and electronic crypto-equipments.

TABLE OF CONTENTS

FIRST LECTURE: The Need for Communications Security

I will spend most of this first period belaboring some seemingly obvious points on the need for communications security; why we're in this business, and what our objectives really are. It *seems* obvious that we need to protect our communications because they consistently reveal our strengths, weaknesses, disposition, plans, and intentions and if the opposition intercepts them he can exploit that information by attacking our weak points, avoiding our strengths, countering our plans, and frustrating our intentions. . . something he can only do if he has advance knowledge of our situation. But there's more to it than that.

First, you'll note I said the opposition can do these things *if* he can intercept our communications. Let me first give you some facts about that supposition. You've all seen the security caveats asserting that "the enemy is listening", "the walls have ears", and the like. One of my irreverent friends, knowing where I work, insists on referring to me as "an electronic spy", and popular paperback literature is full of lurid stories about code-breakers and thieves in the night careening to Budapest on the Orient Express with stolen ciphers tattooed somewhere unmentionable. What is the actual situation? We believe that the Soviet Signal Intelligence effort is greater in sheer manpower than the combined effort of the United States and the United Kingdom; a far larger portion of their national income is invested in signals collection than we invest in ours; their collection facilities include large land based sites, mobile platforms (air and sea), and satellite surveillance; and that they have an extensive covert collection operation. All in all, a truly formidable opponent. So the first "if" underlying our argument for the need for COMSEC (Communications Security) is more than a postulate—a deliberate, large, competent force has been identified whose mission is the exploitation of U.S. communications through their interception and analysis.

It is important to understand at the outset why the Soviet Union (as well as all other major countries) is willing to make an investment of this kind. Because, of course, they find it worthwhile. Sometimes, in the security business, you feel like a jackass having run around clutching defense secrets to your bosom only to find a detailed expose in *Missiles and Rockets* or the *Washington Post* or find it to be the subject of open conversations at a cocktail party or a coffee bar. There are, in fact, so many things that we cannot hide in an open society—at least in peace time—that you will sometimes encouter quite serious and thoughtful skepticism on the value or practicability of trying to hide anything . . . particularly if the techniques you apply to hide information—like cryptography —entail money, loss of time, and constraints on action.

What then, is unique about communications intelligence? What does it provide that our mountains of literature and news do not similarly reveal? How can it match the output of a bevy of professional spies or in-place defectors buying or stealing actual documents, blueprints, plans? ("In-place defector"—a guy with a *bona fide* job in some place like the Department of Defense, the Department of State, this Agency, or in the contractual world who feeds intelligence to a foreign power.) It turns out that there *is* something special about communications intelligence, and it provides the justification for our own large expenditures as well as those of other countries: in a nutshell, its special value lies in the fact that this kind of intelligence is generally accurate, reliable, *authentic*, continuous, and most important of all, *timely*. The more deeply you become familiar with classified governmental operations, the more aware you will become of the superficiality and inaccuracy that is liable to characterize speculative journalism. After all, if we've done our job, we have reduced them to speculation—to the seizing of and elaboration on rumors, and to drawing conclusions based on very few hard facts. This is by no means intended as an indictment of the fourth estate—it is merely illustrative of why Soviet intelligence would rather have the contents of a message signed by a government official on a given subject or activity than a controlled news release or journalistic guess on the same subject. Similarly, the outputs of agents are liable to be fragmentary, sporadic, and *slow*; and there are risks entailed in the transmission of intelligence so acquired. [Conventional SIGINT (Signals Intelligence) activity, of course, entails no risk whatever.]

Let me track back again: I have said that there is a large and profitable intercept activity directed against us. This does not mean, however, that the Soviets or anybody else can intercept *all* our communications ... that is, all of them at once; nor does it necessarily follow that all of them are *worth* intercepting. (The Army has a teletypewriter link to Arlington Cemetery through which they coordinate funeral arrangements and the like. Clearly a very low priority in our master plans for securing communications.) It does mean that this hostile SIGINT activity has to be selective, pick the communications entities carrying intelligence of most value or—and it's not necessarily the same thing—pick the targets most swiftly exploitable. Conversely, we in the COMSEC business are faced with the problem not simply of securing communications, but with the much more difficult problem of deciding which communications to secure, in what time frame, and with what degree of security. Our COMSEC resources are far from infinite; not only are there constraints on the money, people, and equipment we can apply but also—as you will see later on—there are some important limitations on our technology. We don't have that *secure* two-way wrist radio, for example.

In talking of our objectives, we can postulate an *ideal*—total security for all official U.S. Government communications; but given the limitations I have mentioned, our more realistic objectives are to develop and apply our COMSEC resources in such a way as to assure that we provide for our customers a *net advantage* vis-a-vis their opposite numbers. This means that we have to devise systems for particular applications that the opposition will find not necessarily *unbreakable* but too costly to attack because the attack will consume too much of his resources and *too much time*. Here, we have enormous variation—most of our big, modern electronic cryptosystems are designed to resist a full scale "maximum effort" analysis for many, many years; we are willing to invest a big expensive hunk of complicated hardware to assure such resistance when the underlying communications are of high intelligence value. At the other end of the spectrum we may be willing to supply a mere slip of paper designed only to provide security to a tactical communication for a few minutes or hours because the communication has no value beyond that time ... an artillery spotter ames a target; once the shell lands, hopefully on the coordinates specified, he couldn't care less about the resistance to cryptanalysis of the coded transmission he used to call for that strike.

Now, if the opposition brought to bear the full weight of their analytic resources they may be able to solve that code, predict that target, and warn the troops in question. But can they afford it? Collectively, the National Security Agency attempts to provide the commander with intelligence about the opposition (through SIGINT) while protecting his own communications against comparable exploitation—and thus provide the net advantage I spoke of. I'll state our practical objectives in COMSEC once more: not absolute security for all communications because this is too expensive and in some instances, may result in a net disadvantage; but sufficient security for each type of communications to make its exploitation uneconomical to the opposition and to make the recovery of intelligence cost more than its worth to him. Don't forget for a moment that some TOP SECRET messages may have close to infinite worth, though; and for these, we provide systems with resistance that you can talk of in terms of centuries of time and galaxies of energy to effect solution.

The reason I have spent this time on these general notions is the hope of providing you a perspective on the nature of the business we're in and some insights on why we make the kinds of choices we do among the many systems and techniques I'll be talking to you about during the rest of the week. I happened to start out in this business as a cryptanalyst and a designer of specialized manual systems not long after World War II. It seemed to me in those days that the job was a simplistic one—purely a matter of examining existing or proposed systems and, if you found anything wrong, fix it or throw the blighter out—period. In this enlightened spirit, I devised many a gloriously impractical system and was confused and dismayed when these magnificent products were sometimes rejected in favor of some clearly inferior—that is, *less secure* system merely because the alternative was simpler, or faster, or cheaper; or merely because it would *work*.

Those of you who are cryptanalysts will find yourselves in an environment that is necessarily cautious, conservative, and with security *per se* a truly paramount consideration. This, I assert, is *healthy* because you, a mere handful, are tasked with outthinking an opposing analytic force of rhaps 100 times your number who are just as dedicated to finding flaws in these systems as you

must be to assuring none slipped by. But do not lose sight of the real world where your ultimate product must be used, and beware of security features so intricate, elaborate, complex, difficult, and expensive that our customers throw up their hands and keep on communicating in the clear— you have to judge not only the abstract probabilities of success of a given attack, but the likelihood that the opposition will be willing to commit his finite resources to it.

I hope you non-cryptanalysts smiling in our midst will recognize that we're playing with a two-edged sword—you are or ought to be in an environment where there is an enthusiasm for introducing to the field as many cryptosystems as possible at the least cost and with the fewest security constraints inhibiting their universal application. But don't kid yourselves: against the allegation that the COMSEC people of the National Security Agency—we're the villains—are quote pricing security out of the market unquote—is the fact that there is this monolithic opposing force that we can best delight by introducing systems which are not quite or not nearly as good as we think they are.

From this, we can conclude that, to carry out our job we have to do two things: first we have to provide systems which are cryptographically sound; and second, we have to insure that these systems can and will be used for the purpose intended.

If we fail in the first instance, we will have failed those customers who rely on our security judgments and put them in a disadvantageous position with respect to their opposition. But if we fail to get the systems used—no matter *how* secure they are—we are protecting nothing but our professional reputation.

Now that the general remarks about why we're in this business and what our objectives are are out of the way, we can turn to the meat of this course—my purpose, as much as anything, is to expose you to some concepts and teach you a new language, the vocabulary of the peculiar business you're in. To this end I will try to fix in your minds a number of rather basic notions or approaches that are applied in cryptography as well as a number of specific techniques as they have evolved over the past two decades.

There's a fair amount of literature—like the Friedman lectures—which is worth your time and which will trace the art of cryptography or ciphering back to Caesar or therabouts. I'll skip the first couple of millennia and such schemes as shaving a slave's head, writing a message on his shining pate, letting the hair grow back and dispatching him to Thermopylae or where have you. I'll also skip quite modern techniques of *secret writing*—secret inks, microphotography, and open letters with hidden meanings (called "innocent text" systems)—merely because their use is quantitatively negligible in the U.S. COMSEC scheme of things, and this Agency has practically nothing to do with them. What we will be addressing are the basic techniques and systems widely used in the protection of U.S. communications and which we are charged to evaluate, produce, or support.

All of our systems have one obvious objective: to provide a means for converting intelligible information into something unintelligible to an unauthorized recipient. We have discovered very few *basic* ways to do this efficiently. Some of the best ways of doing it have a fatal flaw; that is, that while it may be impossible for the hostile cryptanalyst to recover the underlying message because of the processing given it, neither can the intended recipient recover it because the process used could not be duplicated! On occasion there has been considerable wry amusement and chagrin on the part of some real professionals who have invented sophisticated encryption schemes only to find they were irreversible—with the result that not only the cryptanalyst was frustrated in recovering the plain text, so was the addressee. The inventor of a cryptosystem must not only find a means for rendering information unintelligible, he must use a process which is logical and reproducible at the receiving end. All of you know already that we use things called "keys" which absolutely determine the specific encryption process. It follows from what I have just said that we *always* produce at least two of them, one for the sender, one for the recipient. Through its application, and only through its application, the recipient is able to reverse, unscramble, or otherwise undo the encryption process.

The techniques that we have found useful so far amount to only two: first *substitution* of something meaningless for our meaningful text (our plain language); and second; *transposition*—keeping our original meaningful text, but jumbling the *positions* of our words or letters or digits so they no

longer make sense. This latter technique is so fraught with security difficulties—it's nothing but fancy anagramming—that for all practical purposes you can toss it out of your lexicon of modern U.S. cryptography. To get well ahead of our chronology of U.S. systems, the last transposition system we sponsored was called ALLEGRO and it collapsed utterly as soon as the analysts had a chance to attack a reasonable batch of operational traffic committed to it.

We are left with one very large family of systems in which the basic technique involves the substitution of one value for another. These range from systems whose security stems from a few letters, words, or digits memorized in somebody's head, through a variety of printed materials that permit encryption by use of paper and pencil, to the fancy electronic computer-like gadgets about which you have by now probably heard most. The first category of these systems we're going to talk about is *manual* systems and the first of these is *codes*. Professional cryptographers have been talking about codes, using them, attacking them, and solving them for many years. The traditional definition of them is: Code: "A substitution cryptosystem in which the plaintext elements are primarily words, phrases, or sentences, and the code equivalents (called "code groups") typically consist of letters or digits (or both) in otherwise meaningless combinations of identical length."—JUNE 71— *Basic Cryptologic Glossary.*

This definition provides a convenient way for differentiating a "code" from any other substitution system—all the other systems, which we call "ciphers", have a *fixed* relationship between the cipher value and its underlying meaning—each plaintext letter is always represented by one or two or some other specific number of cipher characters. Incidentally, we use "character" as a generic term to cover numbers or letters or digits or combinations of them. Let's look at a couple of codes:

1. The simplest kind, called a "one-part code", simply lists the plaintext meanings alphabetically (so that you can find them quickly) and some corresponding code groups (usually alphabetized also):

```
BRIGADE. . . . . . . . . . . . . . . . . . . . . . . . .     ABT
COORDINATE(S) . . . . . . . . . . . . . . . . . . . . .     AXQ
DIRECT ARTILLERY FIRE AT____ . . . . . . . . . . . . .     CDL
ENGAGE ENEMY AT . . . . . . . . . . . . . . . . . . . .     GGP
. . . . . . .           . . . . . . . . . . . . . . . . .     HLD
. . . . . . .           . . . . . . . . . . . . . . . . .     JMB
```

There will usually be some numbers and perhaps an alphabet in such a code so that you can specify time and map coordinates and quantities and the like, and so that you can spell out words, especially place names, that could not be anticipated when the code was printed. Such a code has lots of appeal at very low echelons where only a very few stereotyped words, phrases, or directions are necessary to accomplish the mission. They are popular because they are simple, easy to use, and relatively fast. The security of such systems, however, is very, very low—after a handful of messages have been sent, the analyst can reconstruct the probable exact meanings of most of the code groups. We therefore take a dim view of them, and sanction their use only for very limited applications.

2. The kind of code we do use in very large quantities is more complicated, larger, and more secure. It is called a "two-part code": it is printed in two sections, one for encoding and the other for decoding:

```
          ENCODE                              DECODE
BRIGADE . . . . . . . . . . . . . CDL     ABT . . . ------
COORDINATE(S) . . . . . . . . . . AXQ     AXQ . . . COORDINATE(S)
DIRECT ARTILLERY FIRE AT____ JMB          CDL . . . BRIGADE
ENGAGE ENEMY AT . . . . . . . . . GGP     GGP . . . ENGAGE ENEMY AT
------           . . . . . . . . . HLD     HLD . . . ------
----           . . . . . . . . . . ABT     JMB . . . DIRECT ARTILLERY FIRE AT____
```

The main thing that has been done here is to break up the alphabetical relationship between the plaintext meanings and the sequence of code groups associated with them—that is, the code groups are assigned in a truly random fashion, not in an orderly one. This complicates the cryptanalyst's job; but he can still get into the system rather quickly when the code is used repeatedly. As a result, a number of tricks are used to refine these codes and limit their vulnerability. The first trick is to provide more than one code group to represent the more commonly used words and phrases in the code vocabulary—we call these extra groups "variants" and in the larger codes in use today it is not uncommon to have as many as a half-dozen of these variants assigned to each of the high frequency (i.e., commonly used) plaintext values. Here's an excerpt from a code actually in use today showing some variants:

EXCERPTS FROM KAC–13/TSEC VOCABULARY

XXX) RUNNING RABBITS (PULSED INTELLIGENCE)

XXX) SAGE
XXX)

XXX) SCOPE JAMMED ON SECTOR....FROM....
XXX)   DEGREES TO....DEGREES.
XXX)

XXX) SCOPE SATURATED (JAMMING COVERS
XXX)   ENTIRE SCOPE)
XXX)

XXX) SEARCH RADAR
XXX)
XXX)
XXX)

XXX) SECRET

You probably know that "monoalphabetic substitution systems" were simple systems in which the same plaintext value was always represented by the same cipher or code value—repeats in the plain text would show up as repeated patterns in the cipher text, so lovely words like "RECONNAIS-SANCE" convert to, say.

RECONN AISSA NCE   ... duck soup! it says here.
SDEGBB XMLLX BED

Well, with an ordinary code, that's exactly the problem. It is essentially a monoalphabetic system with a few variants thrown in, but with most repeated things in the transmitted code showing up as repeated items. This means, where we have to use codes (and later on, I'll show you why we have to in *huge* quantities), we have to do some things more fundamental than throwing in a few stumbling blocks like variants for the cryptanalyst. There are two techniques which are basic to our business and which we apply not only to codes but to almost all our keying materials. These are crucial to the secure management of our systems. These techniques are called *supersession* and *compartmentation*. They provide us a means for limiting the volume of traffic that will be encrypted in any given key or code; the effect of this limitation is to reduce the likelihood of successful cryptanalysis or of *physical loss* of that material; and further to reduce the scope of any loss that does occur.

SUPERSESSION is simply the replacement of a code or other keying material from time to time with new material. Most keys and codes are replaced each 24 hours; a few codes are replaced as frequently as each six hours; a few others remain effective for three days or more. We have these differing supersession rates because of the different ways in which the materials may be used. Holders of some systems may send only one message a day—everything else being equal, his system will have much greater resistance to cryptanalysis than that of a heavy volume user and his system will not

quire replacement as often. The regular replacement rate of material each six hours or 24 hours or three days or what have you is called the "normal supersession rate" of the material in question. "Emergency supersession" is the term used when material is replaced prematurely because it may have been physically lost.

Once again, the purpose of periodic supersession of keying material and codes is to limit the amount of traffic encrypted in any one system and thus to reduce the likelihood of successful crypta- nalysis or of physical loss; and to limit the effect of loss when it does occur. The resistance to crypta- nalysis is effected by reducing the amount of material the cryptanalyst has to work on and by reducing the *time* he has available to him to get at *current* traffic.

COMPARTMENTATION is another means for achieving control over the amount of classified information entrusted to a specific cryptosystem. Rather than being geared to time, as in the case of supersession, it is geared to communications entities, with only those units that have to inter- communicate holding copies of any particular key or code. These communications entities in turn tend to be grouped by geography, service, and particular operational mission or specialty. Thus, the Army artillery unit based in the Pacific area would not be issued the same code being used by a similar unit in Europe—the vocabularies and procedures might be identical, but each would have unique code values so that loss of a code in the Pacific area would have no effect on the security of messages being sent in the Seventh Army in Europe, and vice versa. Of course some systems, parti- cularly some machine systems, are designed specifically for intercommunication between two and only two holders—between point A and point B, and that's all. In such a case, the question of "com- partmentation" doesn't really arise—the system is inherently limited to a compartment or "net" of two. But this is rarely the case with ordinary codes; and some of them must have a truly worldwide distribution. So our use of compartmentation is much more flexible and less arbitrary than our use of supersession; occasionally we will set some absolute upper limit on the number of holders per- missible in a given system because cryptanalysis shows that when that number is exceeded, the .ne to break the system is worth the hostile effort; but in general, it is the minimum needs, for intercommunication that govern the size (or, as we call it, the copy count) of a particular key list or code.

Now I have said that compartmentation and supersession are techniques basic to our whole business across the spectrum of systems we use. Their effect is to split our security systems into literally thousands of separate, frequently changing, *independent* entities. This means, of course, that the notion of "breaking *the* U.S. code" is sheer nonsense—the only event that could approach such catastrophic proportions for U.S. COMSEC would be covert (that is, undiscovered) penetration of our key list and code production facilities or major storage facilities. To those of you who have had some exposure to S3 and its operations, it will be evident that this would be enormously diffi- cult to do because of access controls there and the sheer mass of undifferentiated and unassigned, and as yet unused, material involved. If there were a major overt loss—say somebody drove off with a whole truckload of our product—or to take an actual case that occurred in 1965—the crash of a courier aircraft carrying about a ton of cryptomaterial—our cost would be considerable money and confusion; but the security impact would be negligible—we simply do not use the missing material; we replace it—that is, supersede it before it is ever put into effect.

The reason I've injected these concepts of compartmentation and supersession into the middle of this discussion of codes, although they have little to do with the structure of codes themselves, is that, despite our variants, and tricks to limit traffic volume, and controls over operational proce- dures, *codes as a class remain by far the weakest systems we use;* and these techniques of splitting them into separate entities and throwing them out as often as possible are essential to obtaining even the limited short-term security for which most of them are intended.

Having said, in effect, that codes as a class are not much good, let me point out that there are specialized paper and pencil systems which more or less conform to the definition of "code" but which are highly secure. Before I do this, let me return to the definition of code we started from, and suggest an alternative definition which more nearly pin-points how they *really* differ from other .hniques of encryption. You remember we said the thing that makes a code unique is the fact that

the code values can represent underlying values of different lengths—to recognize this is important to the cryptanalyst and that is the feature that stands out for him. But there is something even more basic and unique to a code: that is the fact that each code group—that QXB or what-have-you—stands for something that has *intrinsic meaning*, i.e., each underlying element of plain text is cognitive; it is usually a word or a phrase or a whole sentence. In every other system of encryption, this is not so; the individual cipher value stands only for an arbitrary symbol, meaningless in itself—like some binary digit or a letter of the alphabet. So I find, when examining a code, that QXB means "FIRE A GUN," or "REGROUP AT THE CROSSROADS," or "QUARTERBACK SNEAK," or what-have-you. In a *cipher* system, QXB might mean "X" or "L" or "001" or something else meaningless in itself. I've touched on this partly because the new cryptologic glossary has defined a code in terms of the meaning—or meaningfulness—of the underlying textual elements. I wouldn't push the distinction too far—it gets hazy when you are *spelling* with a code; get around it by admitting that, during the spelling process, you are in fact retaining a one-to-one relationship between the size of the underlying values and those being substituted for them—you are, for the moment, "enciphering" in the code.

The "One-Time" Concept.—I have said that at the heart of a code's insecurity is the fact that it is essentially a monoalphabetic process where the same code group always stands for the same underlying plaintext value. The way to lick this, of course, *is to devise a system where each code value is used once and only once.* Repeats don't show up because there aren't any, and we have effectively robbed the cryptanalyst of his "entering wedge" into the cryptosystem. Let's look at several such systems:

ARTILLERY:	ABD	BRIGADE:	MJX
	QVM		ZIY
	CXD		RDF
	EVL		QLW
	QSI		

. . . .

etc.

Well! This thing looks like nothing more than one of those ordinary codes we talked about, but with a set of variants assigned to each item of the vocabulary. Right. But suppose I make a rule that each time you use a variant, you check it off or cross it out, and must not use it again? By this simple expedient, I have given you a *one-time system*—a system which is for all practical purposes immune to cryptanalysis, perfectly secure? Sounds nice, and you might wonder why we have not adopted it for universal use. Well, let's look at some of the constraints inherent in this simple procedure:

Right now, if I have a very large vocabulary in a standard two-part code, it may run up to 32 pages or more. (The largest is 64 pages). If I have to insert say a half-dozen code values for every plaintext entry, my code book gets to be about 200 pages long, rather awkward to jam in the most voluminous of fatigue pockets, and a most difficult thing to thumb through—jumping back and forth, mind you—as you do your encoding or decoding process. So, limitation number one: we have to confine the technique to codes of quite small vocabularies.

Suppose my "compartment" (my net size) is 20 holders for this code. How does any given user know which values other holders in the net have used? He doesn't. He doesn't unless everybody listens to everybody else all the time, and that doesn't often happen. And this is really the killing limitation on most one-time systems of this kind. You wind up saying only *one* holder can send messages in the code, and all other copies are labelled "RECEIVE ONLY". We call this method of communications "Broadcast" and it has rather narrow applications. Alternatively, we can provide each of our 20 holders with a SEND code and 19 RECEIVE codes—but try to visualize some guy in an operational environment scrambling through 19 books to find the right one for a given incoming message; and look at the logistics to support such a system: it turns out that the number of books you need is the *square* of the number of holders you want to serve in this way—400 books for a 20-

holder net—10,000 for 100 holders! So limitation number two: the size of a net that you can practicably operate in this way is very small: preferably just two stations.

Let's turn now to another kind of one-time code; one that we call a "pro forma" system. "Pro forma" means that the basic framework, form or format of every message text is identical or nearly so; the same kind of information, message after message, is to be presented in the same order, and only specific values, *like numbers*, change with each message.

LINE NR.	LINE TITLE	ENCRYPTION/DECRYPTION TABLE

1 — TABLE INDICATOR: (PQA)

2 (W) — NUCLEAR ACTION FORM/SEQ:
```
81 0123456789  8123456789  8123456789  8123456789  8123456789  8123456789
YZ QRSTUVWXYZ  NOPQRSTUVW  WXYZABCDEF  TUVWXYZABCD  KLMNOPQRST  CDEFGHIJKL
```

	ARMY		CORPS		DIV	TASK			CAV	NULLS
ARMY	ARTY	CORPS	ARTY	DIV	ARTY	FORCE	BDE	BN	SQDN	SYU
Y	Z	A	(B)	C	D	E	F	G	H	

3 (K) — TYPE ACTION:
| NOTIFICATION | (REG) | ALERT | ORDER | APPR | CANCEL | CHANGE | RECCE | EMPLACE |
| F | G | H | I | J | K | L | M | N |

| FIRE/LAUNCH | NEG | AFFIRMATIVE | HOLD | SPARE 1 | SPARE 2 | (NULL) |
| O | P | Q | R | S | T | M |

4 (A) — NUC STRIKE DSG/TGT NR:
```
0123456789  8123456789  8123456789  8123456789  8123456789  (NULLS)
CDEFGHIJKL  HIJKLMNOPQ  RSTUVWXYZA  JKLMNOPQRS  IJKLMNOPQR  XHA
```

5 (P) — DESIRED GROUND ZERO:
```
ABCDEFGHIJKLMNPQRSTUVWXYZ  ABCDEFGHIJKLMNPQRSTUV  8123456789  8123456789
PQRSTUVWXYZABCDEFGHIJKLM   LMNOPQRSTUVWXYZABCDE   NOPQRSTUVW  PQRSTUVWXY

8123456789  8123456789  8123456789  8123456789  8123456789  8123456789  (NULL)
STUVWXYZAB  LMNOPQRSTU  OPQRSTUVWX  KLMNOPQRST  XYZABCDEFG  YZABCDEFGH  P
```

6 (T) — TARGET DESCRIPTION RADIUS IN METERS:
```
ABCDEFGHIJKLMNOPQRSTUVWXYZ  ABCDEFGHIJKLMNOPQRSTUVWXYZ
NOPQRSTUVWXYZABCDEFGHIJKLM  EFGHIJKLMNOPQRSTUVWXYZABCD

8123456789  8123456789  8123456789  8123456789  (NULLS)
RSTUVWXYZA  NOPQRSTUVW  WXYZABCDEF  KLMNOPQRST  TU
```

7 (X) — TGT ELEV IN METERS:
```
0123456789  8123456789  8123456789  8123456789  (NULL)
OPQRSTUVWX  WXYZABCDEF  HIJOPQRSTUV  VWXYZABCDE  C
```

8 (L) — TYPE BURST/METERS:
| HIGH | (LOW) | SUR | SUBSUR | 8123456789 | 8123456789 | 8123456789 | 8123456789 | (NULLS STD) |
| O | P | Q | R | KLMNOPQRST | OBRSTUVWXYZ | YZABCDEFGH | XYZABCDEFG | |

9 (M) — TIME OVER TARGET:
```
0123  0123456789  812345  8123456789  81234 8123456789  (LOCAL)  GMT  (NULL)
QRST  VWXYZABCDE  ZAB    STUVWXYZAB   NOPQRS PQRSTUVWXY   L        M    C
```

10 (B) — DELIVERY MEANS:
| AIR | HJ | 8IN.H | NIKE-H | 155H | (SGT) | LJ | RESTN | LANCE | DAVY CROCKETT |
| B | C | D | E | F | G | H | I | J | K |

| PERSH | ADM | SPARE 1 | SPARE 2 | SPARE 3 | SPARE 4 | (NULL) |
| L | M | N | O | P | Q | J |

11 (R) — WEAPON (MK NR):
```
8123456789  8123456789  8123456789  (NULLS GV)
IJKLMNOPQR  TUVWXYZABC  IJKLMNOPQR
```

12 (N) — YIELD:
| (KT) | MT | 8123456789 | 8123456789 | 8123456789 | (DECIMAL POINT) |
| X | Y | GHIJKLMNOP | IJKLMNOPQR | GHIJKLMNO | W |

```
8123456789  8123456789  8123456789  (NULLS VTG)
FGHIJKLMNO  WXYZABCDEF  FGHIJKLMNO
```

13 (S) — LOCATION OF FIRING POINT:
```
ABCDEFGHIJKLMNPQRSTUVWXYZ  ABCDEFGHIJKLMNPQRSTUV  8123456789  8123456789
TZABCDEFGHIJKLMNOPQRSTUV   XYZABCDEFGHIJKLMNOPQ   VWXYZABCDE  QRSTUVWXYZ

8123456789  8123456789  8123456789  8123456789  8123456789  8123456789  (NULL)
PQRSTUVWXY  YZABCDEFGH  WXYZABCDE  FGHIJKLMNO  ZABCDEFGHI  PQRSTUVWXY  G
```

14 (E) — FRIENDLY FORCES SFTY CRIT/DEGREE RISK:
| (WARNED) | UNWARNED | OPEN WOODS | FOXHOLES | (SHELTERS) | TANKS | BLDGS | VEH |
| P | Q | V | W | X | Y | Z | A |

| EMERGENCY | (NEGLIGIBLE) | (NULLS RG) |
| A | B | |

15 (D) — AZ IN MILS/METERS DGZ TO FRIENDLY FORCES:
```
8123456  8123456789  8123456789  8123456789  8123456789  8123456789
NOPQRST  IJKLMNOPQR  MNOPQRSTUV  WXYZABCDEF  KLMNOPQRST  TUVWXYZABC

8123456789  8123456789  (NULLS FUP)
OPQRSTUVWX  CDEFGHIJKL
```

ORIGINAL 17

Now we're beginning to get something more manageable: We still have the constraint of needing small net size or, alternatively, a larger net but with only one or a few senders of information. But it's a dandy where the form of the messages themselves permit this terrible inflexibility. We use a few of them, but machines are the things we're moving towards to meet most of the requirements of this type.

The last one-time code system I want to talk about is one that we use a great deal for Direction Finding Operations. We call it COMUS—which reminds me that we will soon have to come to grips with *nomenclature*—perhaps in the next hour.

```
                1 2 3 4 5 6 7 8 9 0           ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
FREQUENCY       G J F H I D A E B C    CALL SIGN  UV64K80G2LEJ70G5NYTSAB1ZRXHWI9DPCMF3

                1 2 3 4 5 6 7 8 9 0           ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
                A B I J E G H C D F        FMIDTA5ZC4BYB86WDX2E97PRLHK3S1JGOVNU

                1 2 3 4 5 6 7 8 9 0           ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
                G F I H J A E D C B        9WL7DUZMTBPCHSEK48NIF1B23G6VXYQJODRA

                1 2 3 4 5 6 7 8 9 0           ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
                D I H C G F A E B J        KLOX5WZSV3ABF2CYRQH01I8DPGTUNJ9E76W4

                1 2 3 4 5 6 7 8 9 0           ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
                C E B F H I J A G D        64ENCU12G950ZDY7XTVRFS3QCML8HWBKAP1J
```

```
                A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9
TRACKING        M S G E D X C O G V U 9 A T H 2 I 0 B N K J 3 F Z Y R 5 P W 7 1 8 4 6 L
BRG RPT
A  SUKTP  LFXVBGRKNIH  LZDSITAEKXN  OHULXANKGEB   QCBU3HPFW-0  VJTFIQCRSMD  TAJQMSYECWZ  A
   0123N  0123456789N  0123456789N  0123456789N   1234567890G  10123456789  0123456789N
B  OCRKZ  FDQJSPMCIUL  DHSGONOERJE  SIZDBWLCAEV   MLWTPFCUYKX  JGNFUOYMRHP  ZARXVTENBYO  B

C  XNIQU  OPESVBJILKT  PJMCANFYUSC  MSIOEZCURDG   GCVAZTDKEXR  LWNAKFPHOVB  WRYZMQUDCAG  C
   0123N  0123456789N  0123456789N  0123456789N   1234567890G  10123456789  0123456789N
D  INMRZ  OYDSTUWRACQ  YUWIDZXGHPA  FYHOPTDMUIB   FCLMTSNOCRE  SNRACXQVZLE  KBGEFNZMPJV  D

E  PSLMV  FXHRTIYAOJC  JYTMHVEAQBO  KBSCJZHMEDN   LXGD2CPFRSI  UWOFOIXYVGT  WNPEKVGMUBG  E
   0123N  0123456789N  0123456789N  0123456789N   1234567890G  10123456789  0123456789N
F  YTGIU  LWXSZQNDAOH  XNCKEUQYIOH  FWKESRJIVYQ   VJMTRWBALDF  HTUAONLMBCZ  KFTCVIYBJEP  F

G  YNEBI  UCQKRGPIMJD  JVRIWTZLYHK  GKEJCFDTPYS   NQXBSUEDCA3  MILOC2URHNV  TFBZVEYHOWX  G
   0123N  0123456789N  0123456789N  0123456789N   1234567890G  10123456789  0123456789N
H  NRLVQ  YSKFGAWEOBP  FHCLYDGQEXB  AINYPWFGUTG   UPJTMIIKCRA  OLEXSMBCDZJ  TUVCJDQNIXM  H

I  MURXI  QHWDEGYRZBC  WIGFZUTXMHC  AKUBHYWREFI   AQLRY5PDS-V  QNPSZLDTXVQ  MAJIVPXNKST  I
```

In comparing this one-time system and the last one I showed you, I think you'll begin to see a number of characteristics emerge for these specialized codes: first off, they are relatively secure: I say relatively, because there is more to communications security than resistance to cryptanalysis—and while these systems meet that first test—cryptanalysis—admirably, from the *transmission security* point of view, they're pretty bad; but we'll be talking about that on another day. Secondly: they are inflexible, rigidly confined with respect to the variety of intelligence they can convey. Thirdly: they are built for *speed*; they are by far the fastest means of communicating securely without a machine. Finally, they are extremely specialized, narrow in their application, and limited in the size of communications network they can serve efficiently. Being specialized, by the way, and *tailored* to particular needs, they fly in the face of efforts to *standardize* our materials—a very necessary movement in a business where we have to make hundreds of codes, distribute them all er the world, replace most of them daily and, as a result, wind up with a total copy count numbering, at the moment, about 5 million each year.

The business of standardizing on the one hand, for the sake of economy, simplicity, and manageability and of uniquely tailoring systems for maximum efficiency in some particular application, is one of the many conflicting or contradictory themes in our business; just as maximum security may conflict with speed or something else.

SECOND LECTURE: Codes

So far we have been talking about general and specialized codes: they form the largest body of manual systems we have. There are several more types of manual systems, but before we turn to them, there are a few more associations I want you to form with codes. So far we've limited ourselves pretty much to how they work and have hinted at some of their security and operational shortcomings, and have only implicitly indicated where they are used or why they'd be preferable to something automatic like a machine.

By far the biggest use of codes we have is with *voice* communications, with field telephones over wire lines or with radio telephones. The foremost reason for our reliance on them in these applications is because we do not yet have, in quantity, the voice encryption equipment that will be needed to replace them. When we discuss voice encryption equipment—ciphony machines—you will see some of the real technical, operational, and cost considerations which have kept them relatively scarce. For the moment, it is sufficient to remember that their lack is the main reason for the extensive use of codes and for a worse security situation, the use of no cryptography at all—plain language. Even where a unit might be able to afford machine cryptography, codes are sometimes attractive for other reasons—they are generally cheap (a few cents a copy); highly compact and portable (many of them do find their way into pockets and map cases); simple—they require no maintenance, hardly any training, and no power; easily disposed of—just touch a match to them. You can carry them anywhere and use them on any communications system at your disposal.

You will find them most at the lowest echelons: the Army is by far their largest user; they have considerable use in aircraft that don't now have the room or compatible communications systems to work with cryptomachines.

Aside from the security shortcomings of codes, they have one other very serious disadvantage: that is, they are very *slow*, ordinarily permitting the encryption of only a few words a minute, while most machines will operate at least as fast as you can type. Finally, even codes with very large vocabularies are awkward and inflexible because not all the right words are there, with the result that messages may be clumsy and imprecise as well as slow.

****

The next kind of manual system I want to talk about is the *one-time pad*. One-time pads are pure and simple cipher systems (*not* codes); with a one for one replacement of each plaintext character by a cipher equivalent. They consist of page after page of random numbers or letters (which ● call one-time key). The oldest type still in substantial use is called DIANA. Here's a sample.

LFHKY	ZAHBB	JRNXK	BYHFU	KOZAT	
VRETH	JPCSU	RUSYO	JHXHH	BLOEL	
POOTP	JJLVJ	XFSHL	HPLGA	ZXVZY	
TSUIO	XBHKI	HBSHD	KPHPI	OZVOZ	
CYJBU	QBXKR	PHTVY	YTKGK	ATOPU	
NNCJK	FPNSV	BHZZN	QQZYN	CYSDG	
YIIUJ	TBRRZ	GHRDE	YOVRJ	HOCGY	
HALOK	NHIIN	CAIDV	RDTKH	ZDZHP	
OINDS	CHOFE	XBBVJ	CAYSO	IBBHU	
KJSZX	OZJIN	DBRCY	BNUVZ	LFBXT	
●TI	WWIFH	IHNSF	RUVVC	UITRN	
NGQNG	ZUBZB	EPVJX	NCZXY	FBTEX	
VEIOE	HDVTN	GSSHG	LRZWG	UKUQK	
POFRI	QCFAA	NLTKE	DXHDA	QAIHU	
HEIKG	LQTBP	HVBNX	RNUUK	ACPKA	
AYGFS	ZNFOU	SYHVX	IYIPO	RJCEK	
PBOPQ	JFBIO	NYLIX	GBTNC	QQXXH	
FSGNA	UOTLB	UHKAH	HARHG	TZVXN	
UGBOA	JXHFY	HTUHH	WCTXH	OFLSY	

	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A	Z Y X W V U T S R Q P O N M L K J I H G F E D C B A
B	Y X W V U T S R Q P O N M L K J I H G F E D C B A Z
C	X W V U T S R Q P O N M L K J I H G F E D C B A Z Y
D	W V U T S R Q P O N M L K J I H G F E D C B A Z Y X
E	V U T S R Q P O N M L K J I H G F E D C B A Z Y X W
F	U T S R Q P O N M L K J I H G F E D C B A Z Y X W V
G	T S R Q P O N M L K J I H G F E D C B A Z Y X W V U
H	S R Q P O N M L K J I H G F E D C B A Z Y X W V U T
I	R Q P O N M L K J I H G F E D C B A Z Y X W V U T S
J	Q P O N M L K J I H G F E D C B A Z Y X W V U T S R
K	P O N M L K J I H G F E D C B A Z Y X W V U T S R Q
L	O N M L K J I H G F E D C B A Z Y X W V U T S R Q P
M	N M L K J I H G F E D C B A Z Y X W V U T S R Q P O
N	M L K J I H G F E D C B A Z Y X W V U T S R Q P O N
O	L K J I H G F E D C B A Z Y X W V U T S R Q P O N M
P	K J I H G F E D C B A Z Y X W V U T S R Q P O N M L
Q	J I H G F E D C B A Z Y X W V U T S R Q P O N M L K
R	I H G F E D C B A Z Y X W V U T S R Q P O N M L K J
S	H G F E D C B A Z Y X W V U T S R Q P O N M L K J I
T	G F E D C B A Z Y X W V U T S R Q P O N M L K J I H
U	F E D C B A Z Y X W V U T S R Q P O N M L K J I H G
V	E D C B A Z Y X W V U T S R Q P O N M L K J I H G F
W	D C B A Z Y X W V U T S R Q P O N M L K J I H G F E
X	C B A Z Y X W V U T S R Q P O N M L K J I H G F E D
Y	B A Z Y X W V U T S R Q P O N M L K J I H G F E D C
Z	A Z Y X W V U T S R Q P O N M L K J I H G F E D C B

25X3, E.O.13526

Withheld from public release under
§6 of the National Security Act of 1959,
50 U.S.C. 3605 (P.L. 86-36)

So, where volume is very low, for example in a place where pads are held only as an emergency back-up to machine systems and used only when the machines fail, one pad could remain "effective" for years.

One-time pads have undergone a kind of evolution during the past decade or so. The main effort has been to find ways of obtaining more speed. The first major pad system after DIANA did provide a good deal more speed—it is called ORION, and it's three times as fast.

SECRET NOFORN

To understand how the ORION pad is used, it will be helpful to visualize the two illustrations shown above as being printed in exact alignment on reverse sides of the same sheet of paper. To encipher, one sheet of the pad with the straight alphabet side up is placed on a piece of carbon paper, carbon side up. With this arrangement, when a plaintext letter is circled on one side of the paper, a circle will appear on the other side of the paper as surrounding the cipher letter because of the carbon paper. Therefore, by recording the text of the message—one letter per line—on the plaintext alphabet, the enciphered text is available by merely turning over the page.

Here we are able to encipher as quickly as we can circle the letters of our plain text—and because we have reciprocity, the deciphering process is equally fast. But, as usually seems to happen to us with manual systems, we have achieved speed at a very considerable cost in bulk—we have lost the means to compress a great deal of key in a small space. With DIANA, we were able to encipher about 100 words with each page; with this system, only 10 words. All of a sudden we have had to print 26 letters of key for each one letter of plain text, and the result is that the user is stuck with a very large batch of material to store and account for if he has to process many messages. Still, where speed is of the essence, where no machine is available, and where messages are very short or infrequent, the system found a place. You'll note, though, that such a pad entails a very tricky production process. The alphabets on the front and back of each page must be in *exact* alignment—"registration" the printers call it. This slowed down the printing process so much, and was so costly, that we have stopped producing ORION pads, although a number of them are still in use in the field. What we came up with instead is a system equally fast, and easier to make called MEDEA.

```
    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
01  PONMLKJIHGFEDCBA9876543210ZYXWVUTSRQ      26  NMLKJIHGFEDCBA9876543210ZYXWVUTSRQPO

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
02  IHGFEDCBA9876543210ZYXWVUTSRQPONMLKJ      27  ZYXWVUTSRQPONMLKJIHGFEDCBA9876543210

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
03  LKJIHGFEDCBA9876543210ZYXWVUTSRQPONM      28  3210ZYXWVUTSRQPONMLKJIHGFEDCBA987654

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
04  JIHGFEDCBA9876543210ZYXWVUTSRQPONMLK      29  FEDCBA9876543210ZYXWVUTSRQPONMLKJIHG

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
05  BA9876543210ZYXWVUTSRQPONMLKJIHGFEDC      30  LKJIHGFEDCBA9876543210ZYXWVUTSRQPONM

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
06  EDCBA9876543210ZYXWVUTSRQPONMLKJIHGF      31  210ZYXWVUTSRQPONMLKJIHGFEDCBA9876543

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
07  543210ZYXWVUTSRQPONMLKJIHGFEDCBA9876      32  43210ZYXWVUTSRQPONMLKJIHGFEDCBA98765

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
08  WVUTSRQPONMLKJIHGFEDCBA9876543210ZYX      33  GFEDCBA9876543210ZYXWVUTSRQPONMLKJIH

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
09  RQPONMLKJIHGFEDCBA9876543210ZYXWVUTS      34  6543210ZYXWVUTSRQPONMLKJIHGFEDCBA987

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
10  GFEDCBA9876543210ZYXWVUTSRQPONMLKJIH      35  43210ZYXWVUTSRQPONMLKJIHGFEDCBA98765

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
11  QPONMLKJIHGFEDCBA9876543210ZYXWVUTSR      36  EDCBA9876543210ZYXWVUTSRQPONMLKJIHGF

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
12  HGFEDCBA9876543210ZYXWVUTSRQPONMLKJI      37  ZYXWVUTSRQPONMLKJIHGFEDCBA9876543210

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
13  JIHGFEDCBA9876543210ZYXWVUTSRQPONMLK      38  GFEDCBA9876543210ZYXWVUTSRQPONMLKJIH

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
14  YXWVUTSRQPONMLKJIHGFEDCBA9876543210Z      39  10ZYXWVUTSRQPONMLKJIHGFEDCBA98765432

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
15  0ZYXWVUTSRQPONMLKJIHGFEDCBA9876543210     40  CBA9876543210ZYXWVUTSRQPONMLKJIHGFED

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
16  UTSRQPONMLKJIHGFEDCBA9876543210ZYXWV      41  WVUTSRQPONMLKJIHGFEDCBA9876543210ZYX

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
17  6543210ZYXWVUTSRQPONMLKJIHGFEDCBA987      42  DCBA9876543210ZYXWVUTSRQPONMLKJIHGFE

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
18  10ZYXWVUTSRQPONMLKJIHGFEDCBA98765432      43  DCBA9876543210ZYXWVUTSRQPONMLKJIHGFE

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
19  TSRQPONMLKJIHGFEDCBA9876543210ZYXWVU      44  JIHGFEDCBA9876543210ZYXWVUTSRQPONMLK

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
20  210ZYXWVUTSRQPONMLKJIHGFEDCBA9876543      45  GFEDCBA9876543210ZYXWVUTSRQPONMLKJIH

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
21  76543210ZYXWVUTSRQPONMLKJIHGFEDCBA98      46  TSRQPONMLKJIHGFEDCBA9876543210ZYXWVU

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
22  A9876543210ZYXWVUTSRQPONMLKJIHGFEDCB      47  SRQPONMLKJIHGFEDCBA9876543210ZYXWVUT

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
23  RQPONMLKJIHGFEDCBA9876543210ZYXWVUTS      48  ONMLKJIHGFEDCBA9876543210ZYXWVUTSRQP

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
24  XWVUTSRQPONMLKJIHGFEDCBA9876543210ZY      49  GFEDCBA9876543210ZYXWVUTSRQPONMLKJIH

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789          ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
25  0ZYXWVUTSRQPONMLKJIHGFEDCBA9876543210     50  HGFEDCBA9876543210ZYXWVUTSRQPONMLKJI
```

This system looks a lot like that one I showed you for D/F work (COMUS). It, and variations of it, are fairly common these days. Because of its smaller bulk, though, DIANA, and its numerical equivalent (CALYPSO) are still the most used one-time pads.

Now, where are one-time pads used? Not in a single-seater aircraft, surely! And rarely in big cryptocenters where machines are available—sometimes, though, officials need complete privacy for especially sensitive messages; they don't want them read by the cryptographers or others in the communications center, and will use a pad for the most sensitive portions of their message. The communication center will then superencrypt it (encrypt it again) in a machine system. But this is not a very common practice. The main use of pads is in connection with intelligence, agent, or

ther special operations and as a back-up for machine systems. So our main users are people like CIA, the attachés, and Special Forces units; and by organizations such as the Department of State which operate many isolated cryptocenters in locations where machine communications are unreliable. Speaking of agents, here is the actual size of what we called the "MICKEY MOUSE" pad.

Specifications for pads like these can be pretty far out—we can meet the size and legibility requirements alright; we can make it burn without a trace; but darned if we can make it edible! As a matter of fact the paper tastes just fine, but the ink is poisonous.

During FY-72, 86,000 one-time pads were produced. Production is expected to decline to approximately 35,000 pads annually by the end of FY-74 primarily because of the production of all MINUTEMAN pads in the new format.

A final point about one-time pad systems. The mechanical or electronic wizards among you can probably visualize ways in which these encryption processes could be automated—built into a machine. And in fact, it has been done and there are a few such machines operative now. They are used mainly in the centralized headquarters of CIA and Special Forces units so that they can efficiently process the many separate one-time pad messages to and from individual pad holders in the field.

****

The next kind of manual systems I want to talk about are *authentication systems*. Authentication is the process of verifying that a given received communication is bona fide—it is the main defense we have against communications deception or "spoofing" by the opposition. In tactical situations the classic kind of deception usually involves the enemy sending a message to, say, an aircraft pilot and directing him to attack his own forces or luring him to an area where he will be subjected to hostile fire. Here's an excerpt from an actual document captured from the Viet Cong describing these techniques:

> "During an operation, we captured a GRC-9 radio, and succeeded in finding out the enemy operating procedures and schedule used between the enemy posts.
>
> "We have put it to use to monitor (the enemy network) and to mislead (the enemy station) forcing them to waste time in asking repeated questions while we safely withdrew.
>
> "Sometimes, we called enemy artillery to shell their troops or posts, inflicting heavy losses upon them. This caused confusion and suspicion, among the enemy units themselves, and restricted the use of their artillery to our advantage.
>
> "As the enemy code words are widely used, a careful study will enable us to find out these codes since they are composed of slangs and spellings. Example: House number (address) means coordinate; or Viet Cong will be spelled as Ve Vang, Cai Cach. The enemy's weak point is that during an engagement, they usually send out plain messages which will be easily understood by us."

The first thing you ought to grasp conceptually about the process of authentication is that it takes two principal forms—*challenge and reply* where the sender and recipient are in radio or wire contact with one another and can interrogate each other according to some system of authentication to establish their respective bona fides. The other and more difficult form of authentication is called *message authentication* in which the message itself carries with it *something* that tells the recipient that the message he has received is really intended for him and came from a legitimate source. We need this latter protection to prevent hostile intercept activities from faking messages altogether or picking up legitimate messages but *changing* their addresses so the wrong people will try to act on their contents.

The second thing to note about the authentication process is that it finds its greatest application where there is no cryptographic protection for the basic message text. Where full-scale machine cryptography can be employed on line, the basic cryptosystem "authenticates" the message. The message would not decrypt unless the sender had the key, and he would not have the key unless he was one of ours.

The third thing to remember about authentication systems is that there is one feature inherent in them that presents an extreme challenge to the group charged with inventing them—manual authentication systems must be swift and simple; but inherent in the process is the need to give the hostile analysts *both* the plain language (challenge) and the cipher text (the reply). To get ahead of ourselves for a moment, most modern sophisticated crypto-equipments are now good enough that we can hand the hostile analyst reams of our plain language and exactly matched cipher text to go with it, and still not provide him the basis for reconstructing the basic key or recovering any ungiven plain language. But our older machines could not stand up when the enemy was given the opportunity to match up plain language with its corresponding cipher, and we had to go to rather elaborate means to prevent this from happening. With simple manual systems, the difficulty, when you have to expose both your plain text and your cipher text, is even greater; yet that's exactly what we're being asked to do in any authentication system. For when you challenge with, "What is the authentication of ALFA BRAVO?" you are really saying, "What is the encipherment of ALFA BRAVO?" and the recipient is really replying that ALFA BRAVO enciphers to "CHARLIE NOVEMBER" or what have you. The result has been that most of our authentication systems over the years have been not very fast, or not very secure, or limited to very small networks.

25X3, E.O.13526

Withheld from public release under
§6 of the National Security Act of 1959,
50 U.S.C. 3605 (P.L. 86-36)

The primary authentication system used worldwide between and among ships, aircraft and
d forces is called TRITON. This system is illustrated below:

```
A RLCVJFTZQNXDHOKEGYSUPIAMWBYJAC   18-1
B EUYNKWDMLBVHTSCQJIFARZGXPOOKSX   19-2
C AEOKPXUTJLSRQYIWFGMBHNVCZDPGWK   20-4
D RGSZOAVHCINKLXFQJBYMUDEWPTUPHG   21-1
E TYFCKPEWQAJMXOGVNZUHSOBILRTIVN   22-2
F LJAPEQZMTFYWONKBSHXGRUDVICEQAI   23-3
G TDNXGFESKROIABHVMJUQCLZWYPXQMH
H NVRQEYIJDHOPLXMWCGSFKUZATBOKGM
I HOZFUQCRADYXKPJVNGMLBISWETEVBU
J QDLHJOWNCUZKSABEMRFVXYIPGTOWNU
K PSYKWHRCGDMIOBAVLTNQXFZEUJVEOR
L JWFKEAVMXSTDUCRIQBOLZHYPGNOWGH
M JYDZBIOENTHOGLCMKAXUPFRWSVHCLV   00-8
N VXFLJBCRGMHIZYEQASWTKUODNPXBAR   02-5
O FZWMYOAJLTPVUIBDSQNREGKHXCBFNR   04-7
P TASCIRGBJWQVEUHKYMOXFLNDZPPNLY   06-0
Q PFZNWYMXKSHCLBIVRGAUTEOQJDRLHK   08-0
R ONCSLDVURIHWJEB6FXATYPKQHZFUKT   10-4
S EFWBVTSZIHQNJAOYCMLDXURPKGNVWA   12-6
T RUEYZSQMDLFVOKTXHAPWBJGCNIOWTP   14-1
U RFWJHTBDYSKEVZUOLIGANXPCQMWNTJ   16-9
V VYPQKHLBZXFIMACTESOWDJGRNUMYPW   18-3
W RHDYPTIWZGLKQNUXBEQSCVFMAJLENW   20-6
X LHFRVYKDOSEPWIZMJNCQTGBXAUOIXP   22-3
Y JBVAXNLKWODHUSFQTYMREZIPGCHUZQ   24-1
Z JHZBIFRWGCUPLTSDVXYQOAEMNKVTBS   26-8
0 MCNTKZRIUVJDYSEXQWBOHPLFAGPVKA   28-9
1 UKHYLIQWVXJZFPGMCTADNORBSEOVDN   30-5
2 PIDQUTESXANGZHYFWVMKLJOCBRPNKS   32-5
3 BGIWQMLFJZOXSHDNVCUPKTYERAAYSQ   34-8
4 FXQACOSIVYGNWEBTKMUHJLZDPRVAPI   36-1
5 NZFVYOARSKIGTUPMDQWBLJCHEXPMRX   38-6
6 BLDAUFWJCGZMRNEXSKOQYVITHPKDQZ   40-4
7 NLAYDMIGWVOQRKEJHPFZBUXTCSXKJH   42-2
8 ZYLVXUNQROEBIWPGACJTFKSMHDMYSP   44-2
9 JRTPQHAKDGLUXONBWSEYVMCFIZQLDH   46-9
  ACPUMDXHJYTQGISBZEVLNKWORFMZQC   48-7
  PRJCVOKHASTFDQLMWZBIXNGUYECAFW   50-3
  IPVLNBWFGKJQOYMUZHXACTERDSIGHD   52-0
  QBLOGJEMICNYVZPKTRXSUFHWADPUKJ   54-7
  RJYNXPVEDBMGOUCSFHZIWKLTAQHKPI   56-4
  ZASCNQTMJKRGLBPVHYWIEUOXOFKYCI   58-2
DAY 02   1800-2359      KAA-29   EV /TSEC
```

B

DAY 2 1800-2359

A system such as TRITON introduces the notion of a "guess factor." Because the reply is two
rs, there are 26^2 possible answers (676) for a given challenge, but the internal structure of the
: provides as many as twelve correct replies for a given challenge. This means that the opposi-
can guess with one change in fifty-six (676÷12) of being correct. What all this means is that in
f-the-mill authentication, we have to settle for far less than perfect security. We do this to get
thing that can be used fairly quickly and by a great many people using the same table.
n 1974, the TRITON System will be replaced, worldwide, with the authentication system we
'ELE (pronounced PAYLAY). The PELE System, illustrated next is simpler and faster to
an the TRITON System. But, as always seems to be the case in COMSEC, this advantage
plicity and speed was achieved at the sacrifice of some security. With the PELE System, the
factor is reduced to one chance in twenty-six because the reply is only one letter.

You may wonder if it is a good idea to replace the TRITON System with its guess factor of one in fifty-six by a system having a guess factor of one in twenty-six. It is. The holders of TRITON are not using it very much because of its intricate operation. We expect the PELE System to be used far more than TRITON ever was. Here is a COMSEC fact of life for you: A system offering perfect security which is so complicated that the holder of the system cannot (or will not) use it, offers the same degree of security as no system at all.

The last type of authentication system that I want to touch on just briefly is a "one-time" system with the usual great security and narrow applicability. It's called BAMBOO TREE-KAA-101, and looks like this.

```
                    BAMBOO TREE
              AUTHENTICATION SYSTEM #1

          ACFT IN:

          ACFT OUT:

                ATC              GCA
          1. R G    9. Z O    17. R S   25. O X

          2. U H   10. A C    18. G I   26. U M

          3. E C   11. J L    19. H Y   27. C K

          4. W A   12. N N    20. J Q   28. W F

          5. H D   13. S I    21. D <   29. P U

          6. M X   14. M Y    22. Z W   30. N D

          7. T K   15. O R    23. D V   31. V S

          8. F Y   16. C B    24. C W   32. N Q
```

The difficulty with a system such as this is an administrative one—it demands very careful allocation of a small batch of authenticators for each pilot; they have to be assigned to each flight day and these assignments have to be controlled by the ground stations. Pilots cannot authenticate each other—that is, there's no air-to-air authentication capability because pilots cannot carry so large a deck or, even if they did, they don't have time to search through 1000's of cards to validate a particular authenticator.

Before leaving this section, I think a few remarks are in order to put the business of imitative communications deception in perspective for you. There is no doubt that many of our communications are susceptible to spoofing as evidenced by the imitative communications deception activ- of the Viet Cong and the North Vietnamese Army during the war in Viet Nam. I have already given you a live example of some of the techniques they used. I think you will find the following extract both interesting and informative. It is taken, verbatim, from the COMFEY STEED 1-73 JANUARY SUMMARY prepared by the Air Force Special Communications Center.

Imitative Communications Deception

This detailed knowledge of our unsecured tactical voice communications which the VC/NVA possess also contributes to their capability to use imitative communications deception as a tactical weapon. VC/NVA attempts at imitative communications deception, some of which have been successful, include attempts to lure rescue forces into traps, to shift artillery fire support to other targets, to cancel requests for assistance, to order ARVN patrols into positions susceptible to ambush, and to misroute strike aircraft; in addition to general harassment, interference and transmissions of a psychological warfare nature. Instances of sophisticated use of imitative communications deception have been detected and confirmed during the past two years.

In December 1966 an ARVN patrol received a call purportedly from subsector headquarters directing the patrol to a specified location. The message proved to be false and is believed to have been sent by the Viet Cong in an attempt to lure the patrol into an ambush.

In January 1967 the Third Marine Amphibious Force reported six instances of attempted enemy imitative communications deception in one week. Enemy communicators entered the aircraft control nets, speaking English, and attempted to misroute strike aircraft.

In February 1967, during an engagement, members of MACV Advisory Team 36 requested artillery support from their Fire Direction Center. As the Fire Direction Center prepared to furnish the requested artillery support they received another call in clear and distinct English requesting the fire be shifted to another set of grid coordinates. Team 36 overheard the new request and found that the artillery fire had been redirected upon their own position. Fortunately, they were able to contact the Fire Direction Center in time to prevent a serious accident.

In April 1968, during SEAL operations, it was reported that extraction forces received a signal requesting extraction which was not transmitted by the SEAL team.

A Viet Cong returnee, platoon leader of an antiaircraft platoon, stated that his supporting signal platoon was composed of personnel who could all speak English, and who routinely monitored Allied Forward Air Control and Provincial radio nets. They frequently entered the Forward Air Control nets and caused Allied planes to drop bombs on government troops, and then used the fact that government troops were being bombed by their own aircraft to convince them to desert and join the ranks of the Viet Cong.

Units of an Army Division operating near the Cambodian border engaged in a lengthy exchange of voice communications with a radio operator claiming to be the leader of an Australian patrol just ahead of them, when there was no Australian patrol operating in the area. The operator spoke faultless Australian-accented English and made continued efforts to get the American commander to accept him as a bonafide unit of the Allied forces.

A prisoner of war captured in February 1968 stated that his Battalion's procedure was to intercept ARVN air-to-ground and ground-to-ground communications and when the ARVN unit asked for assistance, the Viet Cong would call the assisting force and tell them to disregard the previous message as help was no longer needed. This resulted in confusion and delay and gave his unit more time to take offensive or evasive action.

These are but a few examples of the ever increasing capability of the VC/NVA to take immediate advantage of tactical intelligence derived through the intercept and analysis of our unsecured tactical voice communications. We cannot even estimate the number of attempts at imitative communications deception which have succeeded, and which have not been detected. Due to the VC/NVA successes in this field we can expect such incidents to continue as long as our tactical voice communications carry information of intelligence value to the enemy in the clear, and remain vulnerable to enemy intrusion.

We can see from the above examples that imitative communications deception was widespread in Viet Nam. But spoofing doesn't stop there. Spoofing also occurs in other parts of the world as well, but to a lesser degree because the opportunity for imitative communications deception is less in a "cold" war than in a "hot" war.

Although imitative communications deception is an on-going activity, it is not always an easy one. There is an axiom in the deception business which demands that the deception plan result in a specific action by the enemy which works to his disadvantage and to your advantage. As often as not, it's likely that the spoofing message will call for an action that seems illogical or dangerous to the recipient, and he will tend to double-check if he can.

Let me now make some summary statements about manual systems as a class. First of all, they exist in great variety and I have touched only on some basic types. Second, manual systems tend to get quite specialized and tailored to specific operational requirements. Third, they are slow compared with machines; and most of the ones that serve large networks have a pretty weak security potential.

We have talked about these systems at some length because they form a numerically large part of our inventory, consume a substantial part of our total production capability, and clog our distribution and accounting pipe-lines with very large batches of material. Yet the total amount of U.S. traffic committed to these systems is paltry—our machines carry by far the lion's share of our encrypted traffic; and the great usage of manual systems is where machines can't be used for one reason or another.

THIRD LECTURE: TSEC/KL-7

We're ready to talk now about a machine. It's called the TSEC/KL-7.
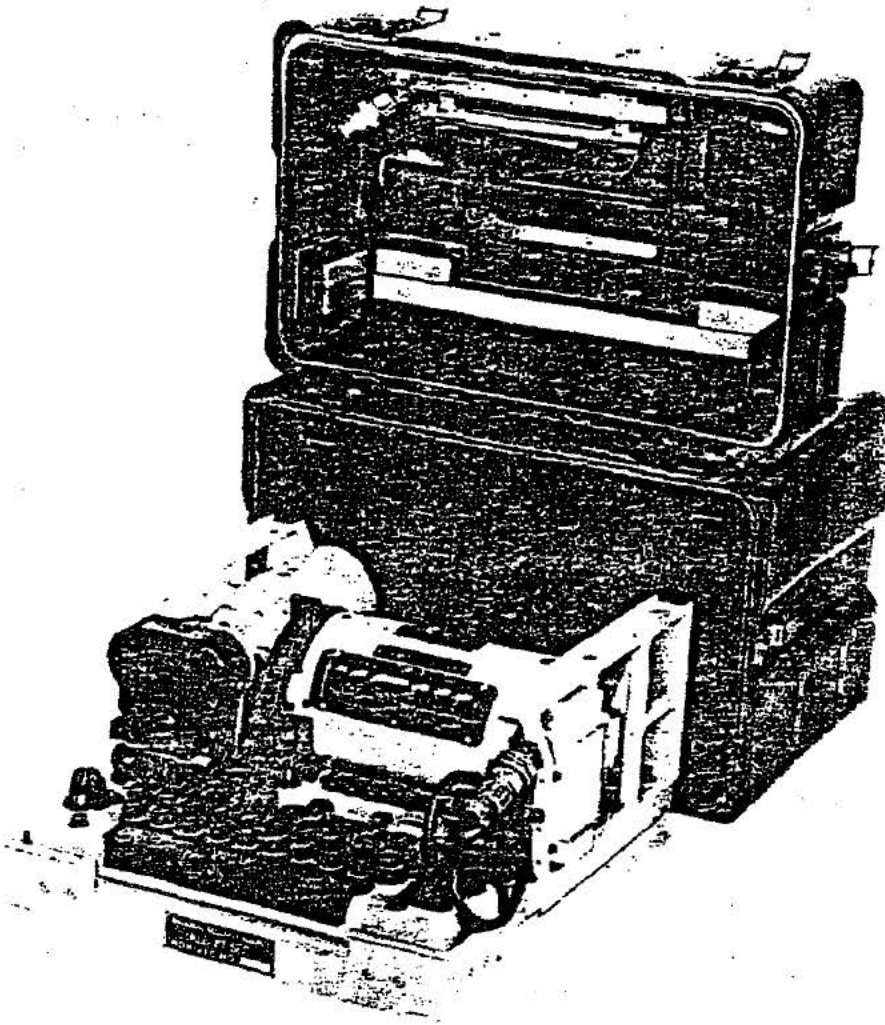
It is a *literal, off-line* cipher equipment.

Now we've *got* to have some definitions:

"Literal": of, pertaining to, or expressed by, letters, or alphabetic characters.

For you liberal arts students, the antonym for "literal," in our business, is not "figurative." We use literal to distinguish intelligence conveyed by letters of our alphabet from that conveyed by teletypewriter characters, speech, or digits. The output of a literal cipher machine looks like this:

DVRIT BLXMD QOGGA, etc., NOT:

+ + − − − − + + − − − − − − − + +, etc., nor

0110010011110010010, etc.

(However, when the communicator gets hold of the output, he may convert it to Morse code, or tele-typewriter characters to facilitate its *transmission.*)

"Off-line" is the term we use to mean that the machine is not connected directly to the trans-mission path; be it a wire line or a radio transmitter. The cipher message is *handed* to a communi-cator who sends it *after* the whole encryption is complete, when he has time and a free circuit to reach the addressee. The opposite term is "on-line" and in this case the cipher machine is hooked directly into the transmission medium, a receiving cipher machine is hooked in at the distant end, and encryption, transmission, and decryption are performed simultaneously.

"TSEC/KL-7": I'm still trying to put off a full massage of this nomenclature business as long as possible; but let me make a beginning because this is the first really formidable set of hiero-glyphics I have used on you, and you out to be aware that it is fairly systematic and formalized.

TSEC/KL-7 is the short title for the machine. The long or spelled out title is: "Electromecha-nical Literal Cipher Machine." TSEC is an abbreviation for Telecommunications Security which in turn is a full formal expansion of the term "Communications Security" or "COMSEC." There are only two important things you need remember about the signification of "TSEC"—one is that the item you see it attached to has *something* to do with securing U.S. communications: the other is that if it appears as the *first* designator of a short title, it refers to a *whole* machine; so TSEC/KL-7 is the whole hunk of hardware. If "TSEC" appears *after* some other characters in a short title, it means that the item referred to is only a component or part of a whole machine: so "KLB-7/TSEC" on the chassis, refers only to the base unit of this machine, *less* other removable components. The "K" in "KL-7" means, quite arbitrarily, that the item has to do with basic cryptographic processes, the actual conversion of something intelligible into encrypted form. If there were an "H" there in-stead, it would mean that the item merely facilitates the processing rather than actually doing it; the equipment is an *ancillary* or aid to the basic process, but does not do the encryption process it-self. We have something, in fact, called the "HL-1" which permits direct decryption of text in tele-ypewriter rather than literal form with a KL-7.

The "L" stands for "literal" which I've already explained; all the machines which produce cipher text in the form of letters of the alphabet carry the designator "KL" unless they are merely ancillary, in which case they are called "HL." You'll find a brief run down of the scheme in KAG-1/T

There is one more thing about these short titles: in common usage around here, we tend to strip them down to their very nub, and we usually refer to this machine as the KL-7. We used to refer to it merely as "the 7" but now there's a KW-7 as well, so we can't do that any more. We have a rule in correspondence, by the way; that is that we use the full short title the first time we mention a machine, and may abbreviate references to it thereafter unless there's a possible ambiguity.

The KL-7 is probably the last major *electromechanical* cipher machine that will see extensive use in U.S. communications. There is a fancier, heavier, more expensive version of it called the KL-47 used almost exclusively by our Navy. I'll say no more about it except to let you know that it exists and is *cryptographically* identical with the KL-7—that is, they can intercommunicate (a sure sign of cryptographic compatibility). From mid-World War II until the mid-fifties, there were quite a number of cipher machines that would process literal text or teletypewriter text and used the principles from which the KL-7 evolved. They had a great variety of names and applications de-pending on whether they were built by the Army or Navy or the British, or by the Armed Forces Security Agency, NSA's predecessor. Cataloguing their names and trying to recall where and how these systems were used is a favorite pastime of the old-timers around here who like to reminisce. Most of them have by now been melted to scrap or are quietly corroding in about 2,000 fathoms of salt water. (The machine, not the old-timers.) The basic principle that they used involves electri-cal commutators called *rotors* to form a fabulous and ever-changing set of electrical paths—a laby-rinth or maze—through which electrical pulses could flow.

SIMPLE THREE - ROTOR MAZE

IN <u> </u>   <u>OUT</u>
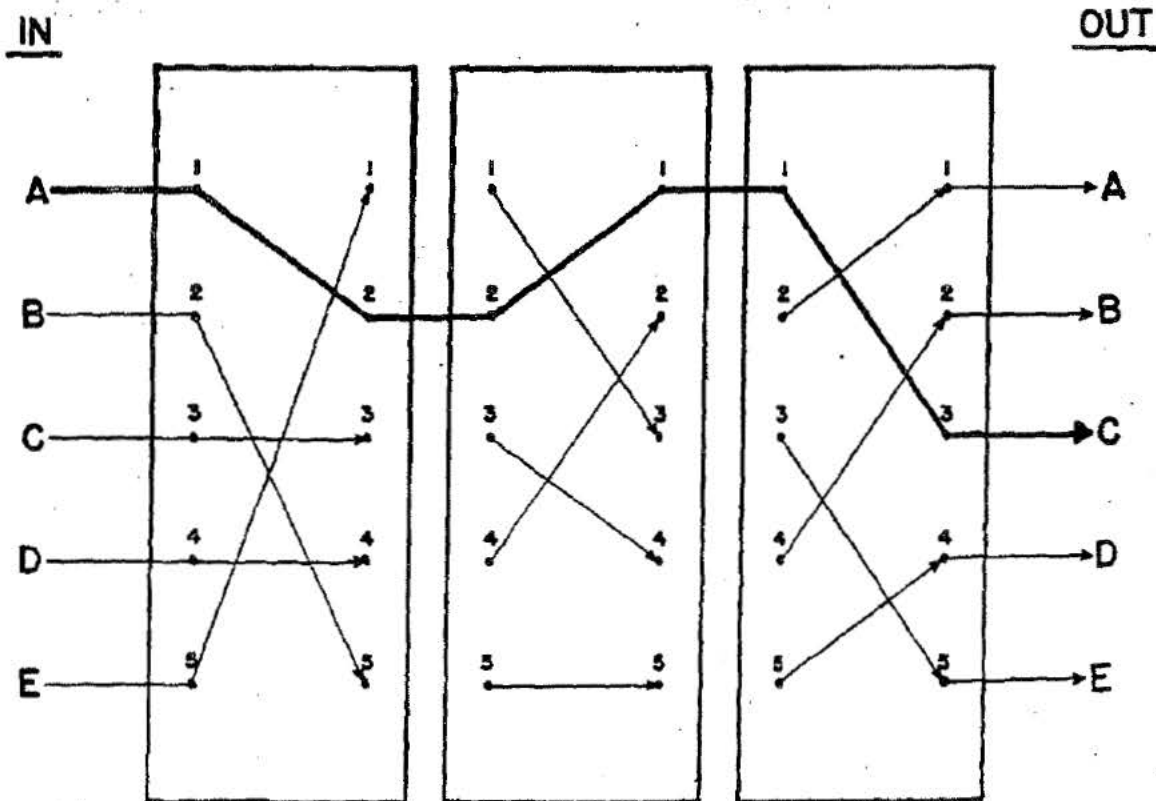
5 - POINT ROTORS

The security of these systems derived from the fact that these rotors could be placed in any of a number of positions, and could be aligned and moved in many different ways. With some reasonable bank of these rotors, say 5, they could be set up each day, *according to a key list* in any of 5 arrangements, and rotated to any of 26³ starting positions; so that any one of millions and millions of starting points were possible, but only one would permit successful decryption. Of course, the people you were sending the message to would have to know what that starting position was. So, the sender would *indicate* this starting point to his addressee through the use of what we call an *indicator system*. A number of such systems for telling the distant end where you had chosen to start were contrived. Some of them involved a separate little device designed exclusively for that purpose; some used what amounted to a one-time pad which listed a series of starting points for each holder, but by the time KL-7 came along, it was clear that the only efficient indicator system had to make use of the KL-7 itself so that users were not burdened with two sets of materials to operate one machine.

The rotors are called "variables"; each contains random wiring that can be changed from time to time (but not very often). We keep the same wirings for from 1 to 3 years in KL-7 rotors sets. Because the security of the system is not greatly dependent on the frequent changes of the rotor wirings, we call them "secondary variables." The *primary variables* are the things changed each day according to the key list—these are changes in how each rotor is put together or *assembled* each day and which position in the maze each rotor takes.

The *motion* of the rotors is important to the security of any system of this type. Various rotors have to move in unpredictable fashion; and in fact, at least two and up to seven of the KL-7 rotors move after each individual letter is enciphered. If none of the rotors moved, but just sat there letter after letter, the old bugaboo, monoalphabetic substitution would result, for example, if "A" hit the path that came out "X" the first time, that same path would be there each subsequent time the A key was struck, and X would always result.

So a number of schemes were used to control the motion of various rotor machines. The most secret and high echelon rotor machine of World War II had enciphered motion with a whole bank of rotors in it whose only purpose was to move another maze through which encryption took place in a random fashion. Another scheme was to use a kind of clock or metering mechanism which would direct one rotor to move every time, another every 26 times, another every 676 times, another every time some other rotor did not move, and so forth.

In the case of the KL-7, notched motion was decided on. According to very complicated rules, the presence or absence of one of these notches on a given rotor will determine whether some other rotor or combination of rotors will move. It's not important for you to understand these schemes, except conceptually, in this particular course. I've dwelt on them because, later on when I cover the strengths and weaknesses of current systems, I'm going to have to refer back to this business of indicators, variables, and rotor motion in the KL-7, because they are involved in some attacks on this system of which we had little idea when we built the machine.

There are some more terms about the principles of the KL-7 with which you ought to be familiar because you are apt to run across them in discussing it and other similar systems. So far, I have described the principle merely as one involving rotors. The effect of these rotors is to provide a means for *permuting* plain language letters to cipher equivalents:

PLAIN	CIPHER
A	X
B	Q
C	E
D	J

With each setting of the rotors, we have generated a new substitution alphabet for all our possible plaintext letters; every plaintext letter has a different and unique cipher equivalent. This, conceptually, is what the cryptographers are talking about when they refer to alphabet generators, or to

permuting rotors, or a permuting maze. Since the maze is set up in a new configuration, i.e., the rotors *step*; with each letter enciphered, we have in effect a little *one-time* substitution alphabet for each process. I'm not going to go much deeper into the details of this system, even in this quasi-technical fashion. I suppose, though, I ought to point out how decipherment is performed. Simple. Turn a switch and the letters struck on the keyboard go through the maze backwards. If the receiver has started in the same place as the sender, he will have an identical initial maze, and his machine will step to successively identical mazes because his machine contains the same variables and their random motion is a controlled one governed by identical things—in the case of the KL-7, the particular patterns of notches and no-notches on the periphery of each rotor.

The KL-7 was introduced into widespread U.S. and NATO use in 1955. Today it seems a rather clumsy and obsolescent machine to us because of what we can now achieve through pure electronic computer-like techniques. There is a limit to how complicated and fast you can make a machine which depends on physical mechanical motion of a lot of parts for its essential activities. We may have approached that limit with the KL-7 and, I suspect, tried to exceed it with one of its contemporary machines, the KW-9 with which we tried, using rotors, to encrypt teletypewriter traffic at speeds up to 100 words a minute. So a good part of our early and continuing problems with the KL-7 were mechanical/maintenance problems keeping the stepping mechanism and printing mechanism in order; keeping the literally hundreds of electrical contacts clean—one pulse may have to travel through as many as 80 such contacts to effect the encipherment of a single letter.

But don't underrate this little machine. With all its troubles, it is still passing thousands of groups of live operational traffic daily. It's resistance to cryptanalysis remains very high and it's useful life will reach well into the 70's. It remains, in my judgment, the best literal cipher machine in the world and we and NATO now have something like 21,000 of them.

Let me touch on some of its advertised features. It was our first machine designed to serve very large nets which could stand matched plain and cipher text. For the first time, the man in the cryptocenter could take a message and simply type it into the machine as written, without changing the spacing between words, or cutting the message in half and sending the last part first, and without having to paraphrase the message text before it was released. It was the first machine in which transmission of the indicator was a straightforward matter of sending out the letters lined upon the machine in the clear (a procedure which we abandoned about 1962 in the face of advancing cryptanalysis). It was the first relatively lightweight and secure electrical cipher machine with a keyboard—relatively light; by that I mean around 30 pounds, vs. about 90 pounds for its predecessors. It was the first equipment that could run off a jeep battery as well as 110 or 220 volt power. It was the first equipment that could encrypt both digits and letters without a clumsy adaptor—I ought to point out to you though, that the equipment turned out to be overdesigned in that respect. Numbers are so critical in typical military texts that the garble of any digit in them may cause real havoc—so, almost always, numbers are spelled out rather than put in upper case by KL-7 operators. It was the first machine designed to permit the ready removal of the classified components for secure storage so the whole thing did not need guarding or chucking in a safe. Finally, the rotors designed for it were the first that could be easily rewired by manually plugging their connections to new positions. All previous rotors had fixed, soldered wires so that changing their patterns was a slower and most costly process.

In 1966 we had about 25,000 of these KL-7 machines. Where were they used and for what? As some of you may know, we keep fairly careful records on the usage of most of our systems: each user provides a monthly Encrypted Traffic Report (or ETR in our jargon) in which he lists the number, length, and classification of messages transmitted. In the case of the KL-7, we found that the highest use was in U.S. Navy networks, next Army, and last Air Force.

It is quite apparent that large numbers of these equipments are rarely used; they are held in reserve, for privacy or as back-up for more efficient on-line teletypewriter equipments in most of the centers where teletypewriter service is available. Networks employing KL-7's range in size from 2 to 2,188 holders; a feature which perhaps I have not sufficiently stressed. Until quite recently, there

were very few machine systems which had the capacity to accomodate a thousand or more holders all using the same key; all intercommunicating without having to use unique sets of variables.

Before we leave the KL-7, let me give you another fragment of the nomenclature picture—that's the use of designators selected from mythology. You heard me use names like COMUS and DIANA to identify some of the manual systems we covered earlier. Some of the machine systems have these names—usually Greek—as well. The KL-7 system is called ADONIS. So is the cryptographically identical system produced by the KL-47. What these designators amount to are convenient means for identifying a specific encryption process regardless of the particular machine doing it. In the decade of the 50's, this method of identifying a cryptographic *process* was quite useful to us, because typically, two or three or four quite different-looking machines could all be made to operate identically; and further, each of them might be able to accomplish several quite different basic encryption processes by the change of some components or switches or procedures. So rather than saying "the system produced by the KL-7 or KL-47 using a 12-rotor set and encrypted indicators," we can say, simply, "the ADONIS system:" the same machines, but using only 8 rotors and indicators sent in the clear we called POLLUX.

These names are superfluous when only a single kind of equipment exists to do a job and that equipment accomplishes only one basic encryption process. Some of the new systems either don't have Greek names at all, or you rarely hear them; instead, we just specify the hardware by short title.

FOURTH LECTURE: One-Time Tape Systems

So far in these lectures, all of the systems I've mentioned have had one thing in common. They have widely differed in structure, process, security and application: the thing that has been the same about them is their relation to the communications process. They are all *off line* which means, once again, that they work essentially independently of the communications set-up; they are not tied into the communications path; the complete encryption process is performed *before* the cipher text is transmitted, and the nature of the communications system to be selected for the eventual transmission is not of much consequence.

From now on, with a few exceptions, the systems we will be talking about will be more and more involved with specific means of transmission; most of them will be on-line systems or systems with both an on-line and an off-line capability. This means that the machines themselves, or the ancillary equipments used with them will be more and more tailored to particular communications techniques and eventually, as you'll see, will involve the *integration* of the cryptographic process into the communication system itself.

The first and simplest set of systems lashed into their associated transmission means are the one-time tape systems. They are called the PYTHON systems for fairly obvious reasons. From World War II until about 1960, these systems were very popular indeed, and are still rather widely used. In both WW II and the Korean War they formed the backbone of secure U.S. teletypewriter communications. I can name more than 12 different machines built since 1945 for PYTHON operations. Their principle is deceptively simple, you merely take a stream of random key in *binary form* and *add* it—*combine* it, *mix* it—element by element, with plain text that has also been produced in *binary* form. To put intelligence into binary form is to convert it (or, in the generic sense, *code* it) into symbols made up of only *two* elements—1's and 0's—the familiar computer language; or pluses and minuses, or on's and off's, or marks and spaces or, as on tape, holes or no holes as indicated in the following illustration:
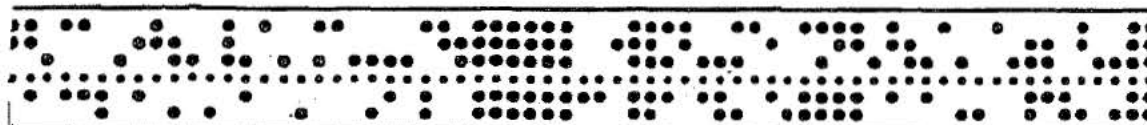
Various teletypewriter equipments automatically convert characters into this binary form, for example, in the Baudot teletypewriter code:

$$A = + + - - - ; R = - + - - ~, \text{etc.}$$

The additive or mixing process is done according to a simple, arbitrary rule: like signs = plus; unlike signs = minus. Now, let's add:

PLAIN TEXT .... $- + - - -$ $- + - + -$

RANDOM KEY .... $- + + - -$ $+ + - - -$

_____

RESULT (CIPHER TEXT!) .... $- - - + +$ $- + + - +$

It turns out, that if you take the same key and add it in the same way to the cipher text, the resultant product is the plain text again—and thus you decipher. If you can find a way to do this mixing mechanically, or electrically or electronically, you can visualize an extremely simple set-up. Your send and receive machines are identical and use identical key tapes in identical ways.

You do not have to reverse your process, switching everything so it goes backwards as we did in the rotor machine. The receiver merely assures that he is using the same tape as the sender, and has started it in the same place, and by adding it to the cipher text he has received, gets a copy of the original plain text printed automatically for him by the teletypewriter equipment.

Like all other one-time systems, though, the key must be used once and only once for encryption; if it's good random key and is used properly, the cryptographic security seems to be absolute. If you use the same key twice for encryption, the security drops to approximately 0, forthwith.

I said I could name about a dozen of the machines. The reason for the variety stems from two causes: first, the adaptation of machines to more and more refined concepts of teletypewriter communication; second, the need to prevent compromising radiation—the electronic emission of intelligence in the form of radio frequency energy from the various switches and contacts and relays in the equipment. We'll talk about *that* problem at some length in the last lectures.

The simplest kind of teletypewriter transmission path is a line from point A to point B with transmissions travelling in one direction only. This is called a *simplex circuit*. There are some obvious disadvantages: B can't talk back. A much more common type of circuit is a path between A and B on which either station can send when the other is silent. This is called a *half-duplex* circuit. Still some disadvantages: they both can't send at once—something communicators like to do, especially if each has a high volume of traffic for the other. The optimum setup permits transmission to flow in both directions simultaneously and is called a *full-duplex* circuit. Such circuits really involve two separate radio paths or two pairs of wire lines, but some of the terminal equipment may be shared. Different kinds of one-time tape crypto-equipment were envolved to fit with these differing communications setups.

The simplest way to send teletypewriter characters over the paths is by what is called "Start-stop" operation. The receiving machine *waits* until it receives a character. deciphers it, moves its one-time tape one position, and waits for another character before operating again. So it keeps *in step* with the sending machine by using each actual cipher character received as a signal to advance. Most of the old one-time tape mixers worked this way. But suppose the transmission fades momentarily, and the receiving machine misses just one character: or suppose some spurious pulse hits the signal line and causes the receive machine to advance when no cipher character was really sent? Then the two machines are out of step—synchrony between send and receive tapes is lost, the keys no longer match, and thereafter the receiver deciphers gibberish until the operator can signal the other station to stop and they get themselves in step again. So they began to design machines which would step along at a fixed rate once they got started together, whether every character was received or not, and the short transmission fades or spurious pulses simply caused a one-letter garble in the received text. These are called *synchronous* machines. and account for two or three more of the dozen mixers that have been in our inventory.

Yet another feature became desirable for some one-time tape circuits. You will recall that I have mentioned the term Transmission Security or "TRANSEC" just once so far. We were discussing a manual one-time system and I alleged some COMSEC shortcomings despite its great resistance to cryptanalysis. The bread and butter of *transmission security* specialists is the information that they can glean merely from analyzing message *externals* as they are transmitted. Call signs tell them something, so do routing indicators, so do cryptographic indicators, so do the numbers and lengths and formats of messages, so does the direction in which traffic flows. If the government is planning a secret operation in some remote or not so remote place, there is almost bound to be a great spurt of message activity to and from that place, and all the opposition need do is note this surge of communications activity to be put on guard. The technique which we now commonly use on teletypewriter links to remove most of these flags on impending activity is called *traffic flow security*. In a one-time tape setup, the way it is accomplished is to simply send cipher text or something that looks exactly like cipher text *all the time*. Instead of cipher characters being transmitted by fits and starts only when an operator is actually typing a real message, or where a few hundred groups are coming out in a stream if the operator is sending his message automatically from a previously punched message tape, the machine is rigged so that whenever an actual mes-

sage is not being sent, the successive characters of random data on the key tape itself are automatically sent instead. So the roll of tape just sits there and unwinds all day, encrypting anything you happen to have for it and being transmitted itself otherwise. The tape on the other end is doing the same thing, of course. All the interceptor sees is an apparently continuous flow of random information. What does the receiver see? Since his tape machine tries to decrypt anything it receives, it winds up decrypting *key* when no bona fide traffic is coming in. Let's have a look at what any one-time key decrypted (i.e., added to itself) looks like. Remember our rule—like signs = plus; unlike's = minus.

$$++--++++-+++--$$
$$++--++++-+++--$$

$$+++++++++++++\ldots.\text{All pluses!}$$

And all pluses equate to the letters shift character in the Baudot code, and it's a relatively simple matter to instruct the teletypewriter to stop operating until it gets something else. Otherwise, you can just let it run. So, equipments with this traffic flow security feature account for a couple of more of our many PYTHON machines.

Well, let's have a look at the advantages and disadvantages of these PYTHON systems. The first advantage is relatively great speed compared to any of the systems we have described so far. In most of the manual systems you feel like a whiz if you can average four or five words a minute; in our off-line rotor machines, we were happy with 25 words a minute and simply couldn't go much more than 40. But a PYTHON system operates at standard teletypewriter speeds—66 or 75 or 100 words a minute. And besides, when you're *on-line*, the message is being received instantaneously at the distant end; so with PYTHON we are moving toward the goal of secure communications in which no delay in message delivery can be attributed to the cipher process itself. You're still consuming a little time in pure cryptographic processes—you have to select and set up the proper tape; you have to send an indicator of "Set" to the distant station to tell him what tape to use and where to start it; but most of the time is spent in preparing the message for transmission—punching it up on a message tape ("poking" they call it) before feeding it into the machine—this is something you have to do anyhow for efficient teletypewriter communications in any volume. So, on the matter of speed, we have made a great leap forward.

The second advantage is its relative simplicity: most of the system consists of standard time-tested teletypewriter machine components which are commercially available; maintenance is relatively easy; teaching an operator to work the system is simple; mistakes are hard to make and only one mistake—the reuse of a tape—is dangerous to the security of the system. (In contrast, on a system like KL-7, there are a dozen or more things that operators can and do do wrong which give us grey hairs.) There are other things that can go wrong of course; technical things, like the tape getting torn and failing to feed properly and the machine going merrily on encrypting all of the message using whatever key character the tape happened to stick at—monoalphabetic substitution again! But there are a number of safeguards built in for contingencies like these, and by and large it is safe to say that a typical one-time tape system is both reliable and highly secure.

So, the advantages, in summary are: fast, simple, reliable, and secure. How about the disadvantages? By now, the first disadvantage ought to leap readily to mind. They are one-time systems, and the inherent disadvantage in all of them applies here. Only two or a few more holders can intercommunicate in a given system—we make a few "five way" tapes and "ten-way" tapes to accommodate some broadcast or conference type teletypewriter communications; but it's a difficult job to get everybody in step and keep them there, and by and large the two-holder or "point-to-point" system prevails.

The second disadvantage is a logistic one: imagine the complexity of the distribution system that gets thousands of pairs of these tapes out, to holders all over the world. Their bulk, in a large communication center in which many tape systems terminate, is staggering. In their heyday

●60,000 rolls of tape were produced by us in 1955. Production is around 55,000 now. The consumption of these tapes is particularly distressing when that transmission security feature—traffic flow security—is employed. One of these eight-inch 100,000 character rolls lasts about 166 minutes at 100 words per minute; they cost us $4.55 each.

At any rate, their usage has begun to decline sharply as more efficient means for doing the same job have evolved. As early as 1942, the people designing cryptomachines had tried to come to grips with the logistic problem associated with one-time tapes. All the one-time tapes used by the U.S. come right out of Operations Building #3 in what is called a tape-factory. Great batteries of tape generation equipment, which will be described to you later in the lectures on the production process, can spew these tapes out at the rate of thousands of three-inch rolls per day. In the old days, the manufacture of these tapes was slower. Very large machines were used to produce carefully checked random data to be punched into the tapes. "Suppose," said the cryptographers, "*you could build a machine that could generate its own key as it went along* and feed that key to a mixing or combining circuit electrically without having to punch it up in a painstaking mechanical fashion on a stretch of tape? Give the man at each end of the circuit a *key generating machine* which, from given starting setups, would produce identical key that could be used in this same old binary additive mixing process that works so well with the one-time tape systems. Then, instead of having to distribute carloads of tapes to these people, we would merely need send them a little printed key list containing the settings that should be used for the variables contained in the little key-generating machines."

And that's what they did. They called the equipment SIGTOT in accordance with some old Army Signal Corps nomenclature scheme. It used rotors, and it worked pretty well. Its key output fed into a standard one-time tape mixing machine and got combined there in the regular old way. But it used rotors with all their mechanical difficulties, and we found ourselves shipping around truckloads of rotors instead of carloads of tape. When you see the tape factory, you'll note that a rather massive batch of machinery with all sorts of checks and alarms are used to assure a completely random ●oduct. When you try to compress essentially the same operation into equipment about as big as ●●readbox, you might expect troubles, and we had them. We wound up with all sorts of precedural ●traints on the use of these systems for security reasons, and eventually had to use a set of no less than 30 rotors to support each machine so as to provide an adequate bank of variables to choose from. Still, the SIGTOT, with various modifications, lumbered on in some quantity from WW II until the mid-fifties and the last ones did not disappear until about 1960.

****

So far, we've confined ourselves pretty much to how these various systems work, what they can do, and what they are for. Before we jump into the electronic age of cryptography, perhaps it would be well to discuss some of the things that go into the production and support of a cryptosystem beyond the provision of sound cryptoprinciples and some techniques for making them work—by embodying them in pads or charts or tables or in some kind of cipher machine. Implicit in what I've said already, you have to have somebody design and develop these systems and, in the case of hardware, that's what NSA's R&D COMSEC organization is for. You have to have somebody *evaluate* these designs; and it seems sound practice to have a body of people who are separate, objective, disinterested, do this job—not the inventors themselves who are apt to have prejudices and blind spots with respect to their own brainchildren; and that's what our COMSEC analysts are for. You have to have somebody who can take these approved designs and prototype equipments and engineer them into fully tested working systems that can be produced efficiently and in quantity—to make a finished product which, in addition to being theoretically secure will be economical, reliable, and practical to produce and maintain. That's what the COMSEC Office of Communications Security Engineering (S2) is for. There are still more things you need. You have to have an organization to produce and distribute these volumes of variables on which every one of these systems in one way or another depends. That's what the Office of Communications Security Production and Control (S3) is for, and, of course, you need instructions. You need the specific operating instructions that tell operators just what to do, what processes to follow, how to react if something goes wrong; you need systems planners to anticipate and meet requirements and to get

the right equipment applied to the right job. You need a very involved and interlocking set of security controls over the materials and equipments in the inventory—you need to decide how to mark, classify, ship, store, account for, and eventually destroy every item. You need a whole system of surveillance to watch over systems as actually used to assure that they meet their security objectives and, where they don't because something has been lost or some other catastrophe occurs, to implement, and implement at once, whatever countermeasures—like the emergency supersession I talked about—that can be put into effect. This means a world-wide reporting system to inform us electrically of events that may effect our COMSEC posture, and a large quantity of back-up or reserve materials for use in an emergency. During FY-72, the Office of Communications Security Applications (S4) was established to better support the systems approach to COMSEC. This organization consolidates and emphasizes the S effort towards the system approach, wherein security is functionally and physically intergrated into communications-electronics systems of all types. It insures a consistent and coordinated effort in meeting NSA's responsibilities to system designers, developers and users for providing COMSEC support and provides a focal point within S for outside organizations to turn to in seeking assistance in systems matters. And finally one of the most difficult jobs of all—you need a large, consistent, coherent, practical, responsive, safe, reasonable, and understandable body of *doctrine* to govern the whole shooting match, and this is what the Office of Communications Security Standards and Evaluations (S1) and the Technical and Planning Staffs are for. And these are all more or less central functions here in NSA; large counterpart organizations, especially in day-to-day monitoring and administration of systems, are required among the users. For what we are talking about here is the management of a very large operation— not only are millions of copies of paper materials involved, but we are supporting on the order of 100,000 relatively delicate, undoubtedly contrary, tricky, recalcitrant, *classified* cipher machines.

Perhaps you did not realize it, but what I've just done is sneaked in on you a rundown of the functional organization of the COMSEC part of this Agency.

I have implied that the business of protection and control of cryptomaterials constitutes a large and difficult area of endeavor for us. While one-time tape machines are fresh in your mind, I want to discuss classification for a moment, because there is a small controversy about the classification of these equipments and it is illustrative of the kinds of control problems we encounter.

25X3, E.O.13526

25X3, E.O.13526

The second reason is clearly a COMSEC one. Even our newest one-time tape mixer is not perfectly secure. I keep titillating you with this business of compromising emanations; we want to keep other people from discovering the techniques we use to suppress these emanations; and we also want to make it difficult for them to find out where we have still been unsuccessful. It turns out that the ideal way to exploit the radio frequency or acoustic emissions from a cipher equipment is to get the thing in a laboratory and test it very thoroughly and minutely to find out in what part of the spectrum, if any—the emissions are escaping and just what their characteristics are. Having done this, you know how to zero in your intercept equipment in the much more difficult environment where machines are actually operating, and your chance of success is much greater than if you have to go at it blind.

There is another related and long-standing notion about classification of crypto-equipment that is worth discussion here. It involves a rather difficult concept, more often misunderstood than not, and one that often causes much anguish among our customers each time it leaks out in distorted or incomplete form. Here it is: whether we're talking about a one-time tape machine, or the KL-7, or a modern key generator system, the essential security lies in the variables supplied with the equipment, *not* in the configuration of the equipment itself—not in its wiring, motion, activity, or processes. This means that if the machine is lost, no past or future messages encrypted by it will be jeopardized unless its variables—its *keys* are lost as well. There's a very practical reason for designing systems this way: no matter how highly we classify an equipment or how carefully we guard it, we cannot *guarantee* that it will not be lost. All of them are designed to be useful for 15 to 20 years and a lot of things can happen in that time—military units can get overrun; planes can crash in hostile territory; people can defect. We simply can't afford to replace 10,000 key generators or 25,000 KL-7's should that happen.

So, in a nutshell, if you lose the equipment, but not the keying material, your traffic is still secure. When the customer hears this, he has a natural question: why in the world do we insist on classifying these machines then? And he has more than an academic interest: the protection of these machines costs him money and time and guards and vaults and specially constructed crypto-centers and a host of attendant headaches.

Well, why *do* we insist that this expense to the user—and it's a real expense—is a worthwhile security investment? I have already touched on the matter of general exposure of our technology. But there are even more cogent reasons for trying to protect principles and details of machine operation *when we can*. The first is this: although we strive for reliability, and sometimes can afford to incorporate rather elaborate alarms, machines do sometimes fail or partially fail. In the case of a modern high-speed key generator, thousands or millions of bits of faulty key or cipher text may be put on the air before the problem is detected and the machine halted. There may be even more insidious failures that do not affect communicators' ability to encipher and decipher messages, but seriously weaken the resistance of the system to analysis. The discovery of exploitability of such situations by hostile interceptors may well depend on whether he understands the fundamental structure of the machine in use; so denying him that information to the extent we can is important. Similarly, operators may make mistakes that may be harmless if the interceptor does not understand the system, and exploitable otherwise. Note, the basic proposition is still that the traffic is secure with the machine known, but with the keys safe. We have to modify that statement to indicate that this is so except in cases where the machine is operating improperly—and sometimes they do operate improperly. And we have said, there's not much problem so long as the keys are safe. The trouble is we *do* lose keys (in FY-72 there were 325 incidents of loss and unauthorized viewing). But a stolen key will generally not do the hostile analyst much good unless he knows how the machine works that uses it. Finally, the most important reason for protecting machines is that a hostile cryptanalyst generally cannot even make a start on the analysis of any cryptosystem until he has been able to discover in some detail what the basic processes of encryption are. This is borne out by the very considerable investments our own SIGINT organization has made simply to find out target systems work; it's a prerequisite to any subsequent analysis.

FIFTH LECTURE: KW-26; KW-37; CRIB: KW-7

Now, after that small excursion into the realm of doctrinal, organization, and classification matters, let's return to hardware. First, I'll bring you up to the present with respect to teletypewriter security equipment. By the mid-fifties, computer technology was fairly far advanced: the impact of this technology on cryptography has been enormous in two respects. In the first place, for all but the one-time machines, security rests on the fact that we provide a very large but *finite* number of variables: we confront the hostile analyst with a system which can be set up in any one of millions or billions of ways so that "guess factor" in a machine instead of being something like 1 in 26 in our weakest authentication systems, is 1 in many billions. So, in a straightforward cryptanalytic attack, what he may want to do is to try out every one of the possible settings in the system, matching each trial with intercepted cipher text and when he hits the right setting, plain text results and he has recovered the day's setup. In the old days with weak systems, analysts might try to do this by hand, making a few hundred guesses or trials a day; later punched card equipment and other electromechanical equipment were used so that 10's of thousands of trials might be practical. But, *with computers*, our analysts and the opposition found a tool that would permit *1,000's or millions of these trials to be made each second.* The result was, that in cryptosystem design, enough variability had to be assured to resist postulated computer attacks of enormous power; perhaps entailing a hundred or more computers operating simultaneously against one system at speeds of 10^4 seconds for years on end!

At the same time, computers provide a practical technology for translating pretty well known mathematical techniques for producing very long unpredictable streams of data into electronic hardware. Such machines could be constructed to accommodate a barrelful of variables; a completely new set of variables could be inserted ("programmed") simply by use of an IBM or Rem-Rand punched card; the circuitry was ideal for performing the usual binary addition to the random data—that is the key stream—with plain text presented to it in digital form. So the notion of a cipher machine which was really a self-contained *key generator*, which had its clumsy beginnings with the SIGTOT rotor machine, came into its own with the computer age and, in 1957 we began delivering the first of about 15,000 TSEC/KW-26 machines for the rapid, secure, on-line synchronous transmission of teletypewriter traffic. Out went the SIGTOT's (by this time having undergone their fourth major security modification and umpteenth procedural change); out went most of the one-time tape machines on high-level TTY links. The KW-26 system turned out to be a jewel. I have heard some Service cryptographers who had been skeptical of the role of this centralized Agency say that this system, the TSEC/KW-26, more than any other, made the reputation of NSA and solidified its position as the authority in cryptographic matters.

The advantages of the system over its predecessors really are manifold. It has no moving parts, and its speed is limited only by the speed of the associated teletypewriter equipment. One three-cent punched card for the daily setup replaced about $20.00 worth of tapes. It could be programmed to operate in a variety of communications modes; it is designed for rack-mounting and was the first major crypto-equipment built to be part of the *communications* center rather than being cloistered in a dark vault-type corner—that aloof, separated *cryptocenter* of the old days.

The cryptoprinciple was based on the mathematical discovery of an Italian name Fibonacci (1170-1248) who is alleged to have contemplated sunflowers and noticed that the number of seeds progressing from the center of the periphery of the flower forms a very peculiar, irregular, and apparently unpredictable numerical sequence. (All this sounds like Newton's apple, and may or may not be apocryphal.)

There's one more thing about the principle of the KW-26 I ought to mention. When we use a one-time tape or a one-time pad to provide key, and add our plain text to it, we use every element of the key: I've said a couple of times that, should you use such key more than once, all security is lost. When two ciphertext messages are based on the same key, the messages are said to be "in

depth"; and the thing that provides the analyst a means for successful attack is the fact that the identical element of key underlies two different cipher characters. To frustrate this kind of an attack on the KW-26, the designers made it so that it produces 32 times as much key as it needs: only one key element out of each thirty-two is used; the rest are thrown away. So should something go wrong with the machine, or should somebody use the same key card twice (and that's hard to do because the card gets automatically cut in half with a knife any time you try to remove it from the machine), only one character in thirty-two is "in depth", and that's not enough for successful cryptanalysis.

But the KW-26 can't do everything. It is essentially a point-to-point system, and you need a great battery of them when you have to communicate with a lot of different stations. In March 1973 here at Fort Meade, where the CRITICOMM system terminates, we had 336 KW-26's lined up and operating all the time. We have some tricks so that a single KW-26 can be used to send to a number of receiving stations at once, but the scheme is not very efficient and I know of only one net employing it.

We do have a requirement for *broadcast* of secure teletypewriter communications, with a few central stations sending out information and instructions to a large number of receiving stations simultaneously. The Navy is the principal user of such systems to notify all the ships at sea of ship movements, weather, general information, instructions to the fleet, etc. The system we have provided for this is called KW-37. The "W", by the way, stands for "teletypewriter", just as it does in the KW-26. The specifications for this system were pretty tough. Not only did the Navy want to be able to reach 100's of receivers simultaneously; they wanted each of those receivers to be able to tune in at any time in the day and, knowing only what the day's key card was, be able to begin decipherment even though the transmitting machine had already been running for hours. You'll recall that in every other machine we've talked about so far, this business of getting machines in step and keeping them there was crucial; and we accomplished it by sending out an *indicator* and, when we were on-line, starting off both machines at essentially the same time. Now we had to find a way to allow some laggard receiver to "catch up" with the sending machine, starting blind, and with no way to communicate with the transmitter to ask him where he was. It wasn't done with mirrors—it was done with *clocks*. The transmitter always gets going at the same time; say 8:00 A.M. Greenwich or "Z" time; the receiver sets his clock close to the actual time when he wants to get into the net—say noon—and then starts his receiver key generator at its initial (8 A.M.) setting and flips a switch that causes it to generate at 570 times its normal speed until it *catches* the transmitter. As it approaches the setting of the transmitting key generator, that is, approaches synchrony with it, it looks at special timing signals coming in from the transmitter, locks on them, and then reverts to normal speed and is able to decipher the incoming traffic thereafter. The time it takes to do this is from a few seconds to a maximum of 2 minutes, depending on how far behind the receiver is when the process is begun.
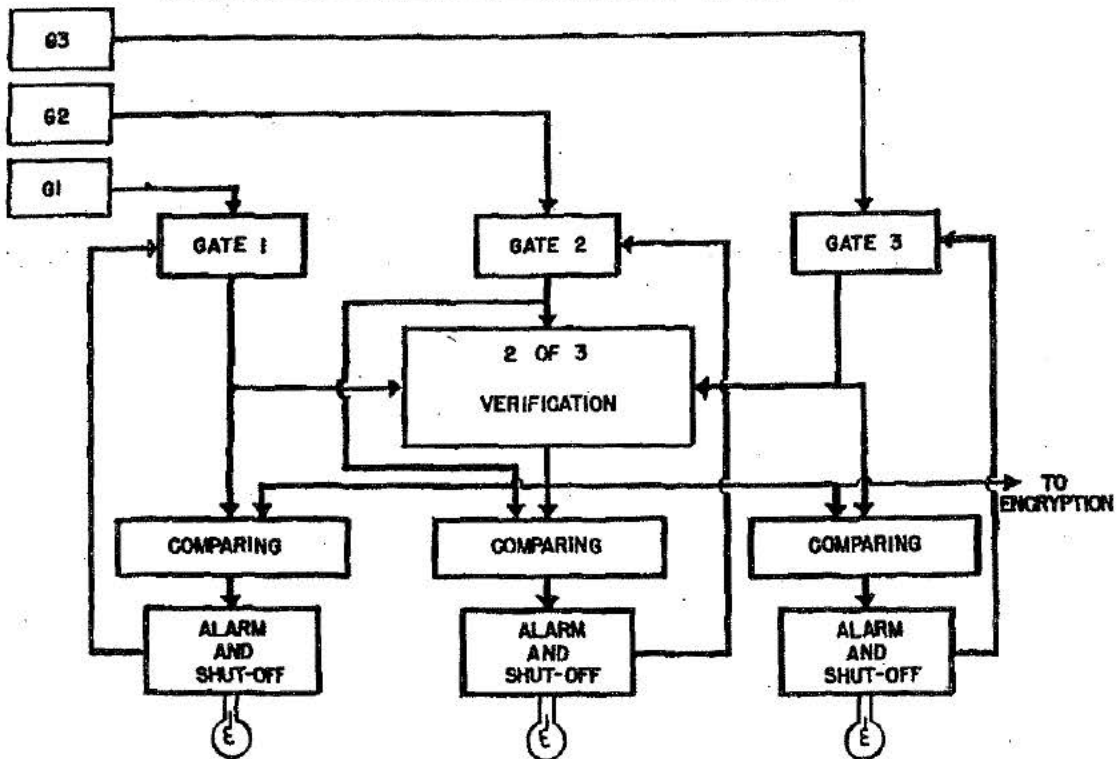
There is yet another difficult requirement associated with broadcast operations: that is that the transmitting equipment must be ultra-reliable. Once it gets going, it can't afford to stop. There are both security and operational reasons for this. In ordinary on-line TTY operations, obvious faults in the transmitting machine are immediately detected by receiving stations because garbled traffic is produced. The receiving station can stop or "BREAK" the sending station before much damage is done and have it straightened out. But without a ready return communication path, as in the case of KW-37 networks, a faulty transmitter might send gibberish to the fleet all day. From the operational viewpoint, even if he does detect it, perhaps by a monitor of his own broadcast, he can't stop transmitting or, rather, when he does, can't get started again because the clocks are all thrown off.

How did they solve this one? I believe I mentioned in passing that most of our modern systems have various alarms in them to detect possible failures. In the KW-37, the concept of alarms has reached, possibly, its ultimate. Instead of using a single key generator in the transmitter, we use three identical ones which, each day, are set up with three identical key cards. They are so interconnected that the output of each key generator is compared digit by digit with the outputs of the other two generators as indicated in the following diagram:

KW-37 VERIFICATION AND ALARM CIRCUITRY - SIMPLIFIED

G3

G2

GI

GATE 1

GATE 2

GATE 3

2 OF 3
VERIFICATION

TO
ENCRYPTION

COMPARING

COMPARING

COMPARING

ALARM
AND
SHUT-OFF

ALARM
AND
SHUT-OFF

ALARM
AND
SHUT-OFF

E

E

E

i all three put out identical key, we know that either they are all operating exactly as they should or that all three have somehow developed some identical fault. We assume the former situation is the case, and begin transmitting. Now, after operation has begun, if one of the generators develops a fault, its key stream will no longer match the other two: the machine operating on a "majority vote" principle assumes that the two matching keys are correct and continues to operate using one of those keys. But lights light and bells ring on the faulty key generator; the maintenance man can pull it out of the rack, fix it or replace it while the machine carries on so long as the outputs of the two remaining key generators continue to match. Foolproof? We thought it was nearly so. But to show you how far out this business can get, and how careful you have to be; and to illustrate "Murphy's law" which says that anything that can possibly go wrong sooner or later will, let me tell you what happened during some of the early Navy testing. The main components of the KW-37—as in most of our modern electronic equipments—are printed circuit boards containing relays and transistors and shift registers and combining circuits and the like. About 80 of these boards go into the makeup of each of the KW-37 key generators. Routinely, during maintenance, some of these boards are removed. The Navy discovered that there were some boards in the KW-37 which could be removed without stopping the machine. But the generator would put out faulty key. They put two key generators into operation with the same boards missing and used a faultless key generator as the third one. Sure enough, the machine went through its majority vote process and, because the two keys from the generators with missing boards matched exactly, the machine used their key and rang bells and lit lights saying the only good generator was bad. So the system had to be modified to include interlocks so it would not work with missing boards. The KW-37 happened to be a Koken, not a Fibonacci: the overall process of key generation is quite similar, but the specific rules of motion for producing successive bits of key are different.

At this point, I ought to mention the CRIB (Card Reader Insert Board), presently in use in the KW-37, certain KG-13 nets, and planned for use on several other keycard equipments.
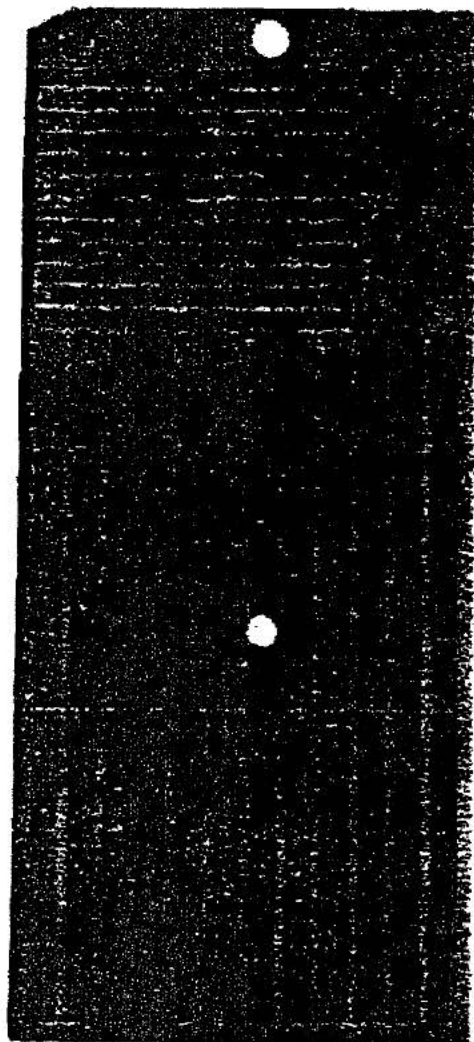
The CRIB is in fact a circuit plate to be mounted in the card reader as a replacement for the circuit plate originally supplied; there it serves as a second keying variable. If the original circuit plate is thought of as one that is "straight wired", then the CRIB can be considered as one in which wiring is "scrambled", for it establishes a different set of interconnections. We issue the CRIB in various editions. Each has a different short title (USKAW-IG/TSEC, USKAW-2F/TSEC, etc.), and each is effective for a specific time period. The conductive paths provided by each edition differ from those of other editions. Two equipments equipped with CRIBS are able to communicate only if both use the same key card and have the same edition of the CRIB installed in their card readers.

So far, the modern machines I've talked about have retained some of the inflexibilities inherent in this business of using a single long stream of key and using it only once—only a few people can *intercommunicate*. Normally two in the case of KW-26; and only one sending and a lot of people listening in the KW-37. What was needed was a new principle or an adaptation of the old one which would permit a large number of people to *initiate* transmissions all using the same key list, or plug board or punched key card or what-have-you. Remember, we had this capability with some of the rotor machines like the KL-7. The way we did it was by sending out some *random* information—an *indicator*—with each message. This indicator started us in one of millions of possible alignments

thin the basic setup of the machine for that day. We needed something analogous in the electronic key generators because it is through this process that you can generate millions of unique streams of key from some basic settings of the machine.

Remember that the Fibonacci principle in the KW-26 was predicated on an initial sequence of random 1's and 0's. The day's punched key card could supply that sequence. Now, if with each message something unique and random was added to it, then we had the basis for generating many key streams—one for each message—and a way, therefore, for many holders to originate messages using the same basic plugging or key card setup. The first equipments using this idea happened to be for voice encryption, but the idea is the same, and it is now used in the brand new tactical tele- typewriter security device called the KW-7. A device called a *randomizer* is provided within each equipment; it uses some unstable or "noisy" diodes that emit electrons in a random fashion; these are converted to digits (1's and 0's again) fed into the transmitting machine and, at the same time sent out to the receiving machine. The effect of this random stream is to alter the day's setup in an unpredictable way, but in the same way in every machine receiving it. Thereafter, the equipment operates like a normal key generator until the message is finished. When it is, and another mes- sage is to be sent, the "Start" buttons is pushed again; a new random stream is provided by the randomizer, and the equipment again operates, but on a new key.

We have more or less backed into the subject of the KW-7 and so far your conception of it must be rather hazy: I've said it's tactical, and that a lot of people can intercommunicate with it because it uses a randomizer to alter the basic key for each message. Also, it is not set up with a punched card. Why not? Because the user decided he didn't like key cards, and wanted a way to set up the machine from some information printed on a piece of paper. We're not sure the user was right about this; and evidently, he's no longer sure either because he is now asking for us to modify some of them to accommodate setup by punched card.

It will be useful to know something about how requirements arise—why new machines are ilt—and how we go about it. The user buys these machines from us although we pay for the re- arch and development work ourselves. The chain of events usually goes something like this: One of the three Services decides it needs a new crypto-equipment—say, a tactical teletypewriter equip- ment. He'll decide this because their existing equipment is obsolescent: too heavy, or too slow, or too expensive, or incompatible with new communications techniques, or this Agency has said its security is becoming marginal, or something. They will then describe what they want in terms of its size, speed, power requirements, amount of security needed, and the like. They will then consult the other Services to get an expression of interest. If the other Services think they also need the same thing or something similar, they may get together and write what are called Joint MC's—or mili- tary characteristics. They will send these MC's to NSA and either ask NSA to build such an equip- ment, or ask that NSA delegate the authority to one of them to develop the equipment. Usually, NSA winds up doing it. Then that functional organization I described to you takes over—R&D decides on a cryptoprinciple to meet the security needs, the intercommunication requirements, the speed and volume of traffic specified, and the kind of communications to be used. S1 evaluates the principle and, having given it the go ahead, R&D develops hardware, usually starting with hand- made "breadboard" models in their own laboratories and finishing with a full development con- tract in industry. S2 tests the development model, arranges for Service Test models to be made—if it seems good enough—or arranges for service testing of the development model to save time; the Services state what they do and don't like about it, and what they want changed, and production models incorporating these changes are made. This whole process can be as fast as 18 months from conception to hardware as was the startling case of the great KW-26, to many years as in the frus- trating case of some of our tactical voice security equipment. Meantime, systems planners and policy makers are not sitting idle; they are looking for optimum applications; establishing programs for phasing out older equipment, deciding whether other requirements can be fulfilled with the oncoming hardware—does NATO need it? Is it in the best interest of the U.S. to release it to NATO nether they need it or not? And so forth.

So, the KW-7 followed that general process. It has features in it to satisfy special needs of each of the Services, e.g., adaptors . . . . It was offered to NATO in competition with some comparable equipment being built by the UK, France, Germany, and Norway. It can provide for secure communications among hundreds of holders all using a common key; it's mounted in some aircraft and on wheeled vehicles, and we expect to see 38,000 in the inventory when production stops.

So, in the teletypewriter field, we have talked about three main equipments—the KW-26 for high-speed point-to-point communications at generally high echelons; the KW-37 for Broadcast; and the KW-7 for multi-holder tactical operations. There are a number of other equipments used for special applications like multi-channel communications where you may need to secure up to 48 channels simultaneously; but for securing teletypewriter traffic and nothing else, these are currently the big three.

They represent significant advances in need, size, reliability, and flexibility. I failed to mention that the KW-7 will very nearly fit in a standard safe drawer.
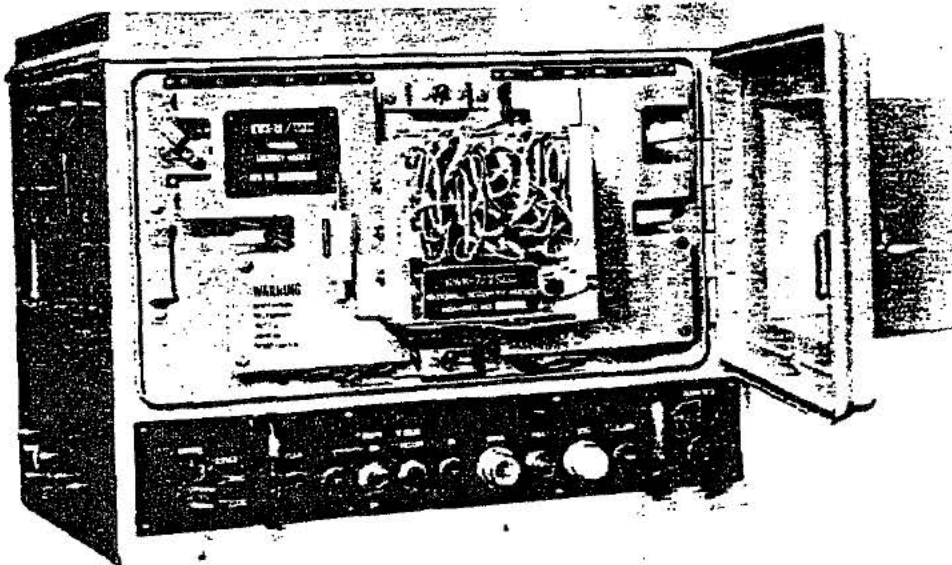
SIXTH LECTURE: Multi-Purpose Equipment

Each of the equipments that I have mentioned to you was designed to take a particular kind of traffic: literal traffic—the letters of the alphabet in the case of the "KL" machines: teletypewriter traffic in the case of the "KW" machines. But as early as World War II, cryptographers and communicators were looking for ways to accommodate a variety of inputs in the same machine—they wanted, for example, a machine which would produce its cipher text in the form of five-letter groups to facilitate transmission where Morse code had to be used, and to have that same machine produce its cipher text in teletypewriter format for use where teletypewriter circuits were available. A little later, as we shall see, they wanted and got equipments containing other options like teletypewriter, and facsimile, and voice encryption all in the same package.

The Signal Corps made the first effort during WW II. It was called the SIGNIN, and was quite a monster. They tried to solve a multitude of problems in one swell flop including the age-old physical security problem we have had with crypto-equipment. They built it in its own special safe and wound up with an equipment about four feet across and weighing Lord knows how much in its solid steel olive drab package. They built their own teletypewriter keyboard instead of hooking into a standard commercial model as had been done previously and since. It would operate either on-or off-line. The machine used rotors, a whole slew of them and, in the teletypewriter mode combined plain text and key in a novel way, all five intelligence bauds of the teletypewriter character being mixed simultaneously with 5 elements of key provided by the machine. This feature caused a brief resurgence of interest in the old monster during the early fifties, once again because of that ubiquitous problem, compromising emanations.

WW II ended before this machine had been perfected for very long, and it never got very heavy use. But the idea for doing a multiplicity of things in one machine was there. The KL-7 and KL-47 systems were coming along, and the utility of having a literal machine able to accept messages for encryption or decryption in teletypewriter punched tape form, and to produce its cipher text in this same form instead of printed on gummed tape had been recognized. Rather than building such features into the machines themselves, which would burden most of the users who had no access to teletypewriter circuits with needless added bulk and cost, a few circuits were built in to permit ancillary teletypewriter equipment to do the work when needed and available. They were called "HL" equipment—the H in the first position stands for ancillary; and L still stands for literal: so an "HL" equipment is one that aids or facilitates but does not actually perform a literal encryption process.

But we had to wait until the mid-50's for the next real multi-purpose equipment to come along. It was designed to meet Navy requirements for the processing of facsimile information or teletypewriter information. It was called the AFSAX-500—the "X" stands for facsimile or "fax" for short: AFSA stands for the Armed Forces Security Agency, which is what NSA was called until late 1953— the change was more than in name only, by the way: our responsibilities became national in scope instead of being limited to the armed forces. Thus, it was that juncture that Departments and Agencies like the Department of State and CIA came under our jurisdiction in cryptographic matters. Anyhow, the AFSAX-500 reflected our growing disillusionment with rotor techniques where high speed processes were needed. In order to encrypt facsimile information at any reasonable speed, it first has to be converted to digital form and then processed at bit rates of anywhere from 1800 bits to 2500 bits per second. Can you imagine rotors going at that speed? Neither could we nor the Navy who really designed the AFSAX-500 under the tutelage of a very famous Navy Captain named Safford. Capt. Safford had played a large part in the invention and development of most of the WW II rotor systems. What was built amounted to an electronic analog of a rotor system—it used up three bays of equipment (a bay is about the size of most of the 4-drawer safes around here.) Since the equipment had to produce lots of key for use in the facsimile mode, there was key to burn for teletype-

writer operations where the speed of the equipment remained limited by the electromechanical properties or the associated TTY equipment—(Truly fast page printing, you realize, had to wait for computers, so that not too much of their valuable time would be lost waiting for some printer to bang out its voluminous rapid-fire products.) Because this extra key was available for TTY use, the machine was built to encrypt about 5 channels of teletypewriter information simultaneously. Then, when no pictures were being sent over the facsimile channel, the communicators could unload their teletypewriter traffic backlog.

Well, the AFSAX-500 worked all right, but not very many of them were ever built: we suspect it was partly because it was *horribly* expensive although the Navy never would say just how much it cost: but there was another reason as well—that is that facsimile requirements have a habit of withering away about the time you have an equipment to serve them. This has been true over the years, and a whole class of systems with "X" in their short titles never repaid the investment that went into their development—which means, hardly anybody bought them or used them.

I want to make just two more points about the AFSAX-500: one is that it continued in use for more than 10 years, but so far as we can tell, it was used nearly exclusively for multi-channel teletypewriter encryption, not for facsimile which had been its real purpose. The other is, that yet another way for keying the equipment—for setting it up—was devised. I have described equipment which is set up from a printed key list that tells you how to put rotors together, arrange, and align them: I have mentioned key cards that use holes and no holes to establish settings in electronic equipment: and I spoke of a plugboard—which is a kind of wiring matrix—that is now being used with the KW-7. The designers of the AFSAX-500 were faced with the problem of setting up a very large number of variables each day—they could have used a very large bank of switches that could be flipped one way or another in accordance with a printed key list. This had been done with the earliest U.S. ciphony equipment—the SIGSALLY—that we'll be talking about in due course. Instead, they chose to use a long segment of one-time tape which was fed into the machine during the setup process and which established the starting configurations for its electronic "rotors". We've toyed with that idea again from time to time but, in most cases better ways have been found. Only one other system used tape segments for its setup. So now we have four different ways to set up our daily variables, and we have barely left the teletypewriter field. It suggests that this business of how to get the variables set up swiftly and accurately constitutes an inherent problem in our business, and this is so. In other courses, you will hear of still different ways being explored.

The next multi-purpose crypto-equipment I want to describe is called the TSEC/KO-6. Strangely enough, in the TSEC nomenclature scheme, that "O" meant "Multi-purpose"; but although a number of subsequent equipments with multiple capabilities were built, the KO-6 is the only one that got assigned an "O". This is because a more generic designator. "G". for *key generator* was decided on, and that's what we used thereafter whether the equipment had a multiple use not.

But the KO-6 was invented before the TSEC nomenclature took effect, and used to be called the AFSAY-806. That "Y" stood for "ciphony" or voice encryption, and that was the primary thing the KO-6 was for. But it could also encrypt either facsimile or—like the AFSAX-500—a number of teletypewriter channels simultaneously. The designers were again faced with the problem of producing a lot of key very rapidly, but were still tied to electromechanical techniques for doing it. What they settled on had at its heart something called a geared timing mechanism (GTM) which would spin six rotor-like notched disks very rapidly and used photo-electric cells to read various notches as they went whipping by. The resultant data, in the form of 1's and 0's again (really light or no light) was combined into a random key stream, and added to digitalized plain text in the usual old binary way. This was a pretty complicated and precision-built device. We put at least one major electronics firm out of business trying to build it for us: but it worked. The last ones were deep-sixed in the latter part of 1966.

A problem looms: how do you put voice into digital form? Let me back-track a little. You have seen that we have means for producing key in binary form in a variety of ways and that, if your plain language is digital, the business of encipherment and decipherment through binary addition

and re-addition is fairly straight forward. But if we don't digitalize speech, how else might we encrypt it? The only alternative means that has gotten much play is to transpose it in various ways—record it and send it out backwards; split it up into little pieces, smaller than syllables, transpose the pieces according to some key, and reconstitute it at the receiving end; or, pull out the various frequencies of the speech and transpose these for transmission. Almost all the commercially available "speech privacy" devices use some such technique as this. But you'll recall that I told you that transposition systems are fraught with security weaknesses; and it has continued to prove true whether you are using a pencil and squared paper or very sophisticated electronics, there's just too much underlying intelligence showing through. But from time to time we try again to do something besides digitalization because it turns out that there would be very important advantages if we could: we could eliminate a battery of expensive and elaborate equipment that we now need to use just to convert the speech to digital form before we begin to encrypt it; and we could cheaply provide ciphony on *narrow-band* communications channels like HF radio and the ordinary telephone. This is now extremely difficult to do because. if you are to describe speech accurately with a series of 1's and 0's, it takes a huge number of these digits for each syllable: this in turn demands a large portion of the radio frequency spectrum, a *broad-band* signal, for transmission. The fewer digits you use to describe speech. the less spectrum you use, and the farther you can transmit it but the less intelligible the speech becomes when you reconvert to a form suitable for the human ear.

At any rate, for security reasons, we had to settle on speech digitalization as part and parcel of any ciphony system. We have three basic ways in which we now do this—vocoding (short for voice coding) which uses relatively few digits to describe speech and is hard to understand unless the vocoder is large and expensive and even then it may leave something to be desired; delta modulation. which uses many digits, gives excellent speech quality, but needs a broad band radio path or special wire-lines like coaxial cables for transmission; and pulse code modulation, which produces similarly high voice quality and has similar transmission constraints.

Since the MC's (Military Characteristics) of the KO–6 called for long-haul (HF) capability, the first of these techniques—vocoding—had to be used. Only 3.200 bits per second to describe the speech—with key stream generated at a comparable rate—were used in contrast to a contemporary system for wide-band (microwave) transmission where the bit rate was on the order of 320,000 bits per second (AFSAY-816).

Because the speech quality was so poor—you could not recognize voices—and because the system was inconvenient to use (push-to-talk procedures and very slow and deliberate speaking; and the need to walk down to or near the cryptocenter to get access to the system) the machine turned out to be less than a roaring success and over the years we were unable to document very heavy usage of it by anybody for voice communications. There did not seem to be much call for facsimile encryption, as I have mentioned, and just before the last KO–6's were retired in 1966. they were used exclusively to encrypt multi-channel teletypewriter traffic.

We're going to come back to the whole subject of speech encryption devices and trace their evolution in some detail. But before we get to that subject, there is one more family of multi-purpose equipments I want to talk about. These are the KG–3/KG–13 series of equipments.

Until around 1960. as I have indicated. each new crypto-equipment was tied to rather specific communications means, and was built to be compatible with input devices like teletypewriters or facsimile equipment with very specific characteristics. Even those multi-purpose devices we have described could work only at a few specific speeds; the KO–6 would work only with the specific vocoder we built to go with it and not with any other speech digitalizer. This specificity of purpose caused the equipments to be inflexible and tended to make them obsolete relatively quickly as new communications techniques and input devices became available. So we did a philosophical about face with the KG–3. We said. why not build a pure and simple key generator divorced from any specific input device or digitalizer: simply an equipment which will put out good random digital key with a large variety of speeds, and a mixing or binary addition component that will accept the encipher and digital signal delivered to it? If somebody wanted to encrypt teletypewriter traffic, or facsimile. or data. or voice, he would provide the equipment that would deliver that information in

binary digital form to the key generator and it would do the rest. And so the KG-3 was born—a straightforward key generator with a randomizer, a power supply, and timing circuits to permit speeds varying from 1 to 100,000 bits per second, and that's about all. And this idea worked fairly well. We had gotten ourselves out of the communications business into which we had become increasingly involved, and back to pure cryptography where we thought we belonged. But there were some difficulties. Because the KG-3 was a single key generator, it could only process traffic in one direction at a time; this meant that to accommodate the full-duplex operations that almost everybody needed, two complete equipments had to be set up at each end of each circuit, and this was a waste. There was no reason why a send and receive key generator could not share the same power supply, thus eliminating one of them, and the same timing circuits, and you really did not need a randomizer in the receiving equipment at all because all the receiving equipment needs to do is to accept the random indicators generated at the distant station; the *send* equipment does the randomizing.

So, the KG-13 was built: it amounts to a pair of KG-3's one used for sending and containing all of the original KG-3 features; the other for receiving and stripped of all the components and functions that the send equipment can supply.

We have now traced the checkered history of multi-purpose equipment and have seen that it took from 1944 or so until 1960 to come up with one that did not really have a single primary purpose in mind with other capabilities included as side benefits. The SIGNIN was primarily for teletype-writer traffic; the AFSAX-500 was for facsimile; and the KO-6 was for voice. The KG-3/13 was for *anything* digital with speeds up to 100 KHz.

SEVENTH LECTURE: Ciphony Equipment and Other Specialized Systems

Ciphony Equipment.—You have already had a preview of some of the problems of voice encryption in the discussion of the KO-6. Since by far the greatest weakness in U.S. COMSEC today stems from the fact that almost all of our voice communications are sent in the clear, the business of finding economical secure ways to secure voice transmissions remains a burning issue and is consuming a good part of our current COMSEC R&D effort.

We have to go back to World War II for a look at our first voice encryption equipment:
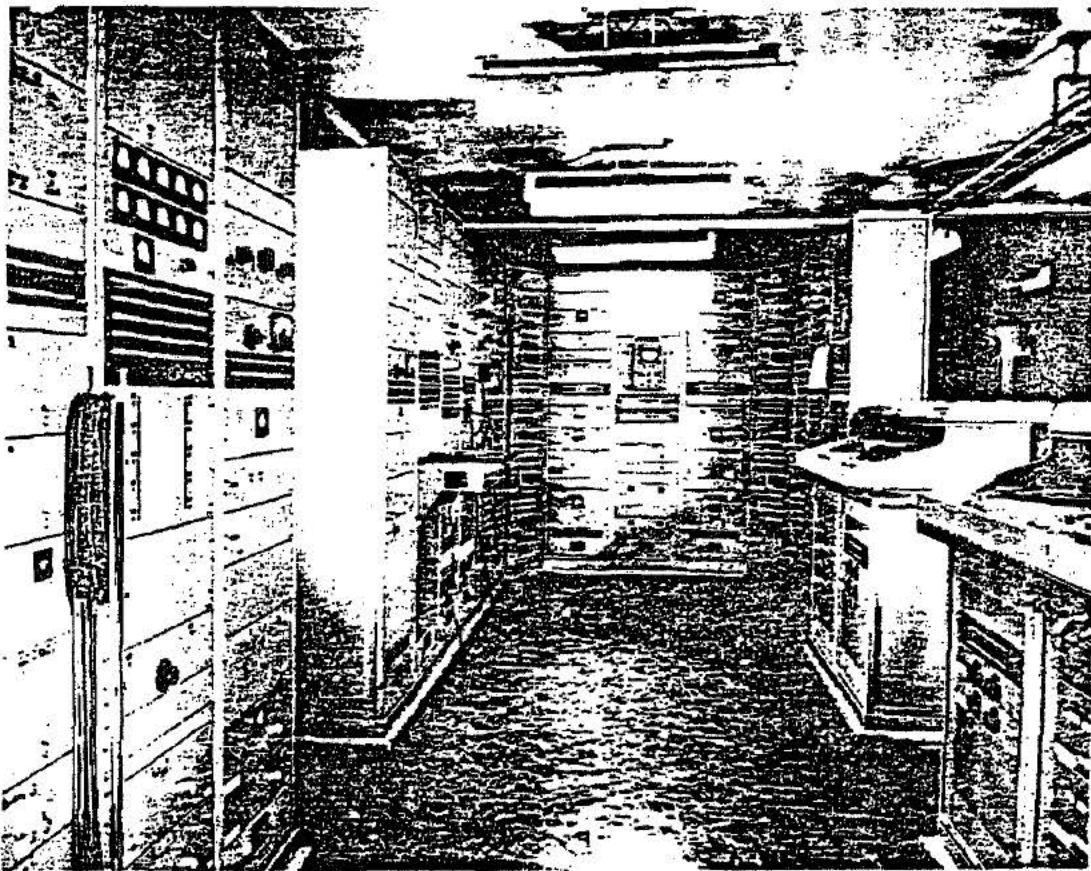
This looks like a whole communications center or laboratory or something; but it's all one cipher machine. It was called SIGSALLY. If you counted the air-conditioners that had to go with it, it weighed something like 55 *tons*. It was used over the transatlantic cable for communication between Washington and London. It used vacuum tubes by the thousands, and had a primitive vocoder. It was hardly the answer to the dream of universal ciphony, and was dismantled soon after the war ended.

The next ciphony system to come along was called the AFSAY-816. It was designed to operate over microwave links—actually, just one link—between the Naval Security Station and Arlington Hall. Since there was plenty of bandwidth to play with (50 KHz), there were no constraints on the number of digits that could be used to convert speech into digital form. The technique used was

called Pulse Code Modulation (PCM): conceptually, it involves sampling the amplitude (size) of an intelligence signal, such as one's voice, at fixed intervals of time determined by a high frequency pulse train, then transmitting the values thus obtained in some sort of binary or baudot code. The following illustration portrays these relationships:

PULSE CODE MODULATION
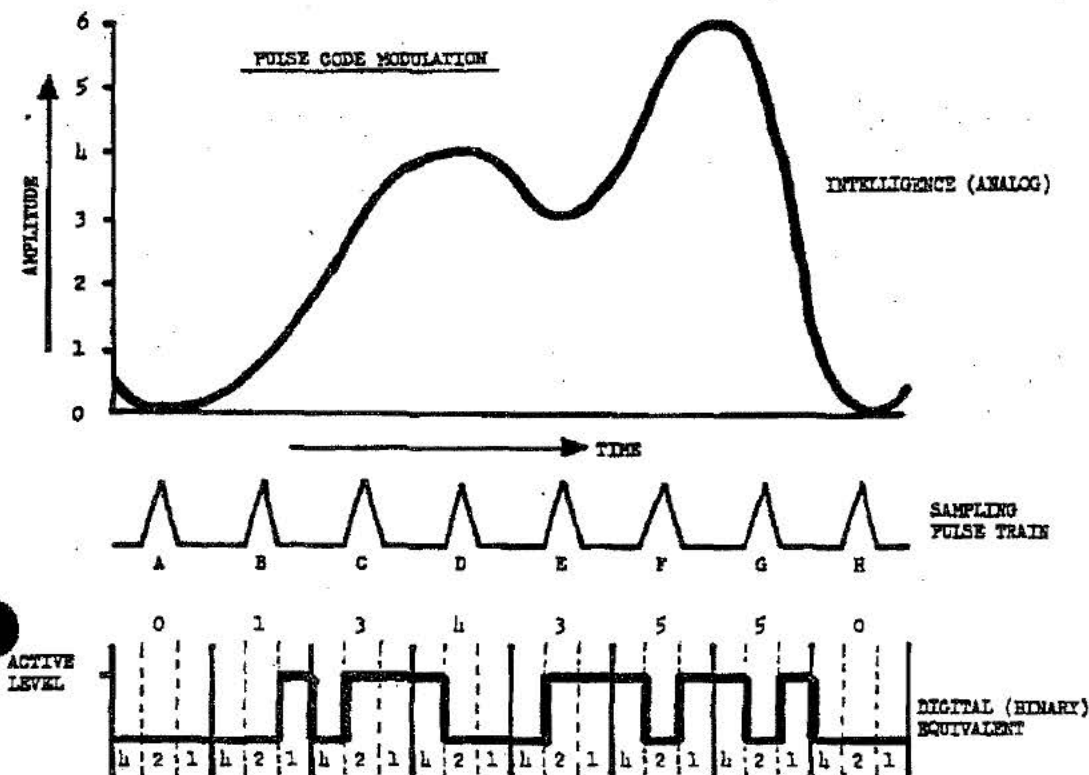
The AFSAY-816 used a primitive vacuum tube key generator with bank after bank of shift registers . . . and, for the first time, we were able to put out more key than we could use. So we used it to provide for encryption of several channels of speech simultaneously. Speech quality was good, reliability was spotty, and security, especially in its last years was marginal since it was in about that time frame that we began to be able to postulate practical high-speed computer techniques as a cryptanalytical tool. We hastened to replace the equipment with one called the KY-11. The KY-11 was the first relatively modern key generator of the breed I described in the KW-26. Instead of using the Fibonacci principle, however, it used something called "cipher text autokey" or "CTAK" for short. I'll tell you something more of the uses to which this principle can be put later.

At any rate, we lived on borrowed time with the AFSAY-816 and on the hope that, because its transmitted signal was fast, complex, and directional, hostile interception and recording would be impracticable.

Don't think for a minute that the same rationale isn't used today for unsecured circuits that happen to use sophisticated transmission techniques. A favorite ploy of the manufacturers of forward tropospheric and ionospheric scatter transmission systems, for example, is to advertise them as inherently secure because of their directivity and because they are beamed over the horizon and theoretically bounce down in only one place. However, because of atmospheric anomalies; it is impossible to predict with certainty what the state of the ionosphere will be at any particular moment. It is because of these anomalies that the reflection of the transmitted signal from the ionosphere is subject to considerable variation and, consequently, subject to interception at an

unintended location. As a matter of fact, there was a "permanently" anomalous situation over parts of Southeast Asia that caused VHF communications to double their expected range.

The general attitude of this Agency is that *no* deliberate transmission is free from the possibility of hostile interception. The thought is that there is really a contradiction in terms of the notion of an uninterceptible transmission: for, if there were such, the *intended* recipient, your own distant receiver, could not pick it up.

Despite all of this, it *is* clear that some transmissions are considerably more difficult and costly to intercept than others and some of them carrying information of low intelligence value may not be worth that cost to the potential hostile interceptor. These factors have a lot to do with the *priorities* we establish for providing cryptosystems to various kinds of communications entities.

But, in the case of voice, which is our subject, it has not been any rationale of non-interceptibility which has slowed us down, it is the set of terrifically difficult technical barriers in the way of getting such equipment in light, cheap, efficient, secure form, either for strategic high-level links, as in the case of all the ciphony equipments I've mentioned so far, or for tactical circuits that we will, in due course, cover.

Still, with the advent of the KY-11, it appeared that we had at least one part of the ciphony problem relatively well in hand: that was for fixed-plant, short-range operations where plenty of bandwidth was available for transmission. These fixed-plant, wide-band equipments—all of them—not only could provide secure good quality voice, but had enough room to permit the encryption of several channels of voice with the same key generator. But just as in the case of teletypewriter security devices, there was a need to move ciphony equipment out of the cryptocenter and nearer to the environment where the actual user could have more ready access. In the case of the teletypewriter encryption systems, you will recall, the move was into the communications center where all the ancillary devices and communications terminal equipment and punched message tapes and message forms were readily available. In the case of ciphony, the real user was the individual who picks up the handset and talks—not some professional cryptographer or communicator—but people like you and me and generals and admirals and presidents. So the next need we faced was to provide an equipment which could be remote from both cryptocenter and communications center, and used right in the offices where the actual business of government and strategic military affairs is conducted. This called for machinery that was smaller and packaged differently than any of the ciphony equipment we have talked about thus far. SIGSALLY you remember, weighed 55 tons: the next system weighed a lot less but still needed 6 bays of equipment. The KY-11 was smaller still, amounting to a couple of racks of equipment configured for communications center use. None of them were at all suitable for installation in somebody's office.

The resultant product was called the TSEC/KY-1. The most striking feature it had, in contrast to its predecessor ciphony devices, was that it was neatly packaged in a single cabinet about two-thirds as tall and somewhat fatter than an ordinary safe. Because it was built not to be in a crypto-center or a classified communications center where there are guards and controls on access to prevent theft of equipment and their supporting materials, this KY-1 cabinet was in fact a three-combination safe that contained the whole key generator, the power supply, the digitalizing voice preparation components—everything except the handset which sits on top.

So, for the first time since World War II with the SIGNIN, we found ourselves building physical protective measures into the equipment itself. The safe is not a particularly good one—hardly any are—but it is adequate to prevent really easy access to the classified components and keying data contained inside. Microwave links or special wire lines were used to transmit its 50 KHz cipher text. The principle was CTAK again: and it had the capacity to link up to 50 holders through some kind of switchboard in a common key. The first network was used here in Washington and served key officials of government—the President, the Secretary of Defense, the Secretary of State, the Director, Central Intelligence Agency, and some others. We soon found that the equipment needed to be installed not only in key government offices, but in the private residences of key officials as well, so that they could consult securely in times of crisis night or day. I think the first such residence was

President Eisenhower's Gettysburg address: later such equipments were used in the homes of a number of other officials.

The KY-1 had some limitations, as almost all first tries at a new requirement seem to: it was essentially a push-to-talk system which annoys most users and makes it impossible to interrupt conversations. Eventually, the cryptanalysts discovered some new possible attacks that lowered our confidence in its security and so the KY-1 was retired in early 1967. This KY-3 is the follow-on equipment to the KY-1. It provides a duplex (no push-to-talk) capability and some security and operational refinements.
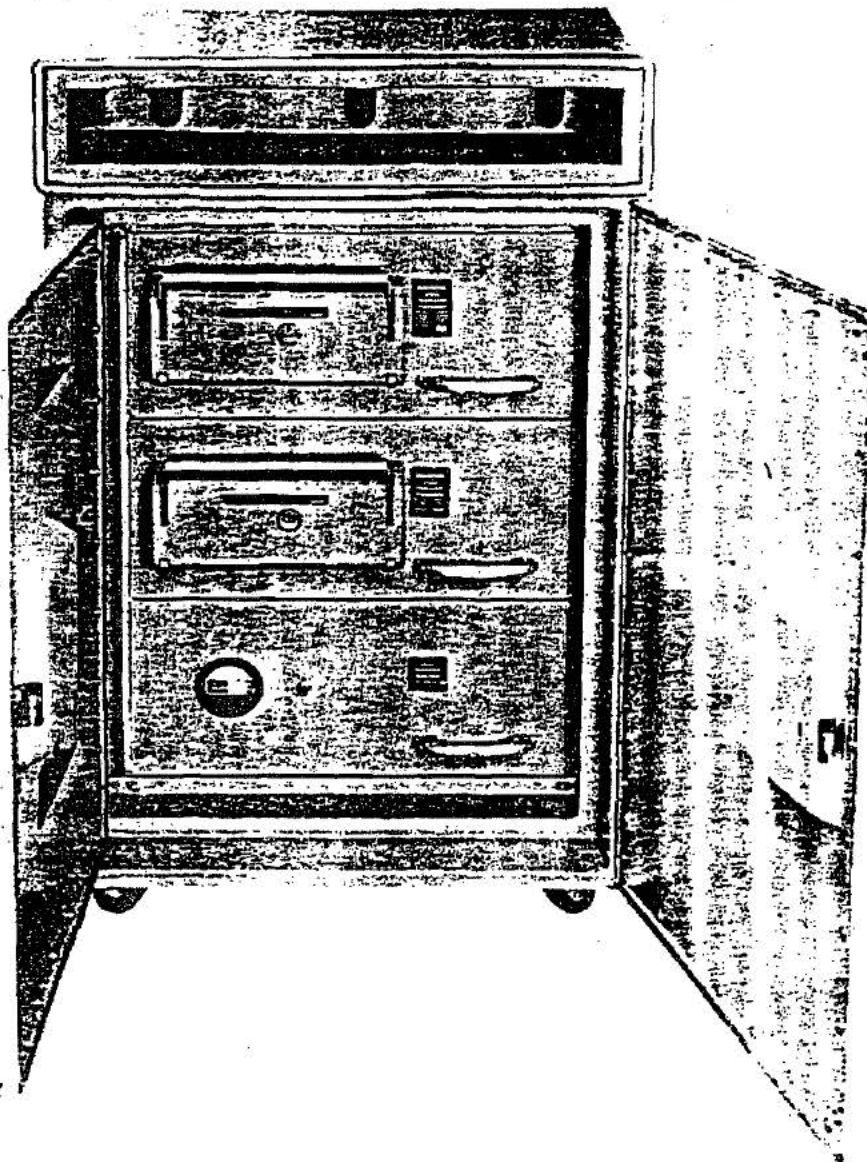
This is perhaps as good as a place as any to go off on another of the tangents that seem to characterize these lectures. As we have been following the evolution of U.S. cryptography, I have talked

quite casually of new equipments coming into our inventory and old ones fading away. In retrospect, the demise of the obsolescent, inefficient, and insecure systems seems natural, easy, inevitable, and relatively painless. But the fact of the matter is that it is usually quite difficult to get the users to relinquish any equipment once it is solidly entrenched in their inventories—especially if it works well, as in the case of the KY-1; but even if it doesn't, as in the case of the KW-9. The reluctance to junk old systems stems from a number of causes, I think. First of all, they represent a large investment; secondly, the users have developed a supporting logistic base for the systems, have trained personnel to operate and maintain it—they've *used* it. Finally, the introduction of a new system is a slow and difficult business requiring new budgetary and procurement action, new training, the establishment of a new logistics base, and—increasingly these days—a costly installation job to match the new system to the facility and communications system in which it is to be used. Because of these problems, our "equipment retirement program" is a halting one, and only when there are very grave *security* shortcomings can we actually *demand* that a system be retired on some specific date. Well, back to ciphony systems.

With all these developments, we are still talking about equipment that weighs several hundred pounds, is quite expensive, and which is limited to specialized and costly communications links. Except in the case of the KO-6, these links are relatively short range.

So, at the same time these wide-band fixed-plant equipments are being developed, we were working on something better than the KO-6 to satisfy long-range, narrow-band communications requirements, something that could, hopefully, be used on ordinary telephone lines or on HF radio circuits overseas. (Ma Bell's telephone system, you understand, has a bandwidth of only 3 KHz—and still has a few quick and dirty WW II links in the mid-west with only a 1500 hertz bandwidth. This situation, as I have said, sharply limits the number of digits we can use to describe speech to be encrypted on such circuits with a consequent loss of quality of intelligibility.)

The equipment which evolved is called the KY-9.
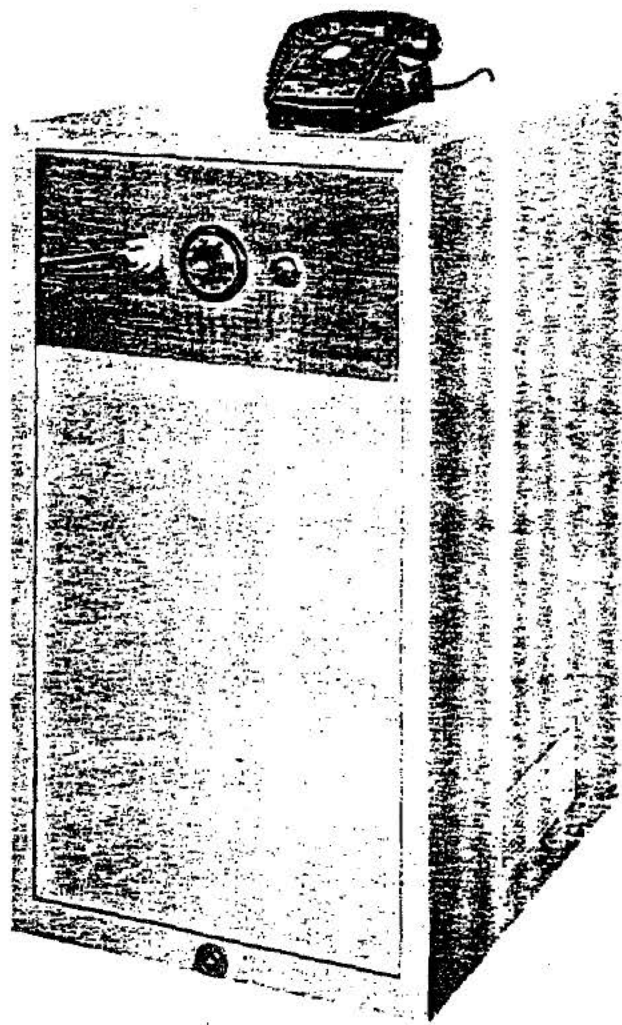
The KY-9 used a vocoder as did its narrow-band predecessors, but a more sophisticated one than had been developed thus far. It was the first of the vocoders to use transistors instead of vacuum tubes, so that the equipment could be reduced to a single cabinet. But transistors were in their infancy; and the ones that went into the KY-9 were hand-made and expensive. Again the equipment was packaged into a safe so that it could be located in an office-type environment. Well, we were getting there: we could use an ordinary telephone line with the KY-9, but the speech still sounds artificial and strained because of that vocoder, and . . . you . . . must . . . speak . . . very . . . slowly . . . and . . . distinctly and you must still push to talk. And besides all that, this bear initially cost on the order of $40,000 per terminal which put it strictly in the luxury category. About 260 KY-9's are in use for high-level, long-haul voice security communications. The majority of the KY-9 subscribers are now being provided this secure capability through use of the Automatic Secure Voice Communications (AUTOSEVOCOM) system; however, it is anticipated that the equipment will ·main in use at least through FY-74. Beyond FY-74, the equipment may be declared excess and ·stored for contingency purposes.

The best and newest long-haul voice equipment uses none other than our multi-purpose friend, the KG-13. Nobody came along with a nice vocoding speech digitalizer to hook into this key generator, and there's really not much call to process speech this way unless you're going to encrypt it, so we wound up—*again*—having to build some of the ancillary equipment ourselves. This equipment is called the HY-2—remember, the H stands for *ancillary*, the Y for *speech encryption*. So the combination referred to as the KG-13/HY-2 is the system we are now counting on to serve the long-haul voice requirement.
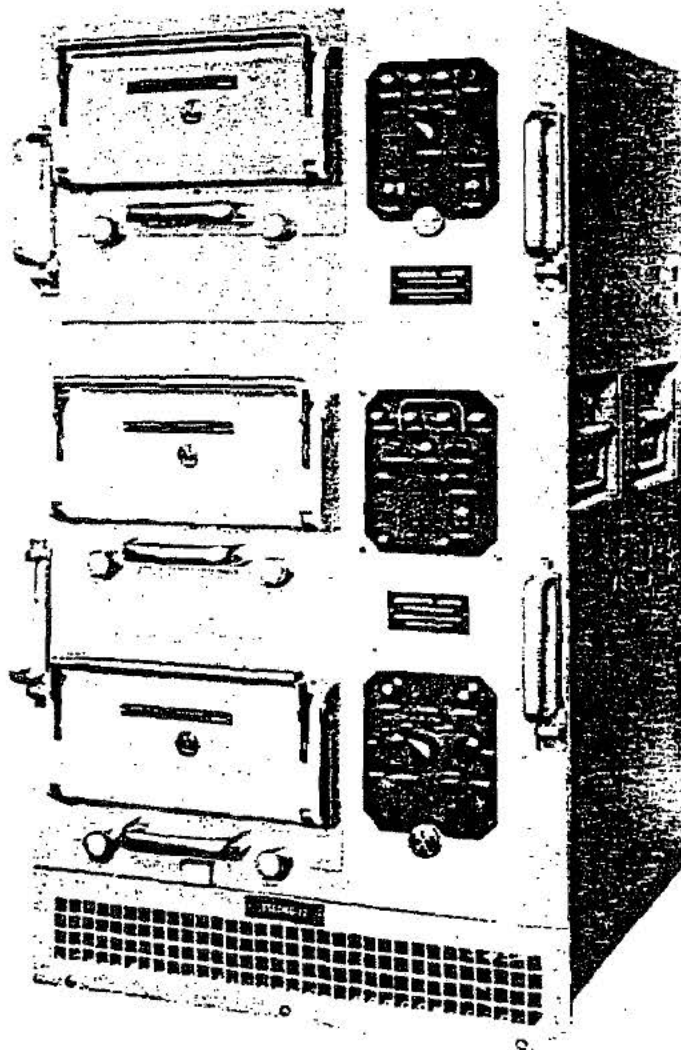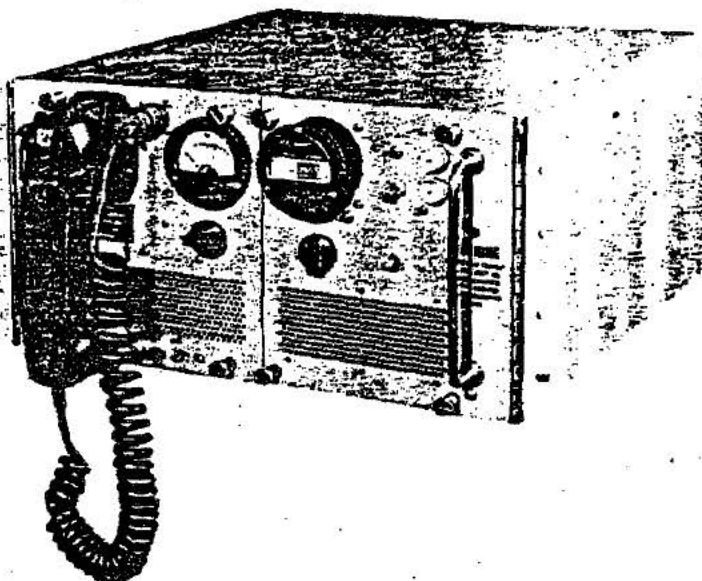
Again. a vocoder was used. and this sounds the best yet, although it still can't match the voice quality that wide-band systems have. This package is not in a safe, and is not suitable for office installation. but it seems to satisfy most of the other long-haul requirements well and does so fairly cheaply for the first time.

Before we talk about tactical voice security equipment, there is a subject related to the big fixed-plant voice equipments we ought to talk about. That's the subject of "approved" circuits. Way back with the KO-6. we were having difficulty getting officials to leave their offices and walk to a crypto-center to use a secure phone. The solution lay in carrying the system or at least the telephone hand-set (which is all he really needs or cares about) to him. This involved running a wire line from an office to the cryptocenter or secure communications center. The difficulty with this solution is two-fold: in the first place there was and is a long-standing Executive Order of the President governing the way classified information may be handled, transmitted, and stored: and in the case of TOP SECRET information, this order forbids electrical transmission *except in encrypted form*. Of course, the informations in the clear. not encrypted. until it reaches the cryptomachine, and this meant that any time one placed that handset remote from the machine. the user. by "law" had to be re-stricted to conversations no higher than SECRET. This is difficult to legislate and control, and reduces the usefulness of the whole system. The second difficulty in this situation stems from the security reasoning lying behind that Executive Order. The reasoning was, and is, that it is extreme-ly difficult to assure that no one will tap any subscriber line such as this, if it is not confined to a very carefully controlled area like a cryptocenter or classified communications center. It means that if you are to use these subscriber lines in some government installation. the whole building or com-plex of buildings must be extremely well guarded, access carefully controlled, or personnel cleared or escorted all the time. Controls such as we have here are simply not feasible in a facility such as the Pentagon or on a typical military post: yet it is in just such environments that these protected wire-lines may be needed.

Some special rules govern communications used to support SIGINT operations, and these rules have been interpreted to permit TOP SECRET traffic such as we use on the grey phone system here—provided certain physical and electronic safeguards are enforced. The JCS applied the same sort of criteria in staffing an action which permitted TOP SECRET information to be passed in the clear over wire lines when certain rigid criteria are met. Until this action went through. we were un-able to make full use of the ciphony capability we now have in systems such as the KG-13/HY-2,

and subscribers were held to SECRET unless they were essentially co-located with the crypto-equipment itself.

Tactical Ciphony.—MC's for tactical ciphony equipment—be they broad-band, narrow-band, or somewhere in between—have existed since before this Agency was created. But the difficulties were terrific. To have tactical usage on field telephones and radio telephones and military vehicles and, especially, in aircraft, the equipment had to be truly light, small, and rugged; and had to be compatible with a large variety of tactical communications systems most of which are not compatible among themselves. In the case of aircraft requirements, there's an old saying that the Air Force will reject any system unless it has no weight, occupies no space, is free, and adds lift to aircraft. We were about ready to believe this in the late fifties when we had gotten a tactical ciphony device, the KY-8, down to about 2/3 of a cubic foot, and it was still not accepted, mainly because it took up too much room. The ironic part of this sad story is that the cryptologic portion of the hardware uses only a modest amount of space: its power supplies and the digitalizers for speech that use up the room. The Air Force did give that small equipment, the KY-8, a good try in high performance aircraft like F-100's: it worked fairly well, but sometimes reduced the effective range of their radios about 5%, a degradation of their basic communications capability they simply could not afford. Besides, the problem of lack of space proved very real and they had to rip out one of their fire-control radars to make room for the test equipment.

Then the Army decided it could use the KY-8, mounting it in jeeps and other wheeled vehicles where space was not so critical as in aircraft. We had attempted to make a ground tactical ciphony equipment for Army, called the KY-4, but it didn't pan out; and the Army had independently tried to develop a tactical voice device that was equally unsuccessful. So Army bought a batch of KY-8's and they and the Marines became the principal users, even though it was really originally designed for aircraft.

There's another point about the KY-8. I've made it sound as if over-choosy users have been the only cause for its slowness in coming and limited use. That's not quite the case. There were some security problems—the compromising emanation business again—that slowed down our production for some time: we finally got going full blast on this equipment by cancelling out most of the delaying features in the contract associated with the radiation problem, accepting this possible security weakness as a calculated risk, and placing some restrictions on where the equipment could be used to minimize that risk.

Today we have a family of compatible, tactical, speech security equipments known as NESTOR—the KY-8/28/38. The KY-8 is used in vehicular and afloat applications; the KY-28 is the airborne version; and the KY-38 is the portable or man-pack model. There are currently about 27,000 NESTOR equipments in the U.S. inventory. No further procurement of NESTOR equipments is planned because the VINSON equipment is intended to satisfy future requirements for wide-band tactical voice security.
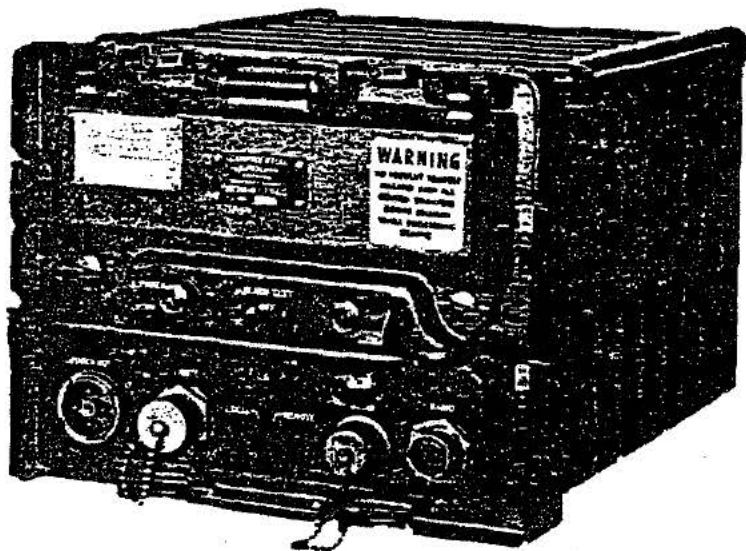
Cipher Text Auto-Key.—We have seen that, in seeking means to produce one or many streams of random key to combine with digitalized plaintext information, we have settled on several mathematical principles such as Koken, Fibonacci and CTAK and that one of the technical problems associated with these techniques is the matter of keeping the local and remote key generators in step. I have said that another problem is the supply, with each new message, of some random information to the distant station, in the form of an indicator, to provide unique settings within the day's key for each new transmission. A principal means for doing this with the electronic systems has been the use of a "randomizer" that sends out a burst of random and unpredictable digits at the start of each message. This presents two difficulties: the first is that the loss or garbling of any one of these digits in transmission—and the stream may be up to *260* bits long—will cause the distant machine to be set up incorrectly, and decipherment will not be possible. In some systems, this difficulty is partially overcome by repeating each digit a number of times—the indicators are redundant and the receiver can select the correct digit by using that majority vote technique we discussed with the KW-37 broadcast system. But this method is not altogether satisfactory—it complicates the hardware for one thing. Another difficulty, with or without the use of a randomizer to effect initial message setups, is this business of keeping the machines synchronized after actual encryption is in process. In the case of equipments like the KW-26 and the KW-37, this is done by clock systems that send out periodic timing pulses—but again, the hardware involved may be rather elaborate. In any multiple holder system that does not have "catch-up" features in the receivers, i.e., with *anything* but a KW-37, the difficulty of getting everybody started at once is serious.

If the designers could find a way to use the cipher text itself instead of a randomizer as the source of new random information with each transmission, and could also use that cipher text as a basis for timing, the equipment would be simplified. The result was the development of *cipher-text auto key* systems. The cipher text was delivered to the binary adders of the receiving equipment, there recombined with key to effect decipherment in the usual way, but at the same time, it was fed into a set of shift registers which formed part of the key generator itself and was used there to form the key to be used in deciphering subsequent incoming cipher information.

CIPHER TEXT AUTO KEY
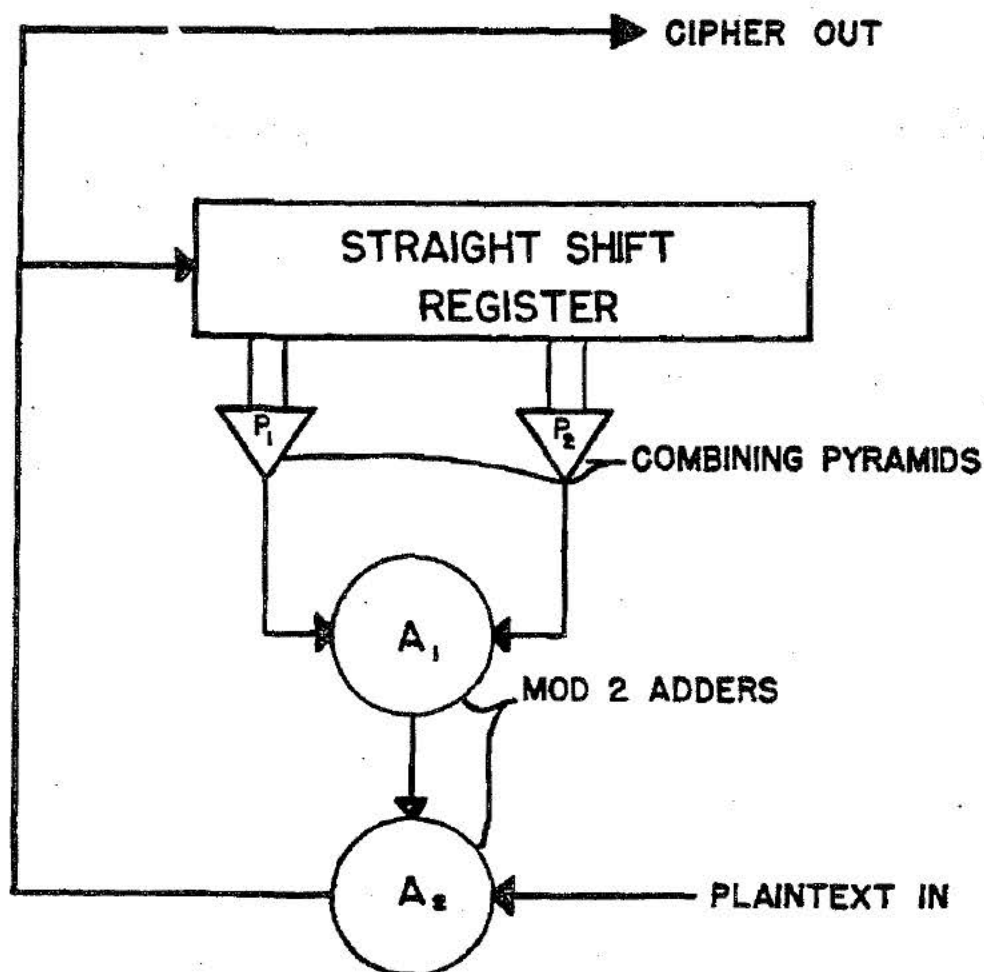
At the same time, this solved the problem of synchrony because, provided that the proper cipher text was received, the receiving equipment could derive proper key, with the correct timing, from that cipher text itself. There remained one major problem. We have said that in an ordinary key generator, the garble of a character in transmission will cause only one (actually two) characters to garble in the deciphered plain text. But as you'll note in the diagram we have had to *fill* a shift register with cipher text in the auto-key system; a single garble in this case spoils the key until the garble has shifted its way through the whole register—typically about 15 to 37 characters. This means that a single garble in transmission will cause up to *38* digits to be garbled in the deciphered text. This means that if this technique is used with something like teletypewriter traffic, the transmission path must be very reliable; otherwise there will be too many long stretches of gibberish in the received messages which the communicators can't tolerate—in fact, one such teletypewriter encryption equipment failed its user tests exclusively for this reason. But if the underlying plain text is something like digitalized speech, where thousands or 10's of thousands of digits go into each

syllable, the loss of this handful of digits is trivial: the effect is so brief a slur in the deciphered speech as to be inaudible. The first system using the auto-key technique was the KY-11 as I mentioned earlier. A half-dozen other machines, mostly ciphony equipments also use this principle.

From the operational point of view, the effect of a system such as this is that any receiver can pick up a transmission in mid-stream just as KW-37 receivers can, but without the elaborate clocks and high-speed catch-up mechanisms. With auto-key, the receiver merely waits until it has received enough cipher characters to fill its shift register, and then begins decipherment.

We have now covered the major equipments and principles in use today. The big systems are:

For Literal Traffic:	The KL-7/47
For Teletypewriter Traffic:	The KW-26, KW-37, KW-7
For Ciphony:	The KY-3, KY-8, KY-9 (KG-13/HY-2
For Multi-purpose:	The KG-3/KG-13

All the principles in the current major electronic key generators involve binary addition of random key streams to digitalized plain language. The big-name principles again are *Fibonacci*, *Koken* (There is also something called *Kokenacci*, combining the features of both) and *cipher-text auto key*.

We have also talked of a number of electro-mechanical equipments that are dead or dying: one-time tape systems, and the KO-6 with its geared timing mechanism being most representative.

The variety of systems which have evolved has stemmed from needs for more efficiency, speed, security and the like: but, more fundamentally, from (1) the need to encrypt different kinds of information—literal traffic, TTY, data, facsimile, TV, and voice, (2) the need to suit encryption systems to a variety of communications means—wire lines, narrow-band and broad-band radio circuits, single-channel and multiplex communications, tactical and fixed-plant communications facilities; and (3) the need to suit these systems to a variety of physical environments.

Specialized Systems.—There are two other types of systems now in the inventory beyond those I have described that I want to touch on briefly. I have left them till last because they are among the most specialized and have as yet seen relatively little use in comparison with the big systems we have talked about. The first of these is the KG-24, designed for the encryption of TV signals—civision we call it. With the requirement for encrypting TV signals, we found ourselves faced with the problem of generating key at extremely high speeds, even by computer standards. So far, the fastest system I have described to you was the old AFSAY-816 with a bit-rate of 320 KHz—but this took six bays of equipment and had security, operational, and maintenance problems almost from the outset. Among the modern systems, the KG-3/13, with bit rates up to 100 kilobits was the fastest. But, as you know, with your home TV set, you tune to megahertz instead of kilohertz and it takes millions of bits each second to describe and transmit these TV signals. The KG-24 does it, and in one fairly large cabinet. During the development, radiation reared its ugly head again, and much of the cost and delay in getting this equipment could be attributed to the efforts that went into suppression of these compromising emanations. When I cover the radiation problem I'll show why there are special difficulties when very high speed signals are generated and show you the solution that was chosen in the particular case of the KG-24. The KG-24 uses the Fibonacci principle and works alright. But there are only 6 (V-1) and 7 (V-2) models in existence, and further procurement is not planned. The main thing wrong with it is simply that it costs much too much.

The second type of modern specialized system I want to talk about is the family of equipment designed specifically to go into space vehicles. There were some obvious and some not-so-obvious difficulties that had to be met in the design of these equipments. One obvious problem was to make them small enough, and this requirement gave a big push to our general work in the micro-miniaturization of hardware. The second problem was also inherent in space technology—that was the need for extreme reliability. For unmanned surveillance satellites, if the system fails, you can't call a maintenance man. So we were faced with more rigid specifications and quality controls than we

had ever seen before. The third problem has to do with the extraordinary complexity of satellite systems as a whole. We have found it next to impossible to provide decent crypto-equipment for our customers without a very full understanding of the whole communications and operations complex in which they are to operate. With our limited manpower, this has proven difficult enough to do with modern conventional communications systems and switching complexes on the ground but, for the space requirements, we had to educate our people to speak and understand the language of this new technology; and we have a little group who live and breathe this problem to the exclusion of nearly everything else.

And finally, we had to throw a lot of our basic *methodology* out the window. Every machine I have talked to you about so far, without exception, is built to have some of its variables changed at least once each day, and some of them more often. Everyone of them is classified and *accountable*: can you imagine how a crypto-custodian, charged with the specific responsibility of vouching for the whereabouts of a classified machine or classified key felt upon watching one of his precious items go rocketing off into space? Of course, we decided that we ought to "drop" accountability at the time of loss, although "lift" accountability might have been a more appropriate term. In any event, here's one of these key generators we use in space:
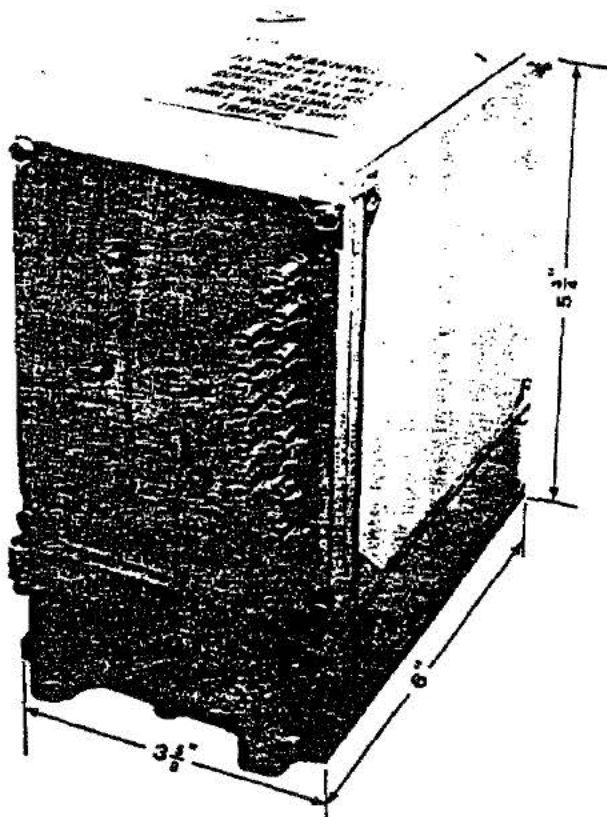
What we built into it was a principle that would put out a key that would not repeat itself for a very long period of time—weeks or months or years, whatever was required. Actually, with many of these new key generators, the matter of assuring a very long unrepeated sequence or, as we call it, a *long cycle*, is not so difficult. Even something as the KO-6 with its geared timing mechanism and just six metal disks would run full tilt for something like 33 years before the disks would reach

their original alignment again, and the daily change of its key was incorporated mainly to limit the scope of any loss that might occur—that business of supersession and compartmentation again. So this little jewel is a unique one-time key generator, good for the life of its parent satellite. That random initial setup of its key generator is wired right into it at the start instead of being controlled by a key card or a set of switches. What we use is a special *plug*, manufactured right here, that sets up unique connections within the generator and establishes the basis for the generation of one long unique key. So far, these things are working well—one technical security problem has been encountered. Radiation again! I hinted in talking about the KG–24 that very high bit rates create certain radiation problems; it turns out that the location of components that process intelligence very close to *transmitting* circuitry also causes problems and, in a satellite, you simply can't get them very far apart.

We have several such systems now. We don't talk about them very much because the whole question of surveillance satellites is a very sensitive one and, of course, that's what these are used for.

Before moving on, there are a few more things you ought to know about the nomenclature system and the equipment development cycle we have touched on from time to time already. The first point is that the TSEC nomenclature we have is *not* assigned to an equipment until it has been worked on by R&D for some time and they have done feasibility studies and have, perhaps, hand-made all or portions of it to figure out the circuitry or mechanical linkages to see if the thing will work. These very early versions are called "bread-board" models, and are likely to bear little or no resemblance to the final product. R&D assigns cover names to these projects in order to identify them conveniently—the only clue to the nature of the beast involved is contained in the first letter of what ever name they assign. The letters generally correspond to the equipment-type designator in the TSEC scheme—with "W" standing for TTY, "Y" for ciphony, etc. So, in the early R&D stage, "YACKMAN" stood for a voice equipment; "WALLER" for a TTY equipment, "GATLING" for a generator, etc.

When it looks like a development is going to come to fruition, TSEC nomenclature is assigned, and *suffixes* are added to the basic designators to indicate the stage reached in each model: these can involve experimental models (designated X), development models (designated D), test models (T), pre-production models (P), and finally, with the first full scale production model, no suffix at all.

So there could have been versions of the KW–26 successively called: W–; KW–26–X; KW–26–D; KW–26–T; KW–26–P, and the first operational equipment called merely KW–26. But, in fact, when some of the early models come out well enough, some of these stages may be skipped; in fact, most of them were with the KW–26, and it has been increasingly the trend to skip as many as possible to save time and money.

But this tortuous path of nomenclating does not end, even here. *After* the equipment gets into production, more often than not, some modifications need to be made to it and, when this occurs, we need some means of differentiating them, mainly for maintenance and logistical reasons, and the suffixes A, B, C, etc., are assigned. So, in fact, we now have four operational versions of the KW–26: the KW–26–A, the KW–26–B, KW–26–C, and KW–26–D.

The following two tables show our current system for assigning nomenclature to both COMSEC keying material and COMSEC equipment:

TABLE I

COMSEC KEYING MATERIAL

Release	Functional Relationship	Purpose	Type Aid
US — Indicates item is NOFORN	C — NUCLEAR Command & Control	A — Operational	A — Authenticator
A — Indicates item is authorized for release to specified allies	K — Cryptographic	M — Maintenance/Test	C — Code
	H — Ancillary	S — Sample	F — Cryptographic Program
	M — Manufactoring	T — Training	G — General Publication
	N — Noncryptographic	X — Exercise	I — Recognition/Identification
	S — Special purpose	B — Compatible Multiple Keying Variable	J — Indicator List
		V — Developmental	K — Key List
			L — Miscellaneous
			M — Maintenance Manual
			N — Computer Keying Material
			O — Operating Manual
			P — One-Time Pad
			R — Rotor
			S — Sealed Systems
			T — One-Time Tape
			W — Crib
			X — Fan Fold
			Y — Key Card
			Z — Permuting Plug
			B — Diagnostic Test Program
			D — Unassigned
			E — Unassigned
			H — Unassigned
			Q — Unassigned
			U — Unassigned
			V — Unassigned

TABLE II

COMSEC EQUIPMENT

I Function	II Type	III Assemblies	IV How to Compare
C — COMSEC Equipment System	G — Key Generation	A — Advancing	1. The nomenclature designator "TSEC" followed by a slant (/) and a diagraph formed with letters selected from columns I & II indicates an equipment or equipment system i.e., TSEC/KG, TSEC/CY.
K — Cryptographic	I — Data Transmission	B — Base on Cabinet	
H — Ancillary	L — Literal Conversion	C — Combining	
M — Manufactoring	N — Signal Conversion	D — Drawer, Panel	
N — Noncryptographic	O — Multi-Purpose	E — Strip, Chassis	
S — Special Purpose	P — Materials Production	F — Frame, Rack	
	S — Special Purpose	G — Key Generator	2. The nomenclature designator "TSEC" followed by a slant (/) and a trigraph formed with letters selected from columns I, II & III indicates a cryptographic component i.e., KGP is a power supply for a cryptographic key generator.
	T — Testing, Checking	H — Key Board	
	U — Television	I — Translator, Reader	
	W — Teletypewriter	J — Speech Processing	
	X — Facsimile	K — Keying	
	Y — Speech	L — Repeater	
		M — Memory, Storage	
		O — Observation	
		P — Power Supply	
		R — Receiver	
		S — Synchronizing	
		T — Transmitter	
		U — Printer	
		V — Removable COMSEC Component	
		W — Logic Programmer Programming	
		X — Special Purpose	

Element Designators
  E — Plus an alphabetical trigraph
Sub-Assemblies
 Z — Plus an alphabetical trigraph

EIGHTH LECTURE: Flops

The next topic we will cover is that of "Flops". In almost all of the basic types or categories of hardware we have talked about such as the literal equipments, TTY equipments, voice equipments, etc., we've created at least one essentially finished product that failed when it met the last hurdle before full-scale production—the Service or "user" tests. Of course, additionally we have made literally dozens of "paper and pencil" systems and simple manual encryption aids (which we call "devices" as distinguished from equipments) that flunked the course for one reason or another.

We're going to talk about some of the more representative of our failures and try to look at some of the causes of those failures with the hope that you profit from the mistakes involved and not be led down the same garden paths as you become embroiled in future developments.

The first flop I want to talk about—rest its soul—was called the KL-17. By 1948, long before this Agency had been formed, the Signal Corps was seeking a small, light, literal cipher machine that would have good security, would require no electrical power, and would operate substantially faster than the one major all-mechanical machine that had been used throughout World War II—the famous Hagelin machine, called the M-209 shown below:
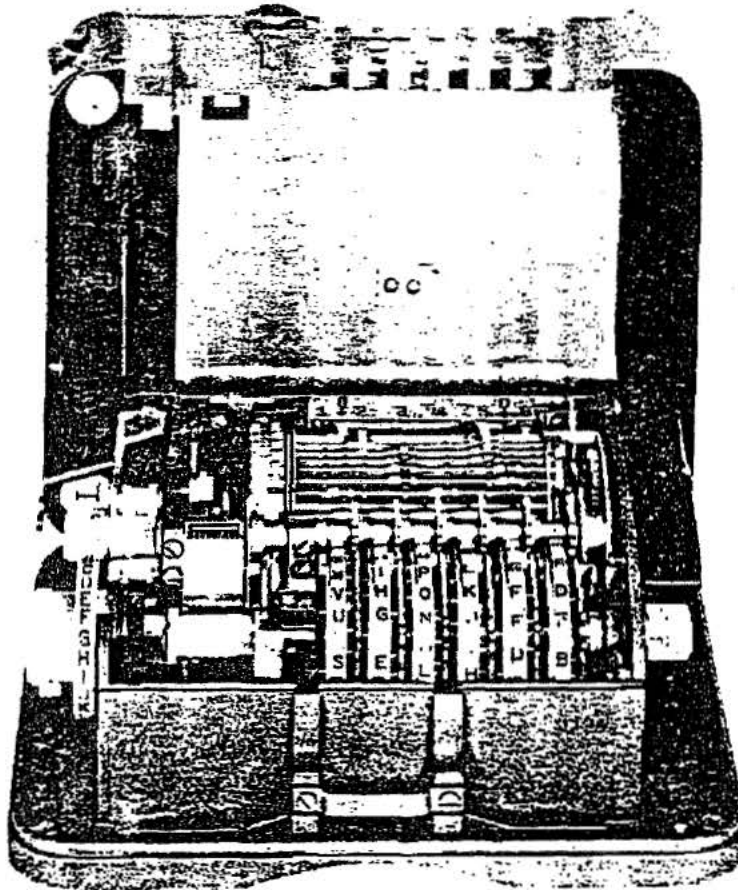
Some of our allies, like the South Vietnamese, still use this equipment; electrical variations of it are common in a number of European, Middle Eastern, and Latin American countries. Used

orrectly it is relatively secure, but in its all-mechanical form it is extremely slow; and we once calcu-
lated that operators had something like 64 separate opportunities to make errors in the course of
setting it up. So something to replace and improve on this equipment was being sought.

So one of ASA's inventive minds—a man named Albert Small—had an idea; why not use a
wired rotor principle but, since the equipment had to operate without electric power, use *air* instead.
And a primitive model was made; but, as you might expect, it had a host of mechanical difficulties
because such a concept demands some rather refined plumbing; besides, the cryptoprinciple turned
out to have weaknesses, so the first version was abandoned. This early equipment was irreverently
referred to as the "BLOWHARD". But Mr. Small was tenacious: he revised his cryptoprinciple,
enlarged the equipment somewhat, and again put forth proposals for an air-driven system. By this
time, NSA, or rather its immediate predecessor, AFSA, was in business. This second version also
failed the cryptanalytic tests and was abandoned. It was referred to as the "DIE-HARD". But this
Agency agreed to pursue such a system in earnest; increased the number of pneumatic rotors,
conceived a very strong cryptoprinciple for it and, working mainly with Corning Glass, developed
high-precision pneumatic rotors that would really work. The technical difficulties were terrific, but
the engineers overcame or nearly overcame all of them. But it took time, more than five years, be-
fore we had a modest batch of KL-17's for the Services to test. The Services, principally the Army,
had estimated that they would need about 20,000 of these machines, if they proved satisfactory and
not too costly; and this was the incentive for the considerable R&D investment we made. We called
it the "RESURRECTION." So, in 1957 we offered this:
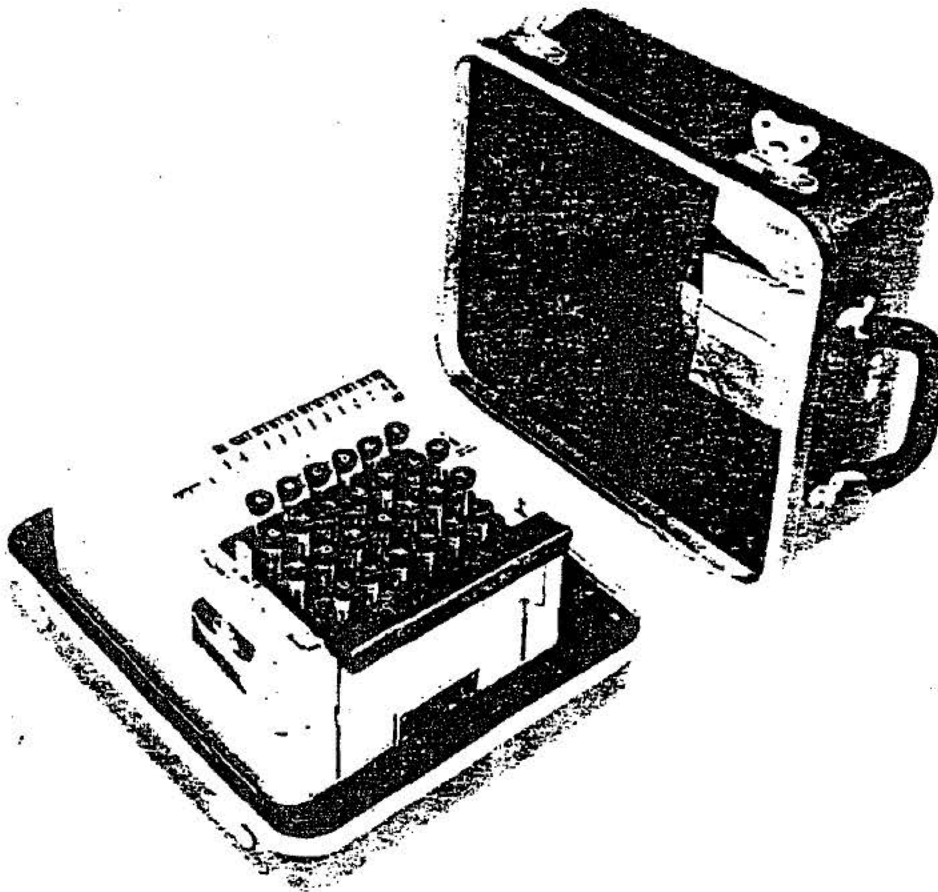
Not bad, huh? Light (12 pounds); compact (.75 cu ft); a good deal faster and a good deal more secure than the M-209; a keyboard instead of wheel; a few minutes instead of about a half-hour to set it up for the day; and for the first (and next to last) time, a means for changing the way the machine itself works—a special variability—in the event a copy is lost. And finally, except for those rotors, almost all of its parts could be stamped out rather than machined, with the result that if it were bought in quantity, it would be inexpensive—something like $500 each; about a third the cost of anything remotely comparable to what we had to offer. So what happened?

The first thing that happened was *time*. About ten years had passed between the expression of a requirement and the production of something that the cryptographers were willing to offer. Notions of warfare had changed drastically. It would be nuclear holocaust or nothing. "Conventional" or even "unconventional" warfare was not likely. From the communications and communications security view points, strategic, high-capacity, electronic systems supporting nuclear strategic striking forces were the things that really mattered, and the notion of ground troops dispersed to an extent where they had no access to power and communications facilities that would accommodate electrically driven cryptomachines was discredited.

None the less, the Army, the big potential customer, dutifully tested the equipment when they finally got it. They used the standard test procedure of measuring the performance of the equipment against an existing alternative system, in this case, the M-209—and found it superior in virtually every way. The equipment came out, technically, with fewer deficiencies cited in the test report than *any* other equipment this Agency had thus far submitted for test. The kinds of deficiencies were mainly in environmental situations which had not been visualized when it was built—e.g., the pneumatic system got unreliable when they took it up past something like 15,000 feet where the air is thin; and operators had difficulty with the keyboard in Arctic conditions.

But, in their conclusions, the Test Board got to the heart of the matter: they said the current Army concept of operations would permit power to be available at the lowest echelons where secure communications would be needed; and at those echelons, electrically powered crypto-equipment would be used—e.g., the KL-7 which, by then, they were using in quantity. Well, that pretty nearly killed the KL-17. Because of our pride of authorship, because we'd put lots of man years and dollars into its development, we made a reclama, in which we suggested that there were about seven requirements that the KL-17 could meet more efficiently and economically than electrically powered equipment—notably for the replacement of a large number of code systems—and requested the Army to reconsider. In due course, the Army responded: "We have reconsidered and have determined that there is no Army requirement for the KL-17." And the KL-17 was dead. So chalk up one museum piece.

Now, the KL-17 I've been talking about was a development effort in response to rather formally stated requirements—Military Characteristics (MC's, we call them) had been developed, jointly agreed, and all the essential features the system was to have had were specified for us by the potential customers; we failed because we couldn't meet the need in time and, perhaps, because neither we nor our customers had really thought through the requirement so that when the system met the last and most acid test, the commitment of funds for production in quantity (and about 10 million dollars would have been involved), enthusiasm waned.

Now, I want to talk about an "almost" system that came about in another way. As I have mentioned, we sometimes build experimental equipments not in response to formally stated requirements, but rather in *anticipation* of them. We see, or think we see, a need that the Services or other customers have not yet expressed, and rather than wait for the long formal process to be completed, we build a prototype system based on our perception of gaps in the COMSEC inventory and informal expressions of "interest" by engineers, communicators, and COMSEC planners. Such was the case in the late 50's when it seemed that there was a crying need for improved *off-line* teletypewriter security. All we had were the one-time tape systems, a rapidly aging trouble-maker called the KW-9, and an even more ancient machine called the two-dash-one for off-line telegraphy. (The great KW-26, you will remember, is on-line and point-to-point.) Relatively efficient and compact means for embodying key generator principles were available to us by then and had been

...roved in a number of machines. It seemed to us that we could answer the communicator's prayer with an off-line machine that would solve most of the problems that plagued its predecessors. We could easily make it go as fast as any teleprinter that might come along—100,200,250,600 wpm? You name it, this machine could hack it. How about multiplicity of holders on the same key? Heretofore possible only with the lumbering electromechanical rotor techniques embodied in the KW-9. The new machine—the KW-3—could do it. How about a rapid way to key the equipment? We could do it. How about frills—adaptors so that the cipher text was produced in five-letter groups to facilitate its transmission where teletypewriter circuits were unavailable or unreliable? Could do. How about a way to take the transmission when received and automatically and instantly decipher it, so that the equipment would act as if it were on-line at the receive end? The machine could do it—it would read the indicator of the incoming message, set itself up accordingly, and automatically decipher—so no time attributable to cryptography was lost.

Sounds like it couldn't miss. The system had high security, had all these desirable operational features, was packaged in a pretty console, and worked just fine. But nobody bought it. Why not? Again, it was a combination of things. This time, time was not the problem; this one was ready before they really asked for it, not ten years later. But the customers had asked for other TTY encryption equipment which was being developed at the same time. Concepts were evolving which would minimize the need for and use of any off-line teletypewriter system. More and more, the users were accepting the notion of integrating cryptography with their communications systems, rather than accomplishing the job in two separate steps. So, with finite budgets, they hoped for smaller equipments with multi-holder rotor TTY systems in the interim. Some lessons begin to emerge from an examination of just these two aborted developments; but before summarizing them, let's talk about a few more.

While the KW-3 was gasping out its last breath, we were engaged in a frontal attack on the Department of State which, for decades, had been insisting on the continued use of certain rotor machines which, for a variety of reasons, were not adequately secure, especially in the very exposed environments where they must habitually operate. Finally, we virtually demanded that they retire some of these equipments, and they retaliated by saying they'd be glad to if we would build a new equipment tailored to their peculiar needs. They described such a system to us, and in less than 18 months, flop number three—the KW-1—was produced. (600 wpm!) This was a cipher-text autokey system which, you will remember has the one operational flaw of exaggerating any transmission garble that occurs,—typically, in teletypewriter operations, causing 10 or 15 characters to be unreadable when a single error in transmission occurs. We had been assured that, generally, highly reliable communications circuits could be used and thought that these "extended garbles" could be tolerated on the few bad circuits that might be used.

25X3, E.O.13526

25X3, E.O.13526

Withheld from public release under
§6 of the National Security Act of 1959,
50 U.S.C. 3605 (P.L. 86-36)

I can dispatch rather briefly another category of equipments that never saw daylight—there were the KX systems; "X" standing for "fax" or facsimile. We had a KX-3, a KX-4, and a KX-5, none of which saw appreciable use. As I have mentioned, it seems that facsimile requirements. at least during the middle and late 50's, had a habit of evaporating each time an equipment that could do the job became available. Such small requirements as there were were picked up by other equipments—the multi-purpose kind—that were in being anyhow, such as the KO-6 and the Navy's AFSAX-500.

So far, our failures have been a matter of time, or lack of a solid requirement, or some tragic operational flaw. or some change in concept. A much more significant and painful set of failures relates to some of the efforts we have made which collapsed because we were technically unable to accomplish what was needed. The most notable case of this has been in the voice security field. For narrow-band. long-haul voice communications, those equipments we have managed to build have gotten pretty good use—can anyone name them? (KO-6, KY-9, and KG-13/HY-2.) I know of no serious NSA attempts in the narrow-band ciphony area—i.e., ideas that got to the hardware stage, that did not go into production. USAF did have grand plans for a multi-purpose system for use in communicating with long-range aircraft—called QUICKSILVER—that would include secure voice capability. It did not pan out because the technical problems could not be surmounted at reasonable cost. But, in broad-band. short-range tactical ciphony, NSA did make two efforts that reached hardware, but failed. The first was called the AFSAY-D-803: it was the rare, perhaps unique, case in which the flop occurred because the *cryptoprinciple* was not good enough, and we did not fully appreciate this dismaying fact until after the machine was made. Naturally, the customer wanted to use it anyway; but we were adamant and had the few dozen models that had been produced dumped in the ocean.

The other attempt was the famous KY-4. It was being built at about the same time as the KY-8; but while the KY-8 was designed for use in aircraft, the KY-4 was to have been used on the ground at tactical echelons, mounted on jeeps, in tanks, and what have you. It was smaller than a bread-box (if you like big bread) 9 x 11 x 13 inches; 35 pounds, ruggedized, and designed to be compatible with field radio sets of various kinds. We had fairly high hopes for it even though speech quality was poor both because we used few digits to describe it and because it was a cipher-text auto-key system, once again exaggerating all transmission garbles. By our modern standards, it did not afford very high security, and the very liberal physical security rules we imposed to facilitate its use in the field anticipated by some years the policies we have now adopted for equipments such as the KY-8 and KW-7. There were a number of things the Services did not like about the equipment; the one that killed it was probably the fact that it reduced the range of the associated radio sets; and from this rejection. a very important lesson emerges again—there will always be a very

gh resistance to any cryptosystem which reduces the communicator's ability to do his job—sometimes it's a matter of time, as in the case of off-line systems: sometimes a matter of flexibility as in the case of systems which are hard or impossible to net; sometimes it's reliability as in the case of systems that compound garbles. In this case, the user was already unhappy at the range limitations of his radios and any further reduction in the ability of the commander to reach his troops was intolerable. The possibility of modifying the contemporaneous KY-8 to meet the ground needs made the death of KY-4 easier to bear and, ironically, it has turned out that the KY-8 has thus far been bought, principally by the Army and Marines for ground use, and not for the aircraft for which it was originally designed. In future courses, you will hear about follow-on equipments like the KY-28 to relieve the airborne problem.

The last equipment to come to a bitter end is the KL-15. Here it is:
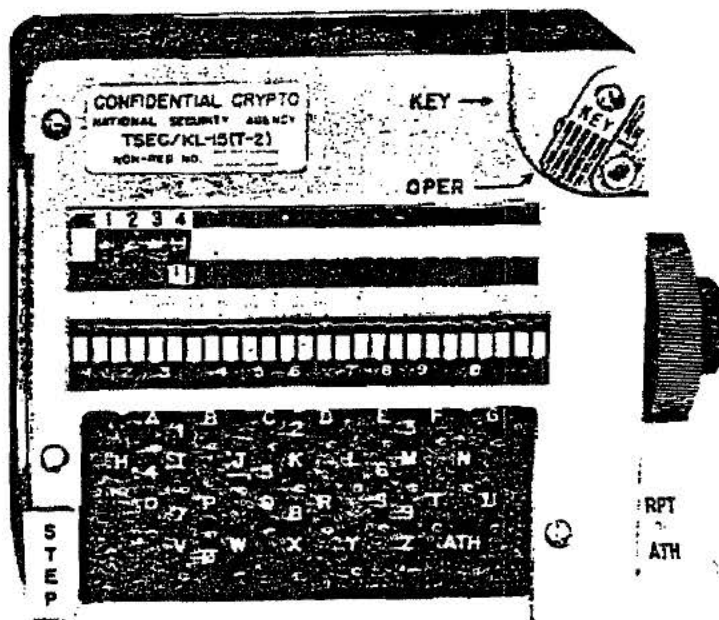
It's a nice compact toy, and it was many years abuilding. It's now headed for the museum. What was it for? It was the closest we could come to a pocket-sized machine with which we could authenticate, or perhaps encrypt call signs, or use for the encryption of short tactical messages. You'll note it has a keyboard of sorts; has self-contained power, and enough rotors and things inside it to make you think it could provide considerable security. Only one other equipment had been built in the last 10 years approaching this size; it was strictly for authentication and, although we built hundreds of them, it never got popular. Here it is, the KL-99: for some reason nicknamed the "double hot-dawg".

Well, back to the KL-15: there were forecasts of requirements for many thousands of these things (51,908)! We hoped to replace awkward, slow paper codes and authentication systems with it and get a much higher degree of security than the paper systems were providing. As a concession, we established procedures to permit encryption of short messages, as I said, although that was not the original intention. What happened? My guess is that we here in NSA had developed a kind of *security blind-spot*. (Another lesson.) The Office of Standards and Evaluations more than anybody else—and perhaps exclusively—has to shoulder the blame. Preoccupied with the fact that we are in the communications *security* business, and offered a mechanical way to encrypt short messages at tactical echelons with much higher security than existing materials could provide, we went overboard, that's all. We maximized its security advantages in our minds, minimized its operational disadvantages, and professed shock when actual service tests produced a jaundiced reaction which, had we thought it through, we might well have predicted 6 or 7 years before when we first got serious about having it built. It doesn't work any faster than a code, and not as fast as some of them. It's more difficult to use than a printed authenticator table. It's heavy. It's expensive; especially when you're buying an operating speed of only four words a minute. We had a counter on an early version. In informal user trials, they suggested it was superfluous and we'd save some money, weight, and complication if we took it off, so we did. The lack of that counter in the final "acceptance" models may have been the last straw. Without it, the user cannot keep track of where he is in enciphering or deciphering; and once he loses his place, he might as well start from the beginning again. Visualize that problem in a rainy foxhole as you try to call for support or instructions in a rapidly developing tactical situation! The lesson: the customer, particularly at tactical echelons, is not likely to be grateful or even impressed by any offer of added security if what you offer him works no better than what he already has. And he shouldn't be. Real-time communications are becoming more and more critical to our people in the field as they cope with or themselves use modern weapons systems. An authenticating pilot now may travel many miles in the time it takes him to derive a correct authenticator from a little printed chart or matrix. If you give him a machine that takes just as long and requires him to use both hands as well, you have not improved his situation.

Before we leave the subject of flops, I'd like to tell you, in case you haven't already guessed, that mistakes are not the private property of the cipher machinery—the administrative machinery also owns a few acres.

In late 1970, we found ourselves with about $70,000,000 invested in more than 10,000 secure tactical voice equipments in Southeast Asia. These equipments—the KY-8/28/38 NESTOR family—

...re sent in record time after an all out effort. There was only problem; most of them could not be used. Because of logistical and administrative errors; equipment was arriving without interconnecting cables, sometimes missing installation kits, occasionally without the correct chassis and often with no radio to match. After sorting out these problems (when they could be sorted out), next came the modifications. The following extract from a report on the subject indicates the kinds of problems we had in this area: "Since much of the communications in SEA are air-to-ground, timing of modifications was very critical. Invariably some air frames were modified, but the radios were not or vice versa. In some cases, those who had all modifications installed had no KY-8/28/38's." To top it off, even when equipments were installed, modified and operating properly, users still couldn't communicate all the time because the users weren't holding a common key.

Enough said.

I have touched on a few false starts out of a great many we have had. Those I have described got farther along than they should have. Many other attempts have been abandoned before they cost us very much. None of these efforts were total losses; each contributed to our knowledge. We do learn, although slowly.

NINTH LECTURE: Strengths and Weaknesses

When this course was being outlined, it was suggested that an overview of the strengths and weaknesses of the U.S. COMSEC effort might be useful; but developing a generalized estimate of this kind is no simple matter. I have chosen to divide this part of the presentation into two parts—one related to the systems—and especially the machines—we now have in being; the other to our program as a whole.

As we speak of the systems themselves, you must remember that we are talking about perhaps 75 quite different animals—including more than 30 machines—each in some way unique in how it works and where it is employed. This multiplicity of systems itself implies certain strengths in our COMSEC posture; it shows that we can afford to tailor systems to specific needs and thus approach optimum efficiency and security on specific circuits or networks. By doing this, we face the hostile cryptanalysts with a variety of separate problems of diagnosis and actual attack so that he must dilute his resources so, if he concentrates on only one or a few of our systems, the balance get off light. This great diversity in our COMSEC inventory also implies certain weaknesses which I have touched on lightly once before—the lack of standardization with all its attendant ills. Complicated logistics, production difficulties, training problems for maintenance and operating personnel, unwieldy systems management—all adding to the cost and detracting from the efficiency of our program as a whole. As I said on the first day, throughout your professional life here, you will be continually weighing these contradictory factors, making "trade-offs" or compromises between optimum security and operational suitability on the one hand, and on producibility and logistic "supportability" on the other. The most secure machine in the world does the user no good if we can't make and supply the tricky components needed to keep it working. Conversely, a system which is the logistician's dream buys us nothing if essential security features or operational characteristics had to be eliminated to simplify production and supply.

You will recall that in a previous lecture, I identified for you the *major* machines in our current inventory. There are now nine of them: for literal traffic, the KL-7 and KL-47; for point-to-point teletypewriter traffic, the KW-26; for multi-holder and tactical teletypewriter traffic, the KW-7; for broadcast teletypewriter traffic, the KW-37; for long-range ciphony, the KY-9 and KG-13/HY-2; for short-range fixed plant ciphony, the KY-3; for tactical ciphony, the KY-8; and for multi-purpose key generating, the KG-3/13. These nine machines will account for about 100,000 equipments out of a total of perhaps 140 thousand. To estimate the overall strength of these systems, we have always to consider them in terms of what each is supposed to do—just what kind of traffic is it designed to protect, and for how long. Is it enciphering a routine D/F report, or a nuclear strike plan? Six factors have to be considered in the case of equipments, five in the case of manual materials:

1. The cryptoprinciple itself.
2. The embodiment of the principle in a machine or on paper.
3. The operational circumstances of use.
4. Transmission security.
5. The physical protection afforded.
6. TEMPEST (if the system is mechanical, electro-mechanical or electronic). TEMPEST will be the subject of the next lecture.

I have touched on most of these factors from time to time throughout these lectures, and will now expand on each in somewhat greater detail. In these comments, I will be generalizing about the major machines rather than codes or things unless I specify otherwise.

Cryptoprinciples.—The first thing important to understand about the principles we use is that they are designed to meet a specific set of standards. For the high-grade, long-term security systems, these standards are rigorous and conservative.

25X3, E.O.13526

25X3, E.O.13526

Embodiment.—In the late 1950's early models of the KY-8 were going through their paces, tests were being made to see how they affected associated radio sets, officials of the Services and other Agencies were attending demonstrations. An aircraft equipped with a KY-8 flew concentric circles around Andrews AFB while interested parties crowded around an equipment on the ground and listened on a loudspeaker as the pilot originated transmission after transmission and came in loud and clear until he proceeded out beyond the radio horizon. There was not a single failure to achieve

synchrony: the potential customers were impressed and we were delighted. As I may have mentioned. the KY-8 is one of those systems that generates a new unique indicator for itself each time an originator pushes to talk. This indicator comes from a *randomizer* that puts out a stream of pulses which set up all receiving machines to a unique setting for the decryption of the message arriving a few milliseconds later.

When the engineers got the pair of equipments back in the lab, they continued using them for a series of tests and experiments for another week or so before they began to wonder about the continued infallibility of the indicator process, and decided to display the output of the randomizer on an oscilloscope. They activated the equipment and out went the "random" indicator. It was:

$$11111111111111111$$
Again: 11111111111111111

And so forth. *every* time. In short, this magnificent little equipment, costing thousands of dollars, containing something like 450 sub-miniature tubes and all sorts of complex circuitry, was producing a mono-alphabetic substitution system having considerably less resistance to cryptanalysis than many of the systems provided on the back of Kellogg's Corn Flakes packages. And thereby hangs a tale. In that fine machine. one tiny component had failed and had rendered it literally worse than useless. For the user had no way of knowing his system was not working properly—there was no alarm: there was no convenient check-point so that the situation could be detected in preventive maintenance: it did not cause any garbles in the receiving machines: they received a sequence of digits at the proper time and of proper length and. with the typical stupid indifference of machines, accepted 111111111111111111 as just as good a place to start as any other.

Of course. the cryptanalysts and engineers had been concerned with various kinds of machine failures for many years and. especially in the larger equipments. had incorporated at least rudimentary checks and alarms to catch the more likely and important failures. As far back as WW II. some of the old rotor machines had interlocks on them which would stop the machine cold if a particular rotor failed to move during 26 consecutive operations of the equipment. But. perhaps as much as any other incident—and there were lots of them—the KY-8 case triggered a full-scale and continuing pre-occupation with the science of "failure analysis". As a matter of course. the cryptanalysts. working with the engineers. must now consider the likelihood of deterioration or failure of various components and determine what the impact of such failure will be on the system. And this impact may vary widely—from catastrophic proportions to a slight reduction in the amount of work necessary for successful cryptanalysis. And based on these judgements, the kinds of safeguards incorporated may vary from that triple key generator in the KW-37 to practically nothing at all.

A modest body of doctrine has begun to evolve with respect to machine failures and what to do about them. Clearly. we cannot afford to incorporate a special safeguard for every conceivable failure—it's too costly: the resultant machinery may be too large or complicated for its intended use; there comes a point when the alarm circuits themselves cause failure. or are so complex as to comprise a maintenance man's nightmare. Those of you who get very deeply involved in this problem will become familiar with what the engineers term "mean time between failure" (MTBF). This relates to how long a given component like a diode or resistor may be expected to last. Some engineers have made calculations for whole machines and suggest a very strong correlation between the gross number of components used and the time when failure is apt to occur—the more components there are, the sooner one of them is likely to let go. Thus. the inclusion of many alarms may tend to be self-defeating. or so they argue. We argue back.

Looked at another way: S3 produces one-time tapes and alternately boasts and laments the fact that they carry out some 64 separate electronic and visual checks on their product. Still, some of them get out that shouldn't have. So, again. we are faced with judgements on how far to go without overdesigning our machinery and yet assure essential safeguards for most of our traffic most of the time. In any event. the main "rules" that have emerged are these:

1. Where very great reliability is essential to having the system be effective at all. we'll go all out to get it. Usually, this is done in one of two ways: excruciating quality control. involving hand-

icking of components and exhaustive testing of each (e.g., the cryptocomponents in satellites); or, heavy reliance on alarms, and pre-operational checks, usually coupled with some redundancy (e.g., the KW-37 transmitter).

Note: The overriding consideration here is *not* security, but operational necessity.

2. If the failure causes the machine to stop operating all together, don't alarm it: that's plenty of alarm in itself and, if you transmit nothing, the security implications are nil.

3. If the failure is immediately obvious to the recipient, and he has a means of telling you so, e.g., by "breaking" you to stop you automatically, or by telling you "I can't understand a word you say," then, *usually*, special alarms are not necessary. (I say "usually", because in some of the systems that operate very fast, producing thousands or even millions of bits of key each second, a few moments of faulty operation might conceivably produce enough data to give the hostile analyst all he needs to exploit that failure, and a warning from the distant end may be too late to prevent attack. Even though you correct the situation, he may still have a basis for recovering all the traffic in the day's key that had been sent before the failure occurred.)

4. Don't demand special alarms based on the effect of two or more independent failures occurring simultaneously. Typically, the analyst might say: "Good lord, if that one little adder fails, the final key to be combined with the cipher text will be all 0's." And the engineer (or budgeteer) may rejoin: "But that's exactly what this little counter is designed to detect, and if it sees all 0's for more than X milliseconds, the machine will stop." If the analyst says, "But what if the counter fails, too?" he will probably lose the argument. He'd lose it, that is, if there is any reasonable way to periodically check that the counter is operative.

In translating a cryptoprinciple into hardware, there's more to it than assuring reliability, of course. There's the matter of assuring that each of the hundreds or thousands of individual elements produces the value or contributes to the process in just the way the logical design says it should. Remember I said that given *everything* about the machine, including its specific key for day, the output has to be perfectly predictable, so that other machines can produce exactly the same thing and thus communicate. This means that a crypto-mathematician or engineer ought be able to make a "paper" model of the machine and, for a particular setting write out what the final generated key should be. We had a scare here some years ago—I have forgotten with which machine: it may have been KW-37—when we finally got the first brand new production model in the laboratory and tried to check its actual key against the theoretical product. The machine seemed to work just fine, but persistently produced different key than we said it would. It took many weeks to discover that an error had been made in its fabrication: one tiny element was inverted and gave us 0's instead of 1's and vice versa.

One difficulty, not just with randomizers, but with other components as well, is in detecting some of the minor failures which cannot be practicably alarmed. In modern electronic key generators, it takes a highly trained maintenance man to note them. His maintenance manuals call for reports of various noted conditions, but in practice we have rarely seen such reports and are somewhat skeptical that the equipments are all behaving as nicely as this lack of reports would imply. We think this is partly due to the inadequacies in the reporting system itself, and partly because detection is so difficult—particularly when the weakness is one that does not stop the machine from working. So, while our current systems are rather well protected against catastrophic failure, we have to chalk up as less than satisfactory our ability to detect the creeping insidious failures in some machines.

Circumstances of Use.—After the principles themselves and their embodiment, the third factor we must consider in judging the degree of security our systems afford has to do with how they are used. In an off-line system, we may use very few internal checks on proper operation of the machine itself because operators should adhere to the general rules of complete check decryption on a separate machine before they release their cipher texts for transmission. If there was something wrong with the first machine, the second machine will surely catch it unless it happened to suffer the same failure at the same point in the process. The trouble is, off-line operations are slow enough already, without doubling message preparation time by duplicating the whole business so, now we no longer require check decryption but suggest it be adopted as an optional procedure.

A few minutes ago, I said we sometimes economized on alarms when, in on-line operations, the distant station has the opportunity to tell you you're going wrong. With a system like the KW-7, for instance, your addressee is not apt to let you produce very much gibberish before he calls you about it. But on some circuits, users may desire to use what they call "unattended operation". In this case, the machines may be left alone for some hours or even all night. Then, if something goes wrong we may lose a whole batch of traffic instead of fragmentary information or, conceivably, may have produced enough faulty key to provide an entering wedge for a cryptanalytic attack on the daily setup of the machine itself thus jeopardizing the traffic of the whole network instead of the output of a single station. So again, our security judgements about the KW-7 can't be absolute. As often as not, our security assessments of various systems will contain careful little "System X, *operating properly and properly used, provides a high degree. . .*"

Despite what I've implied about potential weaknesses in our machines because of shortcuts in the embodiment of principles or some tolerated peculiar circumstances of use, we have not had, in recent years, an occurrence reported which has caused us to declare, for *cryptographic* reasons, a compromise of a day's traffic in a machine system. We *have* lost a good many individual messages, and fragments of many others, because a machine has failed or an operator has erred: but even in these instances, the most usual situation is that the operator has failed to use the machine altogether and has inadvertently sent the message out in the clear.

With our codes, it is quite a different story. The circumstances of their use are the most critical factor in determining how much security they actually afford. You will recall my having said that the non-one-time codes are as a class the weakest things we have anyhow. If volume, message lengths, stereotypes, or spelling is excessive, they may collapse even more quickly than we expect them to and not give even the few days' or weeks' security for which they are typically designed. This question of how a system looks as actually used leads us to the next factor, Transmission Security for, inevitably, TRANSEC people have to find ways of examining systems as they operate, of *monitoring* and analyzing transmissions in the real world.

Transmission Security.—Traditionally, we have thought of transmission security as any and all the measures we take to prevent exploitation of our communications by any means *except* cryptanalysis. Over the years, the U.S. has managed to preserve a pretty sorry TRANSEC posture, and the exception of the one technique called Traffic Flow Security (which I described when we discussed one-time tape systems) we have very few sophisticated means in being to limit the amount and kind of information that can be derived by a mere examination of those parts of our transmissions which are not encrypted. The greatest transmission security weakness of all, of course, results from our need to transmit a great deal of information in the clear; so that hostile SIGINT has a ball in the business of examining "message externals" when the whole darned transmission is external.

What we need, of course, are more and better systems to reduce, and reduce sharply, the amount of information we now send in the clear. After that, we need a whole series of new transmission systems which will make our traffic difficult to intercept. We have a few experimental systems and one operational one that are designed to provide this resistance to interception, but a great deal of our current traffic is there for the taking so that hostile interceptors, by relatively quick and simple traffic analysis, can discover who's talking, who's being addressed, how much traffic is being exchanged and often, because of plain-language transmissions and other collateral, what's being talked about.

Thus we hand him on a platter our order of battle and tip him off about impending plans and activities—in short, warn him about what we may be up to, and when, and where, and with what force.

One of our means of getting insights into the operations of hostile SIGINT is through interrogations of individuals who have defected from the Soviet Bloc.

25X3, E.O.13526

Withheld from public release under
§6 of the National Security Act of 1959,
50 U.S.C. 3605 (P.L. 86-36)

Of the nine major equipments I listed for you, only three have a built-in TRANSEC feature. They are the KW-26, the KW-37, and the KG-3/13. The technique used is the Traffic Flow Security I mentioned. Once they get set up for the day, they send out a continuous flow of cipher text whether actual messages are being sent or not. So the interceptor cannot tell how many messages are being sent or whether, in fact, there is any bona fide traffic being passed. The rest of the systems, to greater or lesser degrees, are vulnerable to traffic analysis. They may encrypt the actual identities of addressees (a technique called CODRESS), but usually call signs or external groups called routing indicators give a pretty good clue as to where they're going.

So now, in our list of factors to be considered in judging current COMSEC strengths and weaknesses; chalk up TRANSEC as pretty bad.

Physical Security.—My remarks will be relatively brief. Perhaps the scope of the problem can best be illustrated by some capsule case histories from our files:

A B-52 crashes in Spain, and for weeks thereafter men sweep the area with scintillators and Geiger counters for fragments of nuclear warhead. Also scattered about are some codes and authenticators used by many aircraft in SAC. A physical security problem.

An Army unit in Seoul is overwhelmed by a horde of North Koreans and Chinese and leaves behind partly smashed, partly burned cipher machines and rotors.

A mob storms the embassy in Taiwan; breaks through the flimsy wall into the cryptocenter, and scales 100 rotors out the window to their friends below.

A Service cryptographer, badly in debt, troubles at home, etc., etc., approaches (or is approached by) a foreign agent. Crypto-documents for sale?

An operational concept for IFF (identification friend or foe) calls for 20,000 aircraft to carry identical key (remember our remarks on compartmentation?) and use it for three days or a week without change (and our comments on supersession?).

A tailgate flies open on a registered mail truck and a thousand documents are scattered along a windy highway.

A man buys fish and chips in Hong Kong and finds it wrapped in a copy of a U.S. code instead of the traditional newspaper.

A U.S. ranger outfit finds pages of a one-time pad being used as trail-markers by the Viet Cong.

A faulty incinerator belches chunks of superseded key lists and codes—as big as your fist—all over Arlington, Va.

And day after day, cryptographers reach for a key list or a key card to set up a machine, or to check it off on inventory, and it's missing. Presumed inadvertently burned.

We handle hundreds of cases annually—two or three each year are apt to be quite dramatic. The problems are knotty and seemingly infinite in their variety; they are present from the cradle to the grave in the life of a classified cryptodocument or machine. How do you produce it? How do you mark it or otherwise identify it? What degree of integrity do you demand for personnel having access to it? Is a background investigation any good? (The French, I'm told, don't clear people until they're at least 25 years old on the theory that an individual hasn't had time to develop a background good or ill until then. The Turks don't "clear" their people at all. If they prove treacherous, they shoot 'em.)

Because of all these problems, our estimate of physical security strengths and weeknesses of current systems has to be relative, just as it is in considering operational circumstances in use. You have to identify which machinery or which cryptographic network you are talking about before a meaningful statement about physical integrity can be made, for this depends on the way the material is packaged, where it's located, how big a network is involved, the level of clearance of users, and so forth. The KY-9 and KY-3, for instance, are designed for use outside of cryptocenters and communications centers in places where there are no trained guards and cryptocustodians or any set of formal controls in force. They go up into normal government office spaces and, in the case of the KY-3, into private residences. Thus, there are special problems in protecting the equipment and its keys. So those machines are packaged in a three-combination safe and we feel better. But not much better, because they aren't very good safes—some of our physical security experts refer to them, not very affectionately, as "sardine cans". But then again, *none* of the safes we can afford to make or buy are very good; they may resist covert penetration for an hour or so but that's all. So we use an important concept called "defense in depth". We use the safe as a deterrent should someone have access. We limit the time the system can be left in an unattended office or home, thus limiting opportunity for a penetration attempt. We sharply limit the amount of key that can be kept with the machine, thus minimizing how much can be lost should that shadowy "unauthorized person" get to it.

If I have to *generalize* on our current physical security posture, I would say it is "good". Not *excellent*, mind you, or we would have fewer of the cases both routine and extraordinary that we have to handle every year. But not *bad*, either, because our known and presumed losses continue to represent a very tiny fragment of the whole, and the exploitation of even those requires a good deal more than mere acquisition of the key list or what have you. Like, man, you have to get that key to somebody who understands it and knows what to do with it. (In the case of the machines left in Seoul, they were still piled up behind the signals center three days later when we re-occupied that sector, apparently undisturbed, although the N. Koreans had obviously picked over the area for things they could use, like ammunition.) Not only do you have to get the material to some SIGINT outfit, you have to get it to them *in time* to do them some good. The bulk of material we physically lose is tactical in nature; intelligence committed to such materials is almost always perishable, of no use within a few days or weeks after it is effective. And of course, the hostile SIGINT organization must have had the foresight to collect the cipher traffic in the key that is captured. It's a rather expensive investment to intercept traffic in the hope that its key will blow off a flightdeck and be recovered in time to do some good.

TENTH LECTURE: TEMPEST

In 1962, an officer assigned to a very small intelligence detachment in Japan was performing the routine duty of inspecting the area around his little cryptocenter. As required he was examining a zone 200 ft. in radius to see if there was any "clandestine technical surveillance". Across the street, perhaps a hundred feet away, was a hospital controlled by the Japanese government. He sauntered past a kind of carport jutting out from one side of the building and, up under the eaves, noticed a peculiar thing—a carefully concealed dipole antenna, horizontally polarized, with wires leading through the solid cinderblock wall to which the carport abutted. He moseyed back to his headquarters, then quickly notified the counter-intelligence people and fired off a report of this "find" to Army Security Agency, who, in turn, notified NSA. He was directed to examine this antenna in detail and perhaps recover it, but although the CIC had attempted to keep the carport under surveillance that night, the antenna had mysteriously disappeared when they checked the next day. Up on the roof of the hospital was a forest of Yagi's, TV-antennas, all pointing towards Tokyo in the normal fashion, except one. That one was aimed right at the U.S. cryptocenter.

In 1964, you will all recall, the highly publicized flap occurred when more than 40 microphones were discovered in our Embassy in Moscow. Most people were concerned about all the conversations that may have been overheard and the resultant compromise of our diplomatic plans ☐
☐ We were concerned with something else: what could those microphones do to the cryptomachines used there? And for what were the unpublicized gadgets also found with the microphones? Why was there a large metal grid carefully buried in the cement of the ceiling over the Department of State communications area? A grid with a wire leading off somewhere. And what was the purpose of the wire that terminated in a very fine mesh of smaller hair-like wires (Litz wire)? And, while we were at it, how did these finds relate to other mysterious finds and reports from behind the Curtain—reports dating clear back to 1953? Intriguing? I guess so. Disturbing? Very.

Why, back in 1954, when the Soviets published a rather comprehensive set of standards for the suppression of radio frequency interference, were those standards much more stringent for their teletypewriters and other communications equipment than for such things as diathermy machines, industrial motors, and the like, even though the teleprinters were much quieter in the first place?

Behind these events and questions lies a very long history beginning with the discovery of a possible threat, the slow recognition of a large number of variations of that threat and, lumbering along a few months or a few years afterwards, a set of countermeasures to reduce or eliminate each new weakness that has been revealed. I am going to devote several hours to this story, because your exposure to this problem may be only peripheral in your other courses, because it has considerable impact on most of our cryptosystems, and because we view it as the most serious technical security problem we currently face in the COMSEC world.

First, let me state the general nature of the problem as briefly as I can, then I will attempt something of a chronology for you. In brief: any time a machine is used to process classified information electrically, the various switches, contacts, relays, and other components in that machine may emit radio frequency or acoustic energy. These emissions, like tiny radio broadcasts, may radiate through free space for considerable distances—a half mile or more in some cases. Or they may be induced on nearby conductors like signal lines, power lines, telephones lines, or water pipes and be conducted along those paths for some distance—and here we may be talking of a mile or more.

When these emissions can be intercepted and recorded, it is frequently possible to analyze them and recover the intelligence that was being processed by the source equipment. The phenomenon affects not only cipher machines but any information-processing equipment—teleprinters, duplicating equipment, intercomms, facsimile, computers—you name it. But it has special signifi-

...ance for cryptomachines because it may reveal not only the plain text of individual messages being processed, but also that carefully guarded information about the internal machine processes being governed by those precious keys of ours. Thus, conceivably, the machine could be radiating information which could lead to the reconstruction of our key lists—and that is absolutely the worst thing that can happen to us.

Now, let's go back to the beginning. During WW II, the backbone systems for Army and Navy secure TTY communications were one-time tapes and the primitive rotor key generator then called SIGTOT. Bell Telephone rented and sold the military a mixing device called a 131-B2 and this combined with tape or SIGTOT key with plain text to effect encryption. They had one of these mixers working in one of their laboratories and, quite by accident, noted that each time the machine stepped, a spike would appear on an oscilloscope in a distant part of the lab. They examined these spikes more carefully and found, to their real dismay, that they could read the plain text of the message being enciphered by the machine. Bell Telephone was kind enough to give us some of their records of those days, and the memoranda and reports of conferences that ensued after this discovery are fascinating. They had sold the equipment to the military with the assurance that it was secure, but it wasn't. The only thing they could do was to tell the Signal Corps about it, which they did. There they met the charter members of a club of skeptics (still flourishing!) which could not believe that these tiny pips could really be exploited under practical field conditions. They are alleged to have said something like: "Don't you realize there's a war on? We can't bring our cryptographic operations to a screeching halt based on a dubious and esoteric laboratory phenomenon. If this is really dangerous, prove it." The Bell engineers were placed in a building on Varick Street in New York. Across the street and about 80 feet away was Signal Corps' Varick Street cryptocenter. The Engineers recorded signals for about an hour. Three or four hours later, they produced about 75% of the plain text that was being processed—a fast performance, by the way, that has rarely been equalled. (Although, to get ahead of the story for a moment, in some circumstances now-adays, either radiated or conducted signals can be picked up, amplified, and used to drive a teletypewriter directly thus printing out the compromising information in real time.)

The Signal Corps was more than somewhat shook at this display and directed Bell Labs to explore this phenomenon in depth and provide modifications to the 131-B2 mixer to suppress the danger. In a matter of six months or so, Bell Labs had identified three separate phenomena and three basic suppression measures that might be used. The first two phenomena were the space radiated and conducted signals I have described to you; the third phenomenon was magnetic fields. Maybe you remember from high school physics having to learn about left hand rule of thumb and right hand rule of thumb, and it had to do with the fact that a magnetic field is created around a wire every time current flows. Well, a prime source of radiation in an old-fashioned mixing device is a bank of magnet-actuated relays that open and close to form the elements of teletypewriter characters being processed. The magnetic fields surrounding those magnets expand and collapse each time they operate, so a proper antenna (usually some kind of loop, I think) nearby can detect each operation of each relay and thus recover the characters being processed. The bad thing about magnetic fields is that they exist in various strengths for virtually all the circuitry we use and are extremely difficult to suppress. The good thing about them is that they "attenuate" or decay rapidly. Even strong fields disappear in 30 feet or so, so they comprise a threat only in special circumstances where a hostile intercept activity can get quite close to us.

The three basic suppression measures Bell Labs suggested were:

1. Shielding (for radiation through space and magnetic fields),
2. Filtering (for conducted signals on power lines, signal lines, etc),
3. Masking (for either space radiated or conducted signals, but mostly for space).

The trouble with these solutions, whether used singly or in combination, all stems from the same thing: that is the fact that, quite typically, these compromising emanations may occur over a very large portion of the frequency spectrum, having been seen from near d.c. all the way up to the megacycle range (and that's a lot of cycles). Furthermore, 5 copies of the same machine may each

exhibit different characteristics, radiating at different frequencies and with different amplitudes. And even the same machine may change from day to day as humidity changes or as contacts become pitted, or as other components age. This means that any shielding used must form an effective barrier against a large variety of signals, and this proves difficult. Similarly, the filter has to be a nearly perfect one and they become big, heavy, and expensive. Furthermore, on signal lines for example, how do you get your legitimate cipher signal through without compromising signals squeezing through with them?

Masking, which is the notion of deliberately creating a lot of ambient electrical noise to override, jam, smear out or otherwise hide the offending signals, has its problems too. It's very difficult to make a masking device which will consistently cover the whole spectrum, and the idea of deliberately generating relatively high amplitude interference does not sit too well with folks like IRAC (The Interdepartmental Radio Advisory Committee) of the Office of Telecommunications (OTP) who don't like the idea of creating herring bone patterns in nearby TV pictures or interrupting legitimate signals like aircraft beacons.

Bell Labs went ahead and modified a mixer, calling it the 131-A1. In it they used both shielding and filtering techniques. Signal Corps took one look at it and turned thumbs down. The trouble was, to contain the offending signals, Bell had to virtually encapsulate the machine. Instead of a modification kit that could be sent to the field, the machines would have to be sent back and rehabilitated. The encapsulation gave problems of heat dissipation, made maintenance extremely difficult, and hampered operations by limiting access to the various controls.

Instead of buying this monster, the Signal Corps people resorted to the only other solution they could think of. They went out and warned commanders of the problem, advised them to control a zone about 100 feet in diameter around their communications center to prevent covert interception, and let it go at that. And the cryptologic community as a whole let it go at that for the next seven years or so. The war ended; most of the people involved went back to civilian life; the files were retired, dispersed, and destroyed. The whole problem was plain forgotten. Then, in 1951, the problem was, for all practical purposes, rediscovered by CIA when they were toying with the same old 131-B2 mixer. They reported having read plain text about a quarter mile down the signal line and asked if we were interested. Of course, we were. Some power line and signal line filters were built and immediately installed on these equipments and they did the job pretty well as far as conducted signals were concerned. Space radiation continued unabated, however, and the first of many "radiation" policies was issued in the form of a letter (AFSA Serial: 000404, Nov. 1953?) to all SIGINT activities requiring them to either:

1. Control a zone 200 feet in all directions around their cryptocenters (the idea of preventing interceptors from getting close enough to detect space radiation easily), or
2. Operate at least 10 TTY devices simultaneously (the idea of masking; putting out such a profusion of signals that interception and analysis would be difficult), or
3. Get a waiver based on operational necessity.

And the SIGINT community conformed as best it could; and general service communicators adopted similar rules in some instances. The 200 feet figure, by the way, was quite arbitrary. It was not based on any empirical evidence that beyond such distance interception was impractical. Rather, it was the biggest security zone we believed the majority of stations could reasonably comply with and we knew that, with instrumentation then available, successful exploitation at that range was a darn sight more difficult than at closer distances and, in some environments not practical at all.

At the same time we were scurrying around trying to cope with the 131-B2 mixer, we thought it would be prudent to examine every other cipher machine we had to see whether the same problem existed. For, way back in the late 40's, Mr. Ryon Page and one of his people were walking past the cryptocenter at Arlington Hall and had heard the rotor machines inside clunking away. He wondered what the effect would be on the security of those systems if someone were able to determine which rotors or how many rotors were stepping during a typical encryption process. In due course, some

assessments were made on what the effect would be. The assessments concluded that it would be bad, and they were filed away for future reference. Now, it appeared that there might be a way for an interceptor to recover this kind of data. So, painstakingly, we began looking at our cryptographic inventory. Everything tested radiated and radiated rather prolifically. In examining the rotor machines, it was noted the voltage on their power lines tended to fluctuate as a function of the numbers of rotors moving, and so a fourth phenomenon, called power line modulation, was discovered through which it was possible to correlate tiny surges and drops in power with rotor motion and certain other machine functions.

Progress in examining the machines and developing suppression measures was very slow. In those days, S2 did not have any people or facilities to work on this problem; no fancy radio receivers or recording devices, no big screen rooms and other laboratory aids, and such things as we obtained we begged from the SIGINT people at Ft. Meade. In due course, they got overloaded, and they could no longer divert their SIGINT resources to our COMSEC problems. So R&D began to pick up a share of the burden, and we began to build up a capability in S2. The Services were called in, and a rudimentary joint program for investigative and corrective action got underway. The Navy, particularly, brought considerable resources to bear on the problem.

By 1955, a number of possible techniques for suppressing the phenomena had been tried: filtering techniques were refined somewhat; teletypewriter devices were modified so that all the relays operated at once so that only a single spike was produced with each character, instead of five smaller spikes representing each baud—but the size of the spike changed with each character produced and the analysts could still read it quickly. A "balanced" 10-wire system was tried which would cause each radiated signal to appear identical, but to achieve and maintain such balance proved impractical. Hydraulic techniques were tried to get away from electricity, but were abandoned as too cumbersome; experiments were made with different types of batteries and motor generators to lick the power line problem—none too successfully. The business of discovering new TEMPEST threats, of refining techniques and instrumentation for detecting, recording, and analyzing these signals progressed more swiftly than the art of suppressing them. With each new trick reported to the bosses for extracting intelligence from cryptomachines and their ancillaries, the engineers and analysts got the complaint: "Why don't you guys stop going onward and upward, and try going downward and backward for a while—cure a few of the ills we already know about. instead of finding endless new ones." I guess it's a characteristic of our business that the attack is more exciting than the defense. There's something more glamorous, perhaps, about finding a way to read one of these signals a thousand miles away than to go through the plain drudgery and hard work necessary to suppress that whacking great spike first seen in 1943.

At any rate, when they turned over the next rock, they found the acoustical problem under it. Phenomenon #5. Of course, you will recall Mr. Page and his people speculating about it way back in 1949 or so, but since the electromagnetic phenomena were so much more prevalent and seemed to go so much farther, it was some years before we got around to a hard look at what sonic and ultrasonic emissions from mechanical and electromechanical machines might have in store.

We found that most acoustical emanations are difficult or impossible to exploit as soon as you place your microphonic device outside of the room in which the source equipment is located; you need a direct shot at the target machine; a piece of paper inserted between, say an offending keyboard, and the pickup device is usually enough to prevent sufficiently accurate recordings to permit exploitation. Shotgun microphones—the kind used to pick up a quarterback's signals in a huddle—and large parabolic antennas are effective at hundreds of feet if, again, you can see the equipment. But in general, the acoustical threat is confined to those installations where the covert interceptor has been able to get some kind of microphone in the same room with your information-processing device—some kind of microphone like an ordinary telephone that has been bugged or left off the hook. One interesting discovery was that, when the room is "soundproofed" with ordinary acoustical title, the job of exploitation is easier because the soundproofing cuts down reflected and reverber-ing sound, and thus provides cleaner signals. A disturbing discovery was that ordinary micro-nes, probably planted for the purpose of picking up conversations in a cryptocenter, could detect

machine sounds with enough fidelity to permit exploitation. And such microphones were discovered in ▢

The example of an acoustical intercept I just showed you is from an actual test of the little keyboard of the KL-15. You will note that each individual key produces a unique "signature". Since (before it died) the KL-15 was expected to be used in conjunction with telephonic communications, this test was made by placing the machine a few feet from a gray phone handset at Ft. Meade and making the recording in the laboratory at Nebraska Avenue from another handset. So that's really a recording taken at a range of about 25 miles, and the signals were encrypted and decrypted in the gray phone system, to boot.

The last but not least of the TEMPEST phenomena which concerns us is referred to as cipher signal modulation or, more accurately, as cipher signal anomalies. An anomaly, as you may know, is a peculiarity or variation from the expected norm. The theory is this: suppose, when a crypto-system is hooked to a radio transmitter for on-line operation, compromising radiation or conducted signals get to the transmitter right along with the cipher text and, instead of just sending the cipher text, the transmitter picks up the little compromising emissions as well and sends them out full blast. They would then "hitchhike" on the cipher transmission, modulating the carrier, and would theoretically travel as far as the cipher text does. Alternatively, suppose the compromising emanations cause some tiny variations or irregularities in the cipher characters themselves, "modulate" them, change their shape or timing or amplitude? Then, possibly, anyone intercepting the cipher text (and anyone can) can examine the structure of the cipher signals minutely (perhaps by displaying and photographing them on the face of an oscilloscope) and correlate these irregularities or anomalies with the plain text that was being processed way back at the source of the transmission. This process is called "fine structure analysis". Clearly, if this phenomenon proves to be at all prevalent in our system, its implications for COMSEC are profound. No longer are we talking about signals which can, at best, be exploited at perhaps a mile or two away and, more likely, at a few hundred feet or less. No longer does the hostile interceptor have to engage in what is really an extremely difficult and often dangerous business, i.e., getting covertly established close to our installations, working with equipment that must be fairly small and portable so that his receivers are unlikely to be ultra-sensitive, and his recording devices far less than ideal. Rather, he may sit home in a full-scale laboratory with the most sophisticated equipment he can assemble and, with plenty of time and no danger carry out his attack. But, so far, we seem to be all right. For several years, we have had SIGINT stations collecting samples of U.S. cipher transmissions containing possible anomalies and forwarding them here for detailed examination. We have no proven case of operational traffic jeopardized this way. ▢

25X3, E.O.13526

I believe we've talked enough about the difficulties we face.

In late 1956, the Navy Research Laboratory, which had been working on the problem of suppressing compromising emanations for some years, came up with the first big breakthrough in a suppression technique. The device they produced was called the NRL Keyer, and it was highly successful. After being confronted with the shortcomings of shields and filters and maskers, they said, "Can we find a way of eliminating these offending signals at their source? Instead of trying to bottle up, filter out, shield, mask, or encapsulate these signals, why not reduce their amplitudes so much that they just can't go very far in the first place? Can we make these critical components operate at one or two volts instead of 60 or 120, and use power measured in microamps instead of milliamps?" They could, and did. NSA quickly adopted this low-level keying technique and immediately produced several hundred one-time tape mixers using this circuitry, together with some nominal shielding and filtering. The equipment was tested, and components that previously radiated signals which were theoretically exploitable at a half mile or so could no longer be

detected at all beyond 20 feet. The next equipment built, the KW-26, and every subsequent crypto-equipment produced by this Agency contained these circuits, and a great stride had been made.

But we weren't out of the woods yet: the communicators insisted that the reduced voltages would give reduced reliability in their equipments, and that while satisfactory operation could be demonstrated in a simple setup with the crypto-machine and its input-output devices located close by, if the ancillaries were placed at some distance ("remoted" they call it), or if a multiplicity of ancillaries had to be operated simultaneously from a single keyer, or if the low level signals had to be patched through various switchboard arrangements, operation would be unsatisfactory. The upshot was that in the KW-26 and a number of other NSA machines, an "option" was provided—so that either high-level radiating signals could be used or low-level keying adopted. In the end, almost all of the installations were made without full suppression. Even the CRITICOM network, the key intelligence reporting system over which NSA exercises the most technical and operational control, was engineered without full-scale, low-level keying.

The next difficulty we found in the corrective action program was the great difference in cost and efficiency between developing new relatively clean equipment by incorporating good suppression features in the basic design, and in retrofitting the tens of thousands of equipments—particularly the ancillaries such as teletypewriters—which we do not build ourselves but, rather, acquire from commercial sources. For, in addition to the need for low-level keyers, some shielding and filtering is still normally required; circuits have to be laid out very carefully with as much separation or isolation as possible between those which process plain text and those which lead to the outside world—this is the concept known as Red/Black separation, with the red circuits being those carrying classified plain text, and the other circuits being black. Finally, grounding had to be very carefully arranged, with all the red circuits sharing a common ground and with that ground isolated from any others. To accomplish this task in an already established installation is extremely difficult and costly, and I'll talk about it in more detail later when I cover the basic plans, policies, standards, and criteria which have now been adopted.

By 1958, we had enough knowledge of the problem, possible solutions in hand, and organizations embroiled to make it possible to develop some broad policies with respect to TEMPEST. The MCEB (Military Communications Electronics Board) operating under the JCS, formulated and adopted such policy—called a Joint policy because all the Services subscribed to it. It established some important points:

1. As an *objective*, the Military would not use equipment to process classified information if it radiated beyond the normal limits of physical control around a typical installation.

2. *Fifty feet* was established as the normal limit of control. The choice of this figure was somewhat arbitrary; but *some* figures had to be chosen since equipment designers needed to have some upper limit of acceptable radiation to work against.

3. NAG-1, a document produced by S2, was accepted as the standard of measurement that designers and testers were to use to determine whether the fifty-foot limit was met. This document specifies the kinds of measurements to be made, the sensitivity of the measuring instruments to be used, the specific procedures to be followed in making measurements, and the heart of the document sets forth a series of *curves* against which the equipment tester must compare his results: if these curves are exceeded, radiated signals (or conducted signals, etc.) can be expected to be detectable *beyond* 50 feet, and added suppression is necessary.

4. The classification of various aspects of the TEMPEST problem was specified.

Documents like these are important. It was more than an assembly of duck-billed platitudes; it set the *course* that the Military would follow, and laid the groundwork for more detailed policies which would eventually be adopted nationally. It had weaknesses, of course. It said nothing about *money*, for example; and the best intentions are meaningless without budgetary action to support them. And it set no time frame for accomplishing the objective. And it provided no priorities for action, or factors to be used in determining which equipments, systems, and installations were to be made to conform first.

The next year, 1959, the policy was adopted by the Canadians and UK, and thus became a Combined policy. This gave it a little more status, and assured that there would be a consistent planning in systems used for Combined communications. In that same year, the first National COMSEC Plan was written. In it, there was a section dealing with compromising emanations. This document was the first attempt to establish some specific responsibilities among various agencies of Government with respect to TEMPEST, and to lay out an orderly program of investigative and corrective action. Based on their capabilities and interest, six organizations were identified to carry out the bulk of the work. These were ourselves, Navy, Army, Air Force, CIA, and State. The plan also called for some central coordinating body to help manage the overall effort. It was also in this plan that, for the first time, there were really explicit statements made indicating that the TEMPEST problem was not confined to communications security equipment and its ancillaries, that it extended to *any* equipment used to process classified information, including *computers*.

And so, it was in about this time frame that the word began to leak out to people outside the COMSEC and SIGINT fields, to other agencies of government, and to the manufacturing world.

You may remember from your briefings on the overall organization of this Agency, that there is something called the U.S. Communications Security Board, and that very broad policy direction for all COMSEC matters in the government stems from the Board. It consists of a chairman from the Dept. of Defense through whom the Director, NSA reports to the Secretary of Defense, and members from NSA, Army, Navy, Air Force, State, CIA, FBI, AEC, Treasury and Transportation. This Board meets irregularly, it does its business mainly by circulating proposed policy papers among its members and having them vote for adoption. The USCSB met in 1960 to contemplate this TEMPEST problem, and established its first and only permanent committee to cope with it. This committee is referred to as SCOCE (Special Committee on Compromising Emanations) and has, to date, always been chaired by a member of the S Organization.

The ink was hardly dry on the committee's charter before it got up to its ears in difficulty. The counterpart of USCSB in the intelligence world is called USIB—the U.S. Intelligence Board. Unlike USCSB, it meets regularly and has a structure of permanent committees to work on various aspects of their business. One part of their business, of course, consists of the rapid processing, by computer techniques, of a great deal of intelligence, and they had been contemplating the adoption of some standardized input-output devices of which the archetype is an automatic electric typewriter called *Flexowriter* which can type, punch tapes or cards, and produce page copy, and which is a very strong radiator. In a rare action, the Intelligence Board appealed to the COMSEC Board for policy direction regarding the use of these devices and, of course, this was immediately turned over to the fledgling Special Committee. The committee arranged to have some Flexowriters and similar equipments tested. They were found, as a class, to be the strongest emitters of space radiation of any equipment in wide use for the processing of classified information. While, as I have mentioned, typical unsuppressed teletypewriters and mixers are ordinarily quite difficult to exploit much beyond 200 feet through free space, actual field tests to Flexowriters showed them to be readable as far out as 3,200 feet and, typically, at more than 1000 feet, even when they were operated in a very noisy electrical environment.

One such test was conducted at the Naval Security Station. (By the way, in case I haven't mentioned this already, the S Organization was located at the Naval Security Station, Washington D.C. until May 1968 when we moved here to Ft. Meade.) Mobile test equipment had been acquired, including a rolling laboratory which we refer to as "the Van". In S3, a device called *Justowriter* was being used to set up maintenance manuals. Our van started out close to the building and gathered in a great potpourri of signals emitting from the tape factory and the dozens of the machines operating in S3. As they moved out, most of the signals began to fade. But not the Justowriter. By the time they got out to the gas station on the far side of the parking lot—that's about 600 feet—most of the other signals had disappeared, but they could still read the Justowriter. They estimated that the signals were strong enough to have continued out as far as American University grounds three blocks away. (The solution in this case, was to install a shielded enclosure—a subject I will cover subsequently.)

In any event, the Committee submitted a series of recommendations to the USCSB which subsequently became known as the *Flexowriter Policy*. The Board adopted it and it upset everybody. Here's why: as the first point, the Committee recommended that the existing Flexowriters not be used to process classified information at all in any overseas environment; that it be limited to the processing of CONFIDENTIAL information in the United States, and then only if a 400-foot security zone could be maintained around it. Exceptions could be made if the equipment could be placed in an approved shielded enclosure, or as usual, if waivers based on operational necessity were granted by the heads of the departments and agencies concerned.

The Committee also recommended that both a "quick-fix" program and a long-range, corrective action program be carried out. It was recommended that the Navy be made Executive Agent to develop a new equipment which would meet the standards of NAG–1 and, grudgingly, DDR&E gave Navy some funds (about a quarter of what they asked for) to carry out that development. Meanwhile, manufacturers were coaxed to develop some interim suppression measures for their product lines, and the Committee published two lists: one containing equipments which were forbidden, the other specifying acceptable interim devices. This policy is still in force; but most users have been unable to afford the fixes, and have chosen to cease operations altogether, e.g., CIA, or to operate under waivers on a calculated risk basis, e.g., most SIGINT sites.

While the Committee was still reeling from the repercussions and recriminations for having sponsored an onerous and impractical policy which made it more difficult for operational people to do their job, it grasped an even thornier nettle. It undertook to take the old toothless Joint and Combined policies and convert them into a strong National policy which:

1. Would be binding on all departments and agencies of government, not just the military.
2. Would establish NAG–1 as a standard of acceptance for future government procurement of hardware (NAG–1, by the way, was converted to *Federal Standard.* (FS–222) to facilitate its wide distribution and use.)
3. Would establish a deadline for eliminating unsuppressed equipment from government inventories.

By now the governmental effort had changed from a haphazard, halting set of uncoordinated activities mainly aimed at cryptologic problems, to a multi-million dollar program aimed at the full range of information-processing equipment we use. Symposia had been held in Industrial forums to educate manufacturers about the nature of the problem and the Government's intentions to correct it. Work had been parcelled out to different agencies according to their areas of prime interest and competence; the SIGINT community had become interested in possibilities for gathering intelligence through TEMPEST exploitation. It, nonetheless, took the Committee two full years to complete the new National policy and coordinate it with some 22 different agencies. Before it could have any real effect it had to be *implemented*. The implementing directive—5200.19— was signed by Secretary McNamara in December, 1964. Bureaucracy is wonderful. Before its specific provisions could be carried out, the various departments and agencies had to implement the implementing directive within their own organizations. These implementing documents began dribbling in throughout 1965, and it is my sad duty to report that NSA's own implementation did not take effect until June, 1966.

All this makes the picture seem more gloomy than it is. These implementing documents are, in the final analysis, formalities. The fact of the matter is that most organizations, our own included, have been carrying out the intent of these policies to the best of our technical and budgetary abilities for some years.

While all this was going on in the policy field, much was happening in the technical area. First, let me cover the matter of shielded enclosures. To do so, I have to go back to about 1956 when the National Security Council got aroused over the irritating fact that various counter-intelligence people, particularly in the Department of State, kept stumbling across hidden microphones in their residences and offices overseas. They created a Technical Surveillance Countermeasures Committee under the Chairmanship of State and with the Services, FBI, CIA, and NSA also represented. This group was charged with finding out all they could about these listening devices,

and developing a program to counter them. In the space of a few years, they assembled information showing that nearly 500 microphones had been discovered in U.S. installations; all of them overseas, 90% of those behind the Iron Curtain. They examined a large number of possible countermeasures, including special probes and search techniques, electronic devices to locate microphones buried in walls, and what-have-you. Each June, in their report to the NSC, they would dutifully confess that the state-of-the-art of hiding surveillance devices exceeded our ability to find them. About the only way to be sure an embassy was "clean" would be to take it apart inch-by-inch which we couldn't afford, and which might prove fruitless anyhow, since host-country labor had to be used to put it back together again. (Incidentally, years later, we began to think we had darned well better be able to afford something close to it, for we found things that had been undetected in a dozen previous inspections.)

The notion of building a complete, sound-proof, inspectable room-within-a-room evolved to provide a secure conference area for diplomats and intelligence personnel. During these years, NSA's main interest in and input to the committee had to do with the sanctity of cryptocenters in these vulnerable overseas installations, and we campaigned for rooms that would be not only sound-proof but proof against compromising electromagnetic emanations as well. State Department developed a conference room made of plastic which was dubbed the "fish-bowl" and some of them are in use behind the Curtain now. CIA made the first enclosure which was both "sound-proof" and electrically shielded. This enclosure went over like—and apparently weighed about as much as—a lead balloon. It was nicknamed the "Meat Locker" and the consensus was that nobody would consent to work in such a steel box, that they needed windows and drapes or they'd get claustrophobia or something. Ironically, though, it turned out that some of the people who were against this technique for aesthetic reasons spent their days in sub-sub basement areas with cinder-block walls and no windows within 50 yards.

The really attractive thing about the enclosures, from the security point of view, was the fact that they provided not only the best means, but the only means we had come across to provide really complete TEMPEST protection in those environments where a large-scale intercept effort could be mounted at close range. So, despite aesthetic problems, and weight, and cost, and maintenance, and enormous difficulties in installation, we campaigned very strongly for their use in what we called "critical" locations, with Moscow at the top of the list.

So again, in the matter of Standards, NSA took the lead, publishing two specifications (65-5 and 65-6) one describing "fully" shielded enclosures with both RF and acoustic protection; the other describing a cheaper enclosure providing RF protection only. And by threats, pleas, "proofs" and persuasion, we convinced the Department of State, CIA, and the Services, to procure a handful of these expensive, unwieldy screen rooms for installation in their most vulnerable facilities. One of the first, thank goodness, went into Moscow—in fact, two of them; one for the Dept. of State code room as they call it, and one for the cryptocenter used by the Military Attaches. So, when highest levels of government required us to produce damage reports on the microphone finds there, we were able with straight faces and good conscience to report that, in our best judgment, cryptographic operations were immune from exploitation—the fully shielded enclosures—were in place.

But none of us was claiming that this suppression measure was suitable for any wide-scale application—it's just too cramped, inflexible, and expensive. We have managed to have them installed not only in overseas installations where we are physically exposed but also in a few locations here at home where the information being processed is of unusual sensitivity. Thus, the Atomic Energy Commission acquired more than 50 of them to house computers and their ancillaries where a heavy volume of Restricted Data must be processed; we have one here in S3 to protect most of our key and code generation equipment—a $134,000 investment, by the way—which you may see when you tour our production facilities. The Navy has one of comparable size at the Naval Security Station for its computers. (But they have the door open most of the time.) At Operations Building No. 1, on the other hand, we don't have one—instead, we use careful environmental controls, inspecting the whole area around the Operations Building periodically, and using mobile equipment to examine the actual radiation detectable in the area.

In about 1962, two more related aspects of the TEMPEST problem began to be fully recognized. First, there was the growing recognition of the inadequacies of suppression effort which were being made piece-meal, one equipment at a time, without relating that equipment to the complex of ancillaries and wiring in which it might work. We called this the "system" problem. We needed a way to test, evaluate, and suppress overall secure communications complexes, because radiation and conduction difficulties stem not only from the inherent characteristics of individual pieces of machinery but also from the way they are connected to other machines—the proximity and conductivity and grounding arrangements of all the associated wiring often determined whether a system as a whole was safe. And so, one of the first systems that we tried to evaluate in this way was the COMLOGNET system of the Army. This system, using the KG–13, was intended principally for handling logistics data and involved a number of switches, and data transceivers, and information storage units, and control consoles. Using the sharpest COMSEC teeth we have, our authority for reviewing and *approving* cryptoprinciples, and their associated rules, regulations, and procedures of use, we insisted that the system as a whole be made safe from the TEMPEST point of view before we would authorize traffic of all classifications to be processed. This brought enough pressure to bear on the system designers for them to set up a prototype complex at Ft. Monmouth and test the whole thing on the spot. They found and corrected a number of weaknesses before the "system" approval was given. A second means we have adopted, in the case of smaller systems, like a KW-7 being used with a teletypewriter and a transmitter distributor, is to pick a relatively small number of most likely configurations to be used and test each as a package. We clean up these basic packages as much as is needed and then approve them. If a user wants to use some less common arrangement of ancillaries, he must first test it. So, in the case of KW-7, we took the three most common teleprinters—the MOD-28 line of Teletype Corporation, the Kleinschmidt (an Army favorite), and the MITE teleprinter; authorized the use of any of these three combinations and provided the specific installation instructions necessary to assure that they would be radiation-free when used. We did the same thing with the little KY-8, this time listing "approved" radio sets with which it could be safely used.

Adequate systems testing for the larger complexes continues to be a problem—one with which S4, S2, DCA, and the Special Committee are all occupied.

The second and related problem that reared its head in about 1962 is the matter of RED/BLACK separation that I mentioned. Over the years, it had become increasingly evident that rather specific and detailed standards, materials, and procedures had to be used in laying out or modifying an installation if TEMPEST problems were to be avoided, and the larger the installation, the more difficult proper installation became—with switching centers perhaps the most difficult case of all. For some years, NSA has been making a really hard effort to get other organizations to display initiative and commit resources to the TEMPEST problem. We simply could not do it all ourselves. So we were pleased to cooperate with DCA when it decided to tackle the question of installation standards and criteria for the Defense Communications System (DCS). It was needed for all three Services; the Services, in fact, actually operate DCS. Virtually every strategic Department of Defense circuit is involved—more than 50,000 in all. DCA felt that this system would clearly be unmanageable unless the Services could standardize some of their equipment, communications procedures, signalling techniques, and the like. General Starbird, who directed DCA, was also convinced that TEMPEST is a serious problem, and desired the Services to use a common approach in DCS installations with respect to that problem. Thus, DCA began to write a very large installation standard comprising a number of volumes, and laying out in great detail how various circuits and equipments were to be installed. NSA personnel assisted in the technical inputs to this document called DCA Circular 175-6A. A Joint Study Group was formed under DCA chairmanship to coordinate the installation problem as well as a number of other TEMPEST tasks affecting the Defense Communications System and the National Communications System (NCS) which interconnects strategic civil organizations along with the Defense Department. In developing the installation standards, the study group and DCA took a rather hard line, and specified tough requirements for isolating all the RED circuits, equipments, and areas from the BLACK ones, i.e., assuring

physical and electrical separation between those circuits carrying classified information in the clear, and those carrying only unclassified information (like cipher signals, control signals, power, and ordinary telephone lines). In addition to shielding and filtering, this called for the use of conduits and often, in existing installations, drastic rearrangement of all the equipment and wiring was involved.

You will remember that the Department of Defense had *directed* that extensive TEMPEST corrective action be taken. I said that the Directive specified NAG–1 (FS–222) as a standard of acceptance for new equipment. It also mentioned a number of other documents as being applicable, and particularly, this very same DCA Circular I've just been describing.

As this whole program gathered steam, the monetary implications began to look staggering; the capability of the government accomplishing *all* the corrective action implied in a reasonable time seemed doubtful: furthermore, we were beginning to see that there were subtle inter-relationships between different kinds of countermeasures; and that some of these countermeasures, in particular situations, might be quite superfluous when some of the other countermeasures were rigidly applied. Remember, by now we had been telling people to shield, to filter, to place things in conduit, to ground properly, to separate circuits, to use low-level keying, to provide security zones and sometimes, to use shielded enclosures. It took us a while to realize some fairly obvious things, for example, if you have done a very good job of suppressing space radiation, you may not need very much filtering of the signal line because there's no signal to induce itself on it; or you may not need to put that line in conduit for the same reason. If you have put a line in conduit, which is a kind of shielding, then perhaps you don't have to separate it very far from other lines because the conduit itself has achieved the isolation you seek. And so forth. We had already realized that some installations, inherently, have fewer TEMPEST problems than others. The interception of space radiation from an equipment located in a missile silo or SAC's underground command center does not seem practicable; so perhaps the expensive space radiation suppressions ought not be applied there. Similarly, the suppression measures necessary in an airborne platform or in a ship at sea are quite different from those needed in a communications center in Germany.

The upshot was that, in 1965, NSA undertook to examine all the standards and techniques of suppression that had been published, to relate them to one another, and to provide some guidelines on how the security *intent* of the "national policy" and its implementing directives could be met through a judicious and *selective* application of the various suppression measures as a function of installation, environment, traffic sensitivity, and equipment being used. These guidelines were published as NSA Circular 90–9 and have been extremely well received.

In December 1970, the U.S. TEMPEST community introduced new TEMPEST laboratory test standards for non-cryptographic equipments. Test procedures for compromising acoustical and electromagnetic emanations were addressed in two separate documents. These laboratory test standards were prepared by SCOCE and superseded FS–222. They were approved by the USCSB and promulgated as Information Memoranda under the National COMSEC/EMSEC Issuance System. NACSEM 5100 is the Compromising Emanations Laboratory Test Standard for Electromagnetic Emanations and NACSEM 5103 is the Compromising Emanations Laboratory Test Standard for Acoustic Emanations. These documents are intended only to provide for standardized testing procedures among U.S. Government Departments and Agencies. They were in no way intended to establish standardized TEMPEST suppression limits for all U.S. Government Departments and Agencies. Under the terms of the USCSB's National Policy on Compromising Emanations (USCSB 4–4), U.S. Government Departments and Agencies are responsible for establishing their own TEMPEST programs to determine the degree of TEMPEST suppression which should be applied to their information-processing equipments.

In January 1971, NSA published KAG–30A/TSEC, Compromising Emanations Standard for Cryptographic Equipments. This standard represented our first effort to establish standardized testing procedures and limits for controlling the level of compromising emanations from cryptographic equipments.

DCA Circular 175-6A was superseded by DCA Circular 300-175-1 in 1969, which in turn was replaced by MIL HDBK 232 on 14 November 1972.

Before I summarize the TEMPEST situation and give you my personal conclusions about its security implications, I should make it clear that there are a number of topics in this field which comprise additional problems for us beyond those I've talked about at length. There are, for example, about a half-dozen phenomena beyond the eight I described to you; but those eight were the most important ones. I have hardly touched on the role of industry or on the program designed to train manufacturers and mobilize their resources to work on the problem. I have mentioned on-site empirical testing of operating installations only in the case of Fort Meade—actually, each of the Services has a modest capability for checking out specific installations and this "mobile test program" is a valuable asset to our work in correcting existing difficulties. For example, the Air Force, Navy, and ourselves have completed a joint survey of the whole signal environment of the island of Guam. As you know, B52 and many Navy operations stage there. As you may not know, a Soviet SIGINT trawler has loitered just off-shore for many months. Are the Soviets simply gathering plain language communications, or are they able to exploit compromising emanations?

Another problem area is the matter of providing guidelines for the design of complete new government buildings in which they expect to use a good deal of equipment for processing classified information. How do we anticipate the *TEMPEST* problems that may arise and stipulate economical means for reducing them in the design and layout of the building itself? We consult with the architects for new federal office buildings, suggesting grounding systems and cable paths that will minimize TEMPEST suppression cost when they decide to install equipment.

Finally, equipment designers face some specific technical difficulties when certain kinds of circuits have to be used, or when the system must generate or handle pulses at a very high bit rate. These difficulties stem from the fact that these pulses are characterized by very fast "rise-times". They peak sharply, and are difficult to suppress. When this is coupled with the fact that on, say, a typical printed circuit board, there just isn't room to get this physical separation between lots of wires and components that ought to be isolated from one another, then mutual shielding or electrical "de-coupling" is very difficult. R&D has published various design guides to help minimize these problems, but they continue to add cost and time to our developments. With crypto-equipment, problems can be particularly acute because, almost by definition, any cryptomachine forms an interface between RED (classified) signals, and BLACK (unclassified) ones, for you deliver plain text to it, and send cipher text out of it—so the notion of RED/BLACK signal separation gets hazy in the crucial machinery where one type of signal is actually converted to the other.

SUMMARY

We have discussed eight separate phenomena and a host of associated problems. We have identified a number of countermeasures now being applied, the main ones being the use of low-level keying, shielding, filtering, grounding, isolation, and physical protective measures. We have traced a program over a period of more than 20 years, with almost all the advances having been made in the last decade, and a coherent national program having emerged only in the past few years. My own estimate of the overall situation is as follows:

1. We should be neither panicked nor complacent about the problem.

2. Such evidence as we have been able to assemble suggests that a few of our installations, but very few of them, are probably under attack right now. Our own experience in recovering actual intelligence from U.S. installations under field conditions suggests that hostile success, if any, is fragmentary, achieved at great cost and—in most environments—with considerable risk.

3. There remain a number of more economical ways for hostile SIGINT to recover intelligence from U.S. communications entities. These include physical recovery of key, subversion, and interception and analysis of large volumes of information transmitted in the clear. But during the next five years or so, as our COMSEC program makes greater and greater inroads on these other weaknesses, and especially as we reduce the amount of useful plain language available to hostile SIGINT, it is logical to assume that that hostile effort will be driven to other means for acquiring

intelligence as more economical and productive, including increased effort at TEMPEST exploitation. Already, our own SIGINT effort is showing a modest trend in that direction. As knowledge of the phenomenon itself inevitably proliferates, and as techniques for exploitation become more sophisticated because of ever-increasing sensitivity of receivers, heightening fidelity of recording devices, and growing analytical capabilities, the TEMPEST threat may change from a potential one to an actual one. That is, it will become an actual threat *unless* we have been able to achieve most of our current objectives to suppress the equipments we will then have in our inventory and to clean up the installations in which those equipments will be used.