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

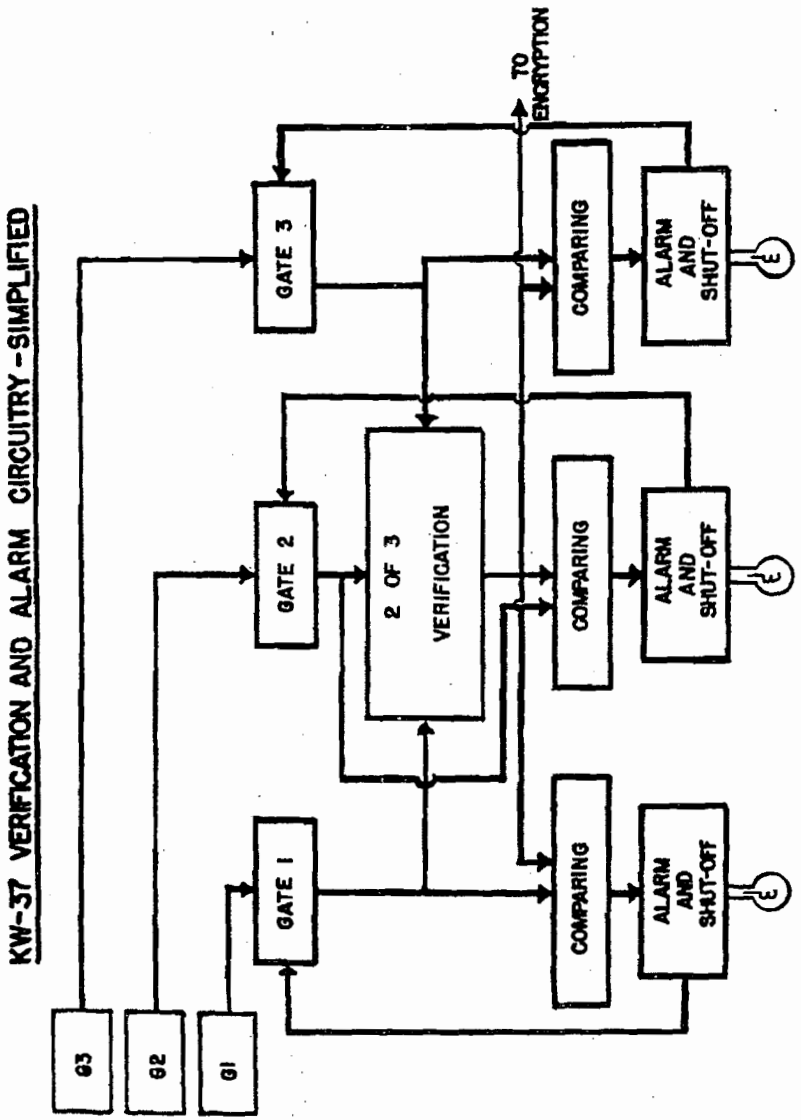
-epth"; and the thing that provides the analyst a means for successful attack is the fact that the identical element of key underlies two different cipher characters. To frustrate this kind of an attack on the KW-26, the designers made it so that it produces 32 times as much key as it needs: only one 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.

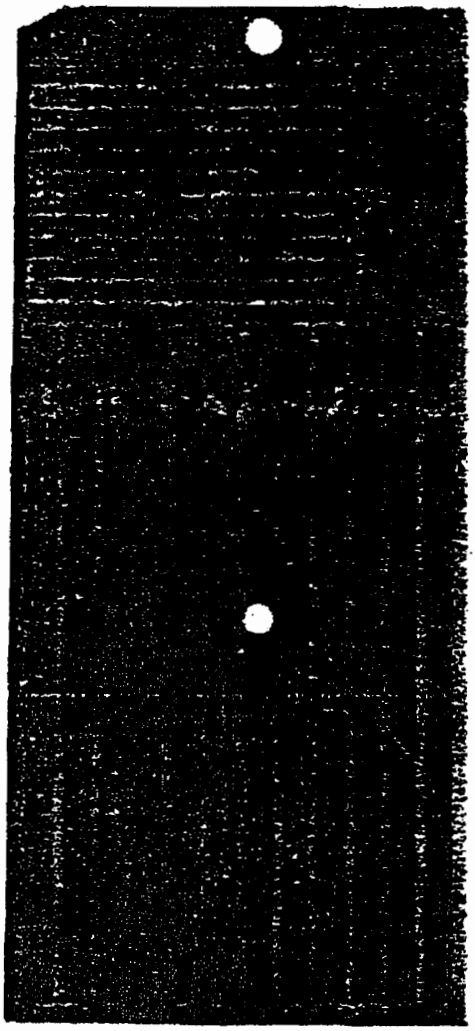
There is yet another difficult requirement associated with broadcast operations: that is that the transmitting equipment must be ultra-reliable. Once it gets going, it can't afford to stop. There are both security and operational reasons for this. In ordinary on-line TTY operations, obvious faults in 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
TO ENCRYPTION
G3
G2
G1
GATE 1
GATE 2
GATE 3
2 OF 3 VERIFICATION
COMPARING
COMPARING
COMPARING
ALARM AND SHUT-OFF
ALARM AND SHUT-OFF
ALARM AND SHUT-OFF

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-1G/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 teletypewriter 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 message 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 equipment. 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 military characteristics. They will send these MC's to NSA and either ask NSA to build such an equipment, 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 handmade "breadboard" models in their own laboratories and finishing with a full development contract 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 frustrating 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.