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 teletypewriter 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.