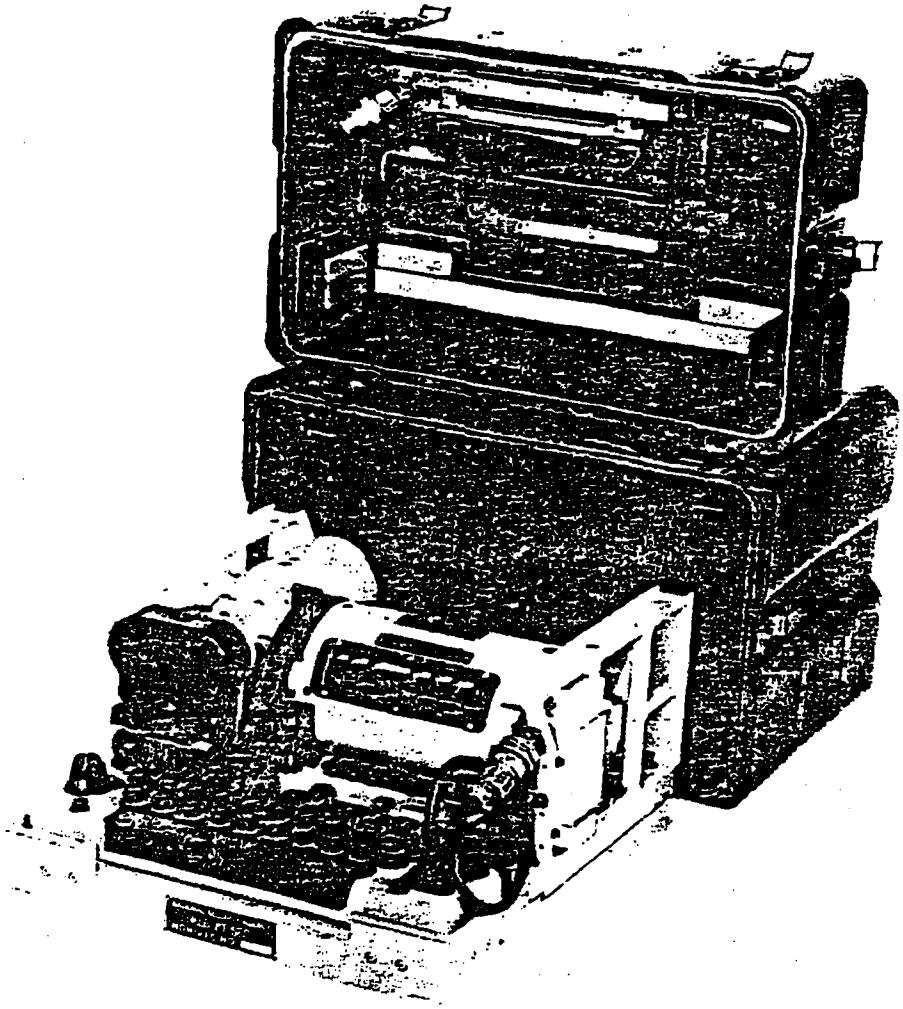
THIRD LECTURE: TSEC/KL-7

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

011001001110010010, etc.

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

[redacted]"Off-line" is the term we use to mean that the machine is not connected directly to the transmission path; be it a wire line or a radio transmitter. The cipher message is *handed* to a communicator 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 hieroglyphics I have used on you, and you out to be aware that it is fairly systematic and formalized.

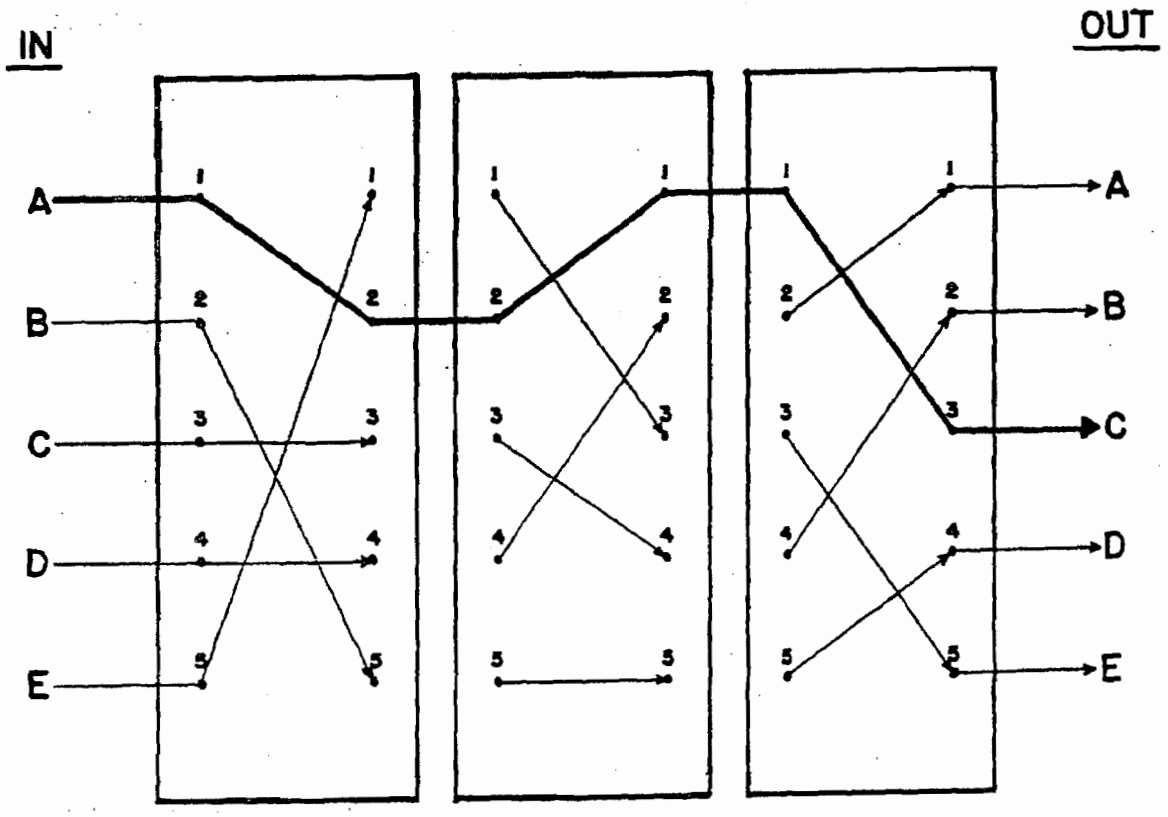
TSEC/KL-7 is the short title for the machine. The long or spelled out title is: "Electromechanical Literal Cipher Machine." TSEC is an abbreviation for Telecommunications Security which in turn is a full formal expansion of the term "Communications Security" or "COMSEC." There are only two important 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 instead, 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 itself. We have something, in fact, called the "HL-1" which permits direct decryption of text in teletypewriter 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/[redacted]

[redacted]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 depending 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 electrical commutators called *rotors* to form a fabulous and ever-changing set of electrical paths—a labyrinth or maze—through which electrical pulses could flow.

SIMPLE THREE-ROTOR MAZE



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 26^4 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.