TENTATIVE LIST OF ENIGMA AND OTHER MACHINE USAGES

Contents

NAVAL ENIGMA

At any one time, a 4-wheel machine uses a fixed reflector, a hand-set wheel, and three moving wheels. There are 2 reflectors, 2 fixed wheels and eight moving wheels available. This allows 2 x 2 x 8 x 7 x 6 = 1344 different wheel orders. The wheel order for the three moving wheels is changed every second day. The fixed wheel and reflector combination is changed monthly. Five of the eight moving wheels are single-notchers while the other three have two notches each. The stepping is of the Enigma type. The rings can be set arbitrarily.

The Stecker is reciprocal and is changed at short intervals. The changes occur daily in the regular problem and either every two or every ten days in the double encipherment problem (Offizier).

Most of the lines of traffic use indicators which are related to the message settings by means of bigram substitution and encipherment at grund, but one system still has indicators which show a throw-on structure. The inner settings for ordinary double encipherment are in sets of 26, designated by the 26 letters of the alphabet, which change monthly. Special settings are occasionally used and, in the case of the Sonderschluessel problem, special steckers, wheels and rings employed.

Most of the Naval traffic has been read currently and completely for about a year and a half. The regular daily problem requires ordinary bombe runs and either grenade run or catalog search. The double-enciphered messages make use of bombes, hype, and bull-dozer. The traffic with the throw-on structure can be handled by means of the 32-unit bombes. If any new reflectors or pluggable reflectors are ever introduced, then Duenna will make it possible to recover the wiring, provided, of course, there is a good crib available.

The present equipment seems to be adequate for all the Naval problems which have arisen so far except, possibly, the Sonderschluessel.

GERMAN ARMY AND AIR FORCE ENIGMA

The machine itself, except for modifications introduced during 1944, is exactly the same as the Naval 3-wheel model. It uses any three out of five wheels, these being the five single-notch Naval wheels with settable rings. It has a fixed reflector (Unkehrwalz "B", same as Naval). The Stecker is pluggable, and, as on the Naval machine, necessarily reciprocal.

During 1944 a pluggable reflector ("D") was gradually introduced, and is now widespread though not yet universal. Some Air Force keys, e.g. Jaguar, have a device called Enigma Uhr which can be attached to the Stecker board; by setting it in any one of 40 positions, 40 (mostly non-reciprocal) Steckers can be produced from the one plugged up for the day.

Whee1-order and Ringstellung usually changes daily (rather than two-daily), as well as Stecker. On some keys, the daily wheel-order is changed cyclically after eight-hour periods. The pluggable reflector is usually changed about every ten days.

There are more keys than in the Navy - about 50 Air and 40 Army keys have been identified. Up to the Fall of 1943, these were distinguishable by external discriminants. Double encipherment is used only as an emergency measure.

A six-letter indicator is used. If, for example, XVE JLG is received, the operator sets his machine at XVE and deciphers JLG, the result being the message setting. "Cillis" are produced by the tendency on the part of the encipherer (1) to take the final setting of one message as the "Grund" (XVE in the example) of the next, and (2) to choose "keyboards" (like PYX, ASD, etc. - adjacent keyboard letters) for message settings.

If the reflector is known, the usual attack is by 3-wheel bombe, using a medium length crib or a menu derived from Cillis. If the reflector is unknown, it may be recovered by means of a long crib (4 to 8 lines of 26 letters) by (1) hand "5tecker-knock-out" method, (2) Duenna, (3) Autoscritcher, or (4) Giant. If the Uhr is used, these "D-methods" are unaffected, since they do not assume Stecker reciprocity. But for a bombe run with known reflector, the diagonal board must be dispensed with.

With known wheel-order, Ringstellung, and Stecker, the setting of a message can be determined as follows. If a short crib is available by (1) hand rodding and catalog, (2) click machine (Br.), (3) grenade (Br. "Eel"). If no crib is available, by (1) "Eins" catalog (Br.), (2) Hypo, (3) Bull-dozer, (4) Dud-buster (Army). Bull-dozer could be used even without known Stecker.

Should long cribs for Duenna become unavailable, a device for breaking Dora on a medium length crib would be desirable. 30 letters or crib is strong enough cryptographically to determine it. Should even medium cribs become unavailable, a statistical Duenna would be desirable, perhaps able to make use also of a short crib. How long a message would be necessary to develop sufficient cryptographic strength has not been computed.

A number of minor German systems have employed Enigma machines. The German Armistice Commission in unoccupied France and in French North A£rica has a ll-l5-l7 machine. Another machine using three single-notch wheels was used by the German railway traffic organization in Northern France. There were probably many other such usages, but they all seem to be only minor variants of standard systems and no special discussion will be given here. These problems have been British for the most part, since they intercept the traffic.

(AES note: Br. means British)

COMMERCIAL TYPE MACHINES

The Spanish Military Attaches and the Spanish Naval Attaches apparently are equipped with Enigma machines with three single-notch wheels, a movable reflector, a fixed QWERTZU input sequence and enigma stepping. Present techniques on bombes and hypo were satisfactory about eight months ago when a new key list went into effect. Since January 1, 1945, traffic has vanished to practically nothing. In the past, poor cryptographic usage of the Naval Attache Machine has enabled the recovery of the wheel wirings from scratch. (British).

There is reason to believe that some years ago the Swiss Government acquired some of the commercial enigma machines with three single-notch wheels, a movable reflector, a fixed QWERTZU input sequence, and enigma steppinge About every two years (this time limit is a guess) the Swiss rewire the three movable wheels. Present techniques on bombes and hypo units are satisfactory for reading current traffic. In the past, poor cryptographic usage has enabled the recovery of wheel wirings from scratch. (Coast Guard and probably U. S. Army). lately this problem has been a U. S. Army Signal Corps problem.

In the past the Coast Guard has worked on German Agent Systems with three single-notch wheels, a movable reflector, a fixed QWERTZU input sequence and enigma stepping. In the summer of 1944 there was some traffic in a system employing the first three so-called service wheels and a variable reciprocal input sequence. In all of these cases, however, present operational equipment and procedures have been sufficient to read the traffic.

MULTIPLE NOTCH MACHINE

ll-15-17 Machines (Coast Guard). At least three types of the ll-l5-l7 machines have been used. These machines in addition to the three multiple-notch wheels have a reflector which is mechanically stepped, a fixed QWERTZU input sequence and cyclometric rather than enigma stepping. For these multiple notch machines, as many as 61 (out of the theoretical maximum of 64) grenade runs may be necessary to exhaust all of the possible stepping sequences for a four letter crib. Modified techniques on hypo (using hypo as a grenade) have been used on this type problem, and another procedure makes the required number (from 37 to 61) of grenade runs on a four letter crib. At times, knowledge of the ring positions which determines the stepping sequence is available - but little or no use of this can be made on the bombes. In the opinion of the writer, present high speed equipment represents a makeshift rather than an ideal approach to this problem. A click machine, a new type of grenade, and a new type of bombe with greatly increased turn-over possibilities have been proposed to aid in the attack on this problem. A pluggable stecker sequence would greatly complicate this problem.

New K.D. Machine (Coast Guard). About January 1945 a new Enigma machine with three (chosen from a set of six) nine-notch wheels appeared. The machine has the fixed QWERTZU input sequence, enigma stepping and a pluggable (Dora) reflector. Attacks on Duenna are possible but the nine-notch pattern will complicate the problem. A pluggable stecker sequence would greatly complicate this problem.

T Machine. In the summer of 1944 a number of the so-called T machines were captured in a warehouse in Normandy. These machines had been built for the Japanese, and used three (from a set of eight) five-notch wheels, a movable reflector, a fixed non-reciprocal input sequence and enigma stepping. No positively identified traffic has appeared in this system - although early in 1945 exhaustive runs were made on two cribs placed at the beginning of two messages suspected of having been enciphered on the T machine. For four letter cribs, 8 (out of a theoretical maximum of 64) grenade runs must be made to cover all the types of stepping sequences. If the T machines were equipped with a variable stecker, an extremely large

number of the present machines would be needed or a radical departure in design (particularly with respect to the steppin~ mechanism) would be necessary to adequately attack the problem.

Dutch Usage. The Dutch Navy uses enigma machines in some of its traffic circuits. There is reason to believe that they use a 11-15-17 machine, but no traffic in the system has been read to date. L8ck of cribs make usual bombe techniques unavailable - the multiple turn-over features would make a statistical bombe approach (for known wiring) a long procedure.

CSP 1515

The CSP 1515 is a machine which produces additives applicable to messages on teletype tape. For a given setting of the machine current enters at five fixed input points and passes through five wired wheels. Fifteen of the output points, in five groups of three are wired to five relays. Each relay is associated with one of the levels on the teletype tape. If current reaches the relay the component appearing on the message tape is reversed as it goes to the cipher tape, a mark becoming a space or a space becoming a mark. If no current reaches the relay, the component on the cipher tape will be the same as the component on the message tape. In this way, an additive modulo 2 is applied to each component of the message tape and incidentally decipherment is the same operation as enciphermente

Five wheels of standard 26 wire type are used at a time. They are chosen from a set of ten and may be inserted straight or in reverse, permitting 967,680 wheel orders. Any one of the five wheels may be designated as the fast wheel, stepping every time. Any other may be made the middle, stepping every twenty-six letters, and a third made the slow wheel, stepping once every 676 times. The other two wheels step in a manner dependent on the additive produced. When the first three relays all receive current simultaneously, the fourth wheel steps and when the last two relays both receive current, the fifth wheel steps. There are no settable rings and no stecker.

A grenade run could be made on a known wheel order, though several runs would be needed to cover the 120 different motions. No other existing equipment appears to be applicable.

THE CCM

The CCM is a wire wheeled enciphering machine. Ezicipherment is through a normal alphabet input, one-way through five wheels, and through a normal alphabet output. Each side of each wheel has an even number of notches, from eight to sixteen. Let us number the wheels 1, 2, 3, 4, 5 from left to right. The middle wheel (#3) steps every time. Wheel 4 moves under the influence of the notches on the right side of wheel 3, and wheel 5 under the influence of the notches on the right side of wheel 4. Similarly, 2 is influenced by the left notches of 3 and 1 by the left notches of 2. A wheel steps if and only if a notch of its governing wheel is in the active position. The five wheels are chosen from a set of ten and may be inserted straight or in reverse. There are thus 20 x 18 x 16 x 14 x 12 = 967,680 wheel orders.

For a known wheel order, the attacks are relatively simple and could be run on a grenade, on Hypo, or by IBM techniques. No equipment and no mode of attack are known for unknown wheel orders, at least in any operational sense.

JAPANESE MACHINES

The Japanese have used 4 electric circuit cipher machines, the Red, the Purple, the Coral and the Jade.

The Red was formerly used on diplomatic channels. In this machine, the circuits were divided into two sections, one of six circuits and the other of twenty. The sections were handled separately by two commutator wheels which effected a simple progressive vigenere substitution. The period of the encipherment was 60, since both commutators stepped after each encipherment. In addition there was an interrupter wheel of period 47, which caused the commutators to skip certain positions

The letters were attached to the circuits by a pluggable sequence which was the same at both ends. However, there was an additional feature which scrambled the plugging further. The details of this additional scrambling have never been completely recovered. This problem is no longer current.

The Purple was introduced to replace the Red on many diplomatic channels, and is still current. The circuits are divided into groups of 6 and 20. The substitutions are effected by telephone selectors. (A telephone selector is a device which applies, in different positions, 25 unrelated substitutions). The six-bank has overall period of twenty five, the circuits traversing just one telephone selector, which steps at every encipherment. The other twenty circuits traverse a sequence of three telephone selector banks. The stepping of these other banks is quasi-metric of a distinctive type, and has 6 variations. Any bank can be made fast, slow or medium speed.

The input and output are independently pluggable, but, in practice, the sequences have always been the same or related.

Cryptanalytically, the machine can be attacked by breaking out the six-bank and cribbing. The letters of the six bank betray themselves by frequency count. Since there is a setting list of 240 starting points and motions, and an almost completely recovered book of 1000 sequences which are used in a systematic fashion, the traffic is read currently without much cryptanalysis. No special cryptanalytic machinery is necessary.

Coral is a machine used by various Naval Attaches. The traf-nc is known as JNA20. It is a three bank 26 circuit tele-phone selector machine. The stepping is strictly metric and only 3 or the 6 possible orders or motion are used. The pluggable sequence is the same at both ends.

The machine is stronger than the Purple cryptanalytically because there is no six-bank, but fortunately the usage is weak. A small setting list (15 settings per originator ex-cept Tokyo which has 30) is in effect for a year at a time, so that the problem of simultaneous stecker and setting re-covery arises only rarely. This problem, which is very dif-ficult has been handled by hand, using symmetric sequences or other ravorable breaks.

Mike has been used to assist in sequence recovery when the setting is known. I.C. machinery has been successful in find-ing settings when the sequence is known. Rattler has been equipped to handle short cribs when the sequence is known.

Jade is a machine used on a rleet operational system. The traffic is known as JN157. It is a 5-bank 25-circuit tele-phone selector machine. Only the first three banks step (counting from the plain text side), and they have a strictly metric motion using only three of the six orders of motion. The 4th and 5th banks are only hand set.

The circuits are used doubly. There are 50 kana used, two for each circuit, an upper and a lower case. Upper case characters encipher as upper case; lower case encipher as lower case. The plug board is on the cipher side only.

The system uses a small setting list, but there are a great number of channels. Plug sequences remain in effect for 10-day periods.

The use or upper and lower case makes cribbing fairly easy. Sequence recovery with known setting can be handled by means similar to those for Coral. Rattler is a grenade for this system which determines the setting for a message when the sequence and a six-letter crib are given.