Copy 8 of 8 copies. 12

MOST SECRET

CX/mmd

3365

SUBJECT: Fish Notes — Report #F 5
TO : CO, SSA, War Dept. — 18 March, 1944

1. One of our men, Sgt. Vergine, has commenced work in the Fish section and is receiving a course of training. I am planning to participate in this course to some extent and to report on what I think significant. These reports may duplicate earlier ones and will, in many cases, include information and procedures well known at A. H. However, they may be useful as a basis for a course of training, as a means of standardizing terminology and conventions, and as an orderly presentation of solution techniques. This traffic is deemed of the utmost importance and I feel sure the British will welcome any assistance we can offer.

2. Trainees, after receiving instruction in the machine and its operation, are required to memorize the Baudot code. The people working on hand methods of solution find it necessary to memorize all combinations of pairs of letters, that is, the full 32 x 32 square. Others are provided with copies of the square and are also taught the following simple technique:- place the fingers of one hand on a table, fingers touching the surface representing dots and those raised representing crosses - then switch each finger corresponding to a cross in the letter to be combined. The result is read from the new finger positions.

3. Nomenclature, Symbols and Conventions

The British use the words dot and cross instead of our dit and x. Their elementary symbols are as follows:

P = Plain text
Z = Cipher text
K = Total key
χ = Chi
ψ = Psi

All of these are used with subscripts to denote a particular impulse. The subscript i denotes a single impulse without specification and similarly ij designates some pair.

Extended Psi is symbolized by ψ' and $\bar{\psi}$ and they call it ψ^{i} dash, not Psi prime.

The motor wheels are called $\mu 37$ and $\mu 61$ and their combination is called M_g. The actual or total motor results from M_g and any limitations which may be present and is called M_T.

In writing out patterns the current convention is to say that the ψ impulse looks at the motor symbol immediately above it to see what to do next. In other words, each motor symbol represents what happens between the encipherment of the impulse directly below it and the next one to the right. Differenced patterns (which they designate by Δ as we do) are written under the first of the two differenced elements. Then, when the motor pattern is written above the

ARMY

MOST SECRET

Report #F 5 (continued)

△ pattern each motor element represents motor action (or inaction) between the two elements represented by the △ symbol immediately below it.

These conventions make it unnecessary to do any staggering at the beginning of the message or to adopt artificial notions to the effect that the motor comes into play only after the first few letters. All patterns start in a single vertical line. With these conventions the X_2 limitation acts on the motor impulse one ahead and the P_5 limitation acts two ahead. These limitations are represented by $\overline{X}_2$ and P_5 but the former is more accurately written $\overline{\overline{X}}_2$. This simply means that the pattern must be inversed before determining its effect on M_3. For example:-

$\overline{\overline{X}}_2$	.xx..x.xx..x.
$\overline{\overline{X}}_2$	.xx..x.xx..x
$\overline{X}_2$	.x..xx.x..xx.
P_5	.x.x..x.xx.x.
$\overline{P}_5$	..x.x..x.xx.
M_3	x.x.x.x..xxx.
M_T	xxxx.xxxxx.

Blanks at beginning in $\overline{\overline{X}}_2$ and $\overline{P}_5$ are filled in with dots.

Symbolically:- $M_T = M_3 \smile (\overline{\overline{X}}_2 + \overline{P}_5)$

The symbol $\smile$ designates Boolean addition, the relations of which are as follows:-

. + . = .
. + x = x
x + . = x
x + x = x

All of this is, of course, only a formalised way of saying that a motor cross is compelled if X_2 combines with P_5 to produce a dot.

4. Sgt. Vergine was required first to do some enciphering and deciphering to familiarise himself with the operations and conventions. He was then given two problems - (1) to recover M_T and all X and Ψ patterns and their settings being known and (2) to recover X_3 and Ψ_3 knowing M_T and the patterns and settings of the remaining X and Ψ wheels.

5. Additional Symbols and Elementary Formulae

Report #F 5 (continued)

D = de-chi = Z + X = P + Ψ
a = proportion of crosses in Ψ
b = proportion of crosses in ΔΨ
p(.) = probability of dot
p(x) = probability of cross

$p(.) \text{ in } \Delta\Psi_{ij} = b^2 + (1 - b^2)$

$p(.) \text{ in } \Delta\Psi'_{ij} = (1 - a) + a[b^2 + (1 - b^2)]$

It is assumed, for the foregoing relations, that b is the same for each of the Ψ wheels. Furthermore, a and b are invariably selected so that their product is approximately equal to one-half. Therefore-

$p(.) \text{ in } \Delta\Psi'_{ij} = b$

By definition-

$p(.) \text{ in } \Delta P_{ij} = 1/2 + \lambda$

Therefore-

$p(.) \text{ in } \Delta D_{ij} = (1/2 + \lambda)b + (1/2 - \lambda)(1 - b)$

$= \lambda(2b - 1)$

6. Will send additional formulae in the near future. Even though they represent nothing new it may be convenient to have them systematically compiled.

Walter J. Fried
Capt. Signal Corps