- TOP SECRET -
FOR BOSS AGENTS ONLY

TOP SECRET

TECHNICAL REPORT 1937-213A

THE SPYCLIST CIPHER CLOCK
(ADDENDUM)

Prepared for

OFFICE OF THE DIRECTOR,
BUREAU OF SECURITY AND SIGNALS INTELLIGENCE

CONTENTS

TOP SECRET

4. FACTORING THE CIPHER OF THE SPYCLIST CIPHER CLOCK

Suppose we call the ciphertext alphabets Ac (the mixed key). When we encipher a text, the ciphertext pointer points to one of the characters in Ac. It should be easy to understand that we can get the same result if the cipher clock has an unmixed ciphertext alphabet, and then we apply a monoalphabetic substitution.

Suppose we call the encryption function of the cipher clock E. It takes a plaintext P and produces a ciphertext C:

$$C = E(Ac, P)$$

Another way to write this is

$$P \rightarrow E(Ac) \rightarrow C$$

As we argued above, we can factor the cipher into a keyless cipher-clock encryptor S and a monoalphabetic substitution M.

$$C = E(Ac, P) = M(Ac, S(P))$$

Or, if you prefer:

$$P \rightarrow \ S \rightarrow M(A_C) \rightarrow C$$

The reason that we wrote the keyless cipher-clock encryptor as S is that it is actually a very simple stream cipher. It has an internal state that simply counts the total number of steps through which the hands of the device have turned. The state is initialized to zero, of course. If we call the internal state I, and identify the characters of our (unmixed) alphabets with integers (such as space=0, A=1, B=2, ...), we can understand the action of the stream cipher's encryptor as a function that implements these operations:

1. Input w_i
3. Find x_i = (w_i - I) modulo m
3. If x_i = 0, then set x_i = m
4. Add x_i to I
5. Find y_i = I modulo n
6. Output y_i

Step 3 handles double letters in the plaintext. Note that the output of the stream cipher can be viewed as an integer in the set {0, 1, ..., n} or as the yth letter of the unmixed ciphertext alphabet.