TOP SECRET

TECHNICAL REPORT 1937-213B

THE SPYCLIST CIPHER CLOCK
(SECOND ADDENDUM)

Prepared for

OFFICE OF THE DIRECTOR,
BUREAU OF SECURITY AND SIGNALS INTELLIGENCE

CONTENTS

5. Cryptanalysis of the spyclist cipher clock page 2
A. Keywords from a known list page 2
B. Partially known plaintext page 2

TOP SECRET

5. CRYPTANALYSIS OF THE SPYCLIST CIPHER CLOCK

A. KEYWORDS FROM A KNOWN LIST

This is typically the most time-consuming attack. No pun intended. The efficiency of the attack depends on the length and quality of the word list.

To use this attack, we will need to know the method of generating the key from a keyword. If we do not know the method, then we need to try all methods. See document "Standards and Practices 013" for key-generating methods known to BOSS.

To perform the attack, we try each word in our dictionary or word list. For each word we generate a key and decipher the ciphertext with it. If the resulting plaintext resembles English text, then we might conclude that we have found the correct keyword. If the decrypted text is imperfect, then we should continue, since a better solution may come later.

B. PARTIALLY KNOWN PLAINTEXT

If we know some part of the plaintext (a "crib"), we can use it to break the ciphertext. To make the attack more efficient, we will encrypt the crib with an unkeyed cipher clock before we compare it to the ciphertext, since the difference between a ciphertext and a text that was encrypted with an unkeyed device is a monoalphabetic substitution. By "unkeyed" we mean to refer to a cipher clock in which the key is an un-deranged alphabet.

Please study the following example of this attack. This ciphertext was enciphered with the spyclists' cipher clock:

```
NA+Y+ UGPJB QOCRP GEH#L HTNHD PRWKH NTNAE MYCTG TDV#M AQUXA
+VGAZ WFVRL TNYLN PRP#O MGPCU KWP+J QECRC VFTCB QGDYE OSTME
USEJR BQC#C YWANI BERBX FMUOI Q#V#N PJNJZ #MCW# MKIOJ LBDBJ
BKGXK MS+UE JVJEL YNF#A C#MYT RZSLE #CNJP EPJTG LRVIO JLPGU
OH#VM H+TYI WKXYU QOVIV GUM#M TWXTU +JHNZ HOVSC NXUGW OPGXU
FEHQF AYFXW V#RME BXFEB SZXAS IT+CT +JDTX QRQTI OJTEB +MOLP J
```

And this snippet is known to be part of the plaintext:

never wear out no matter how long it may stand

The first step is to encipher the crib with the unmixed key ABCDEFGHIJKLMNOPQRSTUVWXYZ#+ to get

NCTANS#UJEKH+AYKB+KXLS#NQNEGRIWSKLSDT

Next we compare the enciphered crib to the ciphertext, one position at a time. We begin at the beginning:

```
NA+Y+UGPJBQOCRPGEH#LHTNHDPRWKHNTNAEMYCTGTDV#MAQUXA...
NCTANS#UJEKH+AYKB+KXLS# NQNEGRIWSKLSDT
^    ^                  ^  ^
```

Notice that we have a problem: 'N' in the enciphered crib is paired with 'N', '+', 'H', and 'P' in the ciphertext. This cannot happen with a monoalphabetic substitution. Therefore we must reject this position and move to the next.

The only acceptable alignment is at position 85:

```
...CV FTCBQGDYEOSTMEUSEJRBQC#CY WANIBERBXFMUOIQ...
   NCT ANS#UJEKH+AYK B+KXLS#NQNEGRIWSKLSDT
   ^   ^                       ^ ^
```

Now, 'N' always pairs with 'C' in the ciphertext. The same is true for all other ciphertext symbols; each pairs with only one. By tabulating the pairings, we can reconstruct the key:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ#+
WONDER+CLK#ABFGHIJMPQSTUVXYZ
```

If not all pairings are present, then we must try to determine the missing pairs by trial and error.

Deciphering the full ciphertext with the reconstructed key gives us the plaintext, which you should recognize as a paragraph from The Wonder Clock by Howard and Katharine Pyle.

> CLICK BUZZ WENT THE WHEELS AND THEN TICK TOCK TICK TOCK FOR THE WONDER CLOCK IS OF THAT KIND THAT IT WILL NEVER WEAR OUT NO MATTER HOW LONG IT MAY STAND IN TIMES GARRET DOWN I SAT AND WATCHED IT FOR EVERY TIME IT STRUCK IT PLAYED A PRETTY SONG AND WHEN THE SONG WAS ENDED CLICK CLICK OUT STEPPED THE DROLLEST LITTLE PUPPET FIGURES AND WENT THROUGH WITH A DANCE AND I SAW IT ALL