CIPHERTEXT-ONLY CRYPTANALYSIS OF ENIGMA

by

James J. Gillogly

This paper orinally appeared in Cryptologia October 1995;Volume XIX, Number 4.

At the end of this paper is a link to Ralph Erskine's letter

Other Papers by Gillogly

• Cryptograms from the Crypt	• The Beale Cipher: A Dissenting Opinion
• Breaking an 18th Century Shorthand System	

ABSTRACT: Enigma messages can be solved by recovering the message key settings, the ring settings, and the plug settings individually. Recovery of the message key setting is sensitive enough to distinguish the correct rotor order. The method is demonstrated on a 647-letter message, and its performance is estimated for different message lengths and numbers of plugs used.

KEYWORDS: Enigma, cryptanalysis.

INTRODUCTION

Polish and British solutions to encrypted German Enigma traffic relied on sophisticated known plaintext attacks. The rotor wiring was known through brilliant cryptanalysis by the Polish mathematician Marian Rejewski [3] and later through capture of naval Enigma rotors [4]. Reading each day's messages required discovering the order of the three rotors (later four) selected from three, then five and finally eight possible standard rotors. The key also included the ring settings for each rotor (A-Z or 1-26), the message key settings for each rotor (A-Z or 1-26), and the positions of up to ten plugs which interchanged pairs of letters on input and output [5]. Weather reports, standardized salutations and signatures, and regularities and repetition in the selection of initial settings provided cribs for the "bombe" machines to recover daily keys for each traffic net [2]. The interested reader may refer to [5] for a detailed description of the construction and operation of the Enigma.

Deavours and Kruh [6] report that a ciphertext-only attack was considered, but "apparently never put into use, probably because of German foresight in keeping the individual message lengths to about 200 characters." In fact, this constraint on German cipher clerks was regularly violated. A rough count of English translations of Enigma solutions from the Bletchley Park cryptanalysts for two arbitrarily selected days in 1943 shows means of about 340 letters (107 messages on 6 Aug 43) and 550 letters (89 messages on 13 Nov 43). On both days several translations of over 1000 letters were forwarded from Bletchley Park: four on 6 Aug 43 and ten on 13 Nov 43 [10]. The longest were about 1500 and 2300 letters respectively. I assume the lengths of the German plaintexts were not dramatically different.

In this paper I describe a ciphertext-only attack effective for short (about 300 letter) messages with keys including up to six plugs, and for longer messages using up to ten plugs. The underlying techniques were known at the time [7], but the necessary hardware may not have been available, since it requires accumulating (in effect) squares of frequencies for each of several thousand trial plaintexts. However, it would not have been surprising for the boffins of Bletchley to cobble together a device to do something similar: the actual processing for this attack requires fewer operations and less sophistication than the bombe attack, since it does not need to try multiple cribs.

The attack exploits a weakness in the use of the plugboard: not all letters are interchanged. If we decrypt a message with the correct rotor order, ring settings, and rotor message key settings but with no plugs in the plugboard, some of the letters in the output will have their correct plaintext value: in particular, all of the letters that did not encounter a plug on the way in from the keyboard or on the way out to the lights. The number of these untouched letters will vary depending on the number of plugs in use and the length of the message. We do not know which letters in the output are correct, but if the message is long enough we can see their effect in the overall statistics of the message. Similarly, messages decrypted with partially correct ring and message key settings will have islands of plaintext that are reflected in an overall measure of redundancy.

The sample German plaintext encrypted for Figure 1 includes the three messages from [6], a signal from the Bismarck [5], and a (very) final partially-decrypted message reported by Kahn [8]. I used the original German settings of the first message in [6] to encrypt the set in one 647-letter message.

```
QKRQW UQTZK FXZOM JFOYR HYZWV BXYSI WMMVW BLEBD MWUWB TVHMR
FLKSD CCEXI YPAHR MPZIO VBBRV LNHZU POSYE IPWJT UGYOS LAOXR
HKVCH QOSVD TRBPD JEUKS BBXHT TGVHG FICAC VGUVO QFAQW BKXZJ
SQJFZ PEVJR OJTOE SLBQH QTRAA HXVYA UHTNB GIBVC LBLXC YBDMQ
RTVPY KFFZX NDDPC CJBHQ FDKXE EYWPB YQWDX DRDHN IGDXE UJJPV
MHUKP CFHLL FERAZ HZOHX DGBKO QXKTL DVDCW KAEDH CPHJI WZMMT
UAMQE NNFCH UIAWC CHNCF YPWUA RBBNI EPHGD DKMDQ LMSNM TWOHM
AUHRH GCUMQ PKQRK DVSWV MTYVN FFDDS KIISX ONXQH HLIYQ SDFHE
NCMCO MREZQ DRPBM RVPQT VRSWZ PGLPI TRVIB PXXHP RFISZ TPUEP
LKOTT XNAZM HTJPC HAASF ZLEFC EZUTP YBAOS KPZCJ CYZOV APZZV
ELBLL ZEVDC HRMIO YEPFV UGNDL ENISX YCHKS JUWVX USBIT DEQTC
NKRLS NXMXY ZGCUP AWFUL TZZSF AHMPX GLLNZ RXYJN SKYNQ AMZBU
GFZJC URWGT QZCTL LOIEK AOISK HAAQF OPFUZ IRTLW EVYWM DN
```

Figure 1. Sample Enigma ciphertext

INDEX OF COINCIDENCE

The first steps of this process require calculating the Index of Coincidence [7] of the partially-decrypted plaintext to give an estimate of how close that trial is to credible German. It is defined by:

$$IC = \frac{\sum_{i=A}^{Z} f_i(f_i-1)}{N(N-1)}$$

where f_i is the frequency in the sample text of letter i, and N is the total number of letters in the sample. For random 26-letter text the IC is approximately 0.038; standard German shows about 0.07. The IC measures the roughness of a distribution, with higher numbers rewarding distributions with higher-frequency letters.

ROTOR ORDER

The attack uses a (virtual) bank of Enigma machines, each testing one possible rotor order. In this example I test five rotors, with 60 possible arrangements. For each rotor order, set the rings at 1 1 1, leave the plugboard empty, and run through all possible initial rotor settings. This requires 26 * 26 * 26 trials; each initial setting is possible, although Enigma's period is only 26 * 25 * 26 due to a kick in the middle rotor's gallop. For each of these 17,576 starting positions, decrypt the message and calculate the IC of the result, saving the best starting position.

The six highest-ranked rotor orders by this measure are:

Order	IC	Message Key
II I III	0.0416	2 11 6
III I IV	0.0414	20 8 17
V II I	0.0413	20 16 3
II III V	0.0412	20 20 26
III I V	0.0411	19 16 20
IV I II	0.0411	4 20 7

The IC for order II I III is somewhat higher than the others at its best message key setting of 2 11 6, though still not close to the value expected for German. This step fails for short messages with many plugs: not enough redundancy survives the misalignment of ring settings and an empty plugboard to show through in the Index of Coincidence. If fewer plugs are used, a shorter message will show enough discrimination; with more plugs, more text might be necessary to determine the correct rotor order. This step dominates the cost of the attack: rotor orders * 17,576 * decryption time.

RING SETTINGS

Next we recover the best ring settings for this message key setting and the assumed rotor order. Try each possible ring setting on the fast rotor first, since it will on average affect more output characters than a bad ring setting on the middle rotor. The ring setting of the slowest rotor does not need to be changed, since it has no effect on the encryption. The rotors must stay registered with the recovered message key setting, so as each ring is moved, the trial message key setting for that rotor is moved in the same direction; thus only 26 ring/message key settings need to be tested for each rotor. We again use the Index of Coincidence to screen the candidates.

Spinning the fast rotor from the current assumed position (ring setting 1, rotor message key setting 6) and keeping the other rotors constant, we find an improved rotor/message key combination:

```
          Rotor index 2, ring  1, message key  6:  0.0416
          Rotor index 2, ring  2, message key  7:  0.0418
          Rotor index 2, ring  3, message key  8:  0.0416
   --->   Rotor index 2, ring  4, message key  9:  0.0422
          Rotor index 2, ring  5, message key 10:  0.0420
          Rotor index 2, ring  6, message key 11:  0.0416
          Rotor index 2, ring  7, message key 12:  0.0416
```

Using this position (ring setting 4, rotor message key setting 9) on the fast rotor and holding the slow rotor constant, we spin the middle rotor:

```
          Rotor index 1, ring 20, message key  4:  0.0432
          Rotor index 1, ring 21, message key  5:  0.0428
          Rotor index 1, ring 22, message key  6:  0.0437
   --->   Rotor index 1, ring 23, message key  7:  0.0440
          Rotor index 1, ring 24, message key  8:  0.0437
          Rotor index 1, ring 25, message key  9:  0.0429
          Rotor index 1, ring  0, message key 10:  0.0423
```

Again we select the maximum IC value for the middle rotor ring setting.

PLUGBOARD

Finally we recover the plugboard settings, assuming the correctness of the recovered rotor order, ring settings, and message key settings:

```
        Rotors: II  I III
        Rings:   1 23  4
        Message: 2  7  9
```

A single plug exchanges two letters between the keyboard and the first rotor, and the same two letters between the output of the rotors and the display lights. For each of the 625 possible two-letter plugs, we decrypt the original message using the recovered settings. For plug recovery we use a different performance measure. Although for longer messages the IC effectively distinguishes good from bad decryptions in this phase, for shorter messages a trigraph score gives better discrimination. For these experiments I used a table of base-2 logarithms of raw trigraph counts from The Communist Manifesto. More appropriate would be trigraphs from actual German Enigma messages reflecting the use of (for example) 'q' for 'ch' and 'j' around proper names. Each decrypted potential plaintext was scored by summing the logs of the trigraphs that appeared in the table.

Before trying to recover the first plug, the trial plaintext starts:

```
      Score Plaintext
      577 AIZLJWZHODZTFUWGSRZYLZRNQLJHAVUCPCPZIBAFGCSTSEGEFC
```

The best single plug from this point interchanges E and Z, yielding:

```
   E-Z 1029 AIELJWEHBDETJUWGSREYLEFNQLJHAVUCPCPEIUAFGCSTSZGZFC
```

The new plaintext is still Quatsch (nonsense), but the score has improved considerably. Adding the E-Z plug and repeating this step, we find:

```
   R-W 1258 AIFLEREHBDETJURGSWENLEFEQLJHAVECPCUEIUAFGBSESZGZFP
   M-V 1457 AIFLEREHBDETJUEGSWENLEFEHLJHAMERSSUEIUAFABSESZPZTP
   I-U 1751 AUFLEFEHBDETJIEGSWENLEFEHLJHALERSSIEUIAFABBESZPZTP
   B-L 2121 AUFBEFEHLDETJIEGSWENBEFEHLJHABERSSINDIMFALLEPZPZTP
   P-X 2454 AUFBEFEHLDESJIEGSWENBEFEHLSHABERSSINDIMFALLEXZXZTX
   J-O 2814 AUFBEFEHLDESOBERSTENBEFEHLSHABERSSINDIMFALLEXZXZTX
```

No additional interchange of a pair of letters results in an improvement in the IC. The recovered settings are:

```
        Rotors:    II   I  III
        Rings:      1  23   4
        Message:    2   7   9
        Plugboard: EZ RW MV IU BL PX JO
```

The resulting plaintext (Figure 2) ends, with punctuation added:

```
        DER FUEHRER IST TOT X DER KAMPF GEHT WEITER X DOENITZ X
        The Fuehrer is dead.  The battle continues.  Doenitz.
```

```
AUFBEFEHLDESOBERSTENBEFEHLSHABERSSINDIMFALLEXZXZTX
UNWAHRSCHEINLICHENXFRANZOESISQENANGRIFFSDIEWESTBEF
ESTIGUNGENJEDERZAHLENMAESKIGENUEBERLEGENHEITZUMTRO
TZZUHALTENXFUEHRUNGUNDTRUPPEMUESSENVONDIESEREHRENP
FLIQTDURQDRUNGENSEINXABSXDEMGEMAESSBEHALTEIQMIRDIE
ERMAEQTIGUNGZURPUFGABEDERBEFESTIGUNGENODERAUQVONTE
ILENAUSDRUECKLIQPERSOENLIQVORXABSXAENDERUNGDERANWE
ISUNGXOKHXGENXSTXDXHXERSTEABTXNRXDREIDREIZWOEINSXD
REIAQTGXKDOSXVOMJULIEINSNEUNDREIAQTBLEIBTVORBEHALT
```

```
ENXDEROBERBEFEHLSHABERDESHEERESKRKRFLOTTENCHEFANOK
MMMXXTORPEDOTREFFERACHTERAUSXSCHIFFMANOEVRIERUNFAE
HIGXWIRKAEMPFENBISZURLETZTENGRANATEXESLEBEDERFUEHR
ERXDERFUEHRERISTTOTXDERKAMPFGEHTWEITERXDOENITZX
```

Figure 2. Plaintext decrypted with recovered keyciphertext

EFFECTIVENESS

Figure 3 summarizes a series of experiments designed to determine the effectiveness of this attack. I encrypted different-sized sets of actual Enigma plaintext with random rotor (three selected from five), ring, message key, and plug settings, then attempted to decrypt each given the correct rotor order. Each number of plugs from 0 to 13 and each of six message lengths from 161 to 1463 letters was tried with 100 different randomly-selected settings. I claimed success if the decrypted plaintext was 80% accurate or better -- a close solution could be improved by re-doing the earlier steps with the recovered plug settings, so the success criterion could in fact be set considerably lower.

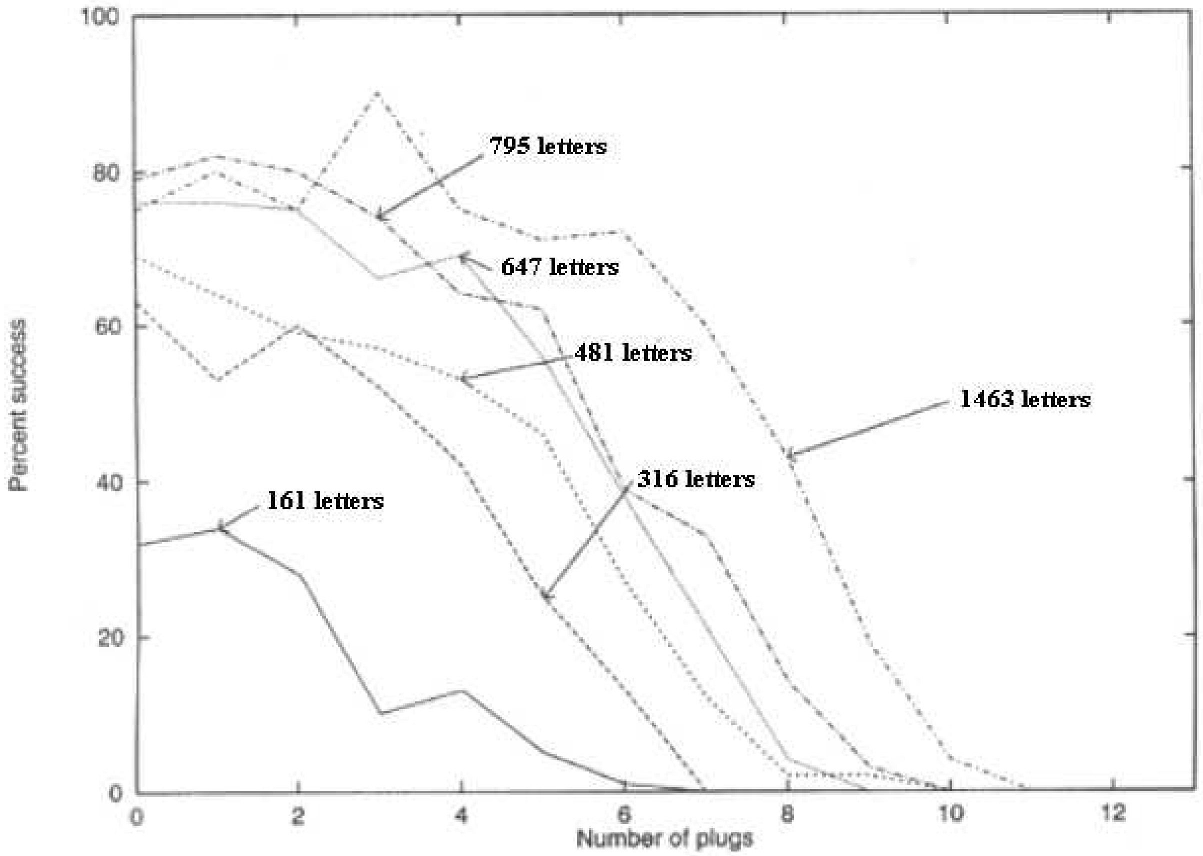

Figure 3. Key Recovery as a function of plugs and message length.

Recovering one message in each traffic net per day would constitute a practical break. This attack appears to be practical for the level of traffic decrypted at Bletchley Park for keys using up to nine or ten plugs.

FINAL OBSERVATIONS

The Germans were right to mandate short Enigma messages, since the uneven distribution of plaintext was not fully concealed by the plugboards -- at least for the number of plugs normally in use. In messages using fewer plugs, less ciphertext is needed for a solution. Conversely, messages using more plugs require more text; only one very long message using 13 plugs has been solved by this method, and that probably by chance. Actual German message traffic used from four to thirteen plugs; after 1939 the usual number was ten. [5] Sometimes shorter messages can be solved by this method at the cost of a little more work: the first step need not identify the correct rotor order, as long as it does find a suitable initial message key setting for each rotor. The subsequent steps are cheap compared to finding the message key setting, and they can be repeated for each candidate rotor arrangement.

In difficult cases the key recovery steps may be reversed, interleaved, or repeated; a few correct plugs may help disambiguate ring settings with similar scores.

More expensive attacks can make shorter messages vulnerable: with 26^4 tests one could recover the ring setting on the fast rotor simultaneously with the message key settings; and with 26^5 (12 million) tests both ring settings could be recovered at once. Modern equipment makes these approaches quite practical.

If this attack was beyond the technology of Bletchley Park during the war, it was certainly accessible only a few years later. The Germans themselves might have been able to use these methods with Konrad Zuse's Z3 general-purpose relay computer [1], completed in 1941, to conduct a similar attack. Evidently Enigma machines were in use long after the war [9]; if later users exercised as little discipline in keeping their messages short, their traffic was potentially vulnerable to inexpensive and automatic ciphertext-only attacks.

ACKNOWLEDGEMENTS

I thank Jim Reeds for providing a "starter set" Enigma implementation modified from an original by Bob Morris, and for setting me straight on some implementation details; Larry Harnisch for test data and encouragement; and Frode Weierud for keying information.

REFERENCES

1. Augarten, S. 1984. *Bit By Bit*. New York, Ticknor and Fields.

2. Dakin, A. "The Z Watch in Hut 4, Part I". In F. Hinsley and A. Stripp. 1993. *Codebreakers*. Oxford, Oxford University Press.

3. Kozaczuk, W. 1984. *Enigma*. University Publications of America.

4. Kahn, D. 1991. *Seizing the Enigma*. Boston, Houghton Mifflin.

5. Deavours, C. and L. Kruh. 1985. *Machine Cryptography and Modern Cryptanalysis*. Norwood MA: Artech House.

6. Deavours, C. and L. Kruh. 1990. "The Turing Bombe: Was it Enough?" Cryptologia. 14(4) 331-349.

7. Friedman, W. 1922. *The Index of Coincidence and Its Applications in Cryptography*. Publication No. 22. Geneva IL: Riverbank Publications.

8. Kahn, D. 1967. *The Codebreakers*. New York, MacMillan. 459.

9. Kahn, D. 1974. "Enigma Unwrapped." *New York Times Book Review.* 29 Dec 1974. Quoted in Kozaczuk [3].

10. Public Record Office. "Ultra: Secret German messages from World War II". UPA Academic Editions, Frederick MD (1989), by permission of Her Britannic Majesty's Stationary Office (microfilm).

BIOGRAPHICAL SKETCH

James J. Gillogly is a computer scientist at RAND, specializing in system design and development, computer security, and C hacking. He edits the Cipher Exchange column for The Cryptogram (organ of the American Cryptogram Association), coordinates a mailing list dealing with the Voynich Ms., and sings drinking songs in period costume at Renaissance Faire while juggling.

Mail Jim Gillogly

Read Erksine's letter

Converted to hypertext by Joe Peschel December 7, 1999; revised October, 2000