CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

March 10, 1996
Revision 1

LECTURE 9

GERMAN REDUCTION CIPHERS
ENIGMA IN HISTORICAL AND MODERN TIMES

SUMMARY

In Lecture 9, we circumvent the schedule for another real treat - the ENIGMA cipher machine. Considering the focus of the 1995 ACA convention, several articles in CRYPTOLOGIA, a recent book by Robert Harris called " Enigma ", a Randomhouse challenge cipher contest based on the Enigma (won by several of the KREWE), many questions from my students, I thought we would address the subject of ENIGMA.

I have had the pleasure to work with ESSAYONS on a project in which we looked at the security of the original Enigma D machine in terms of 1995 technology improvements. ESSAYONS has brought to light some brilliant insights.

The ENIGMA 95 computer program cited in this lecture is available at the CDB. Contact NORTH DECODER for access.

Students have asked 1) what is Enigma and 2) where does Enigma fit into history of radio communications in WWII?

There are three pillars of radio-intelligence: direction finding, traffic analysis and deciphering. Direction finding equipment and technology is outside the scope of this course. Traffic analysis has been discussed in a previous lecture. We will quickly revisit its value and then follow Professor Jurgen Rohwer's analysis of the Atlantic Warfare to understand Enigma's position in cryptographic history. [ROHE]

The Enigma machine is actually a good starting point for my discussion on polygraphic and polyalphabetic cipher analysis (originally planned for Lecture 9). We start at the endpoint of a discussion and return to the beginning to build up the cryptanalytic tools to understand the cleverness of the ENIGMA. We will continue with the Friedman and MASTERTON in Lecture 10 and following. [MAST], [FR2], [FR3]

TRAFFIC ANALYSIS REVISITED

Recall that traffic analysis yields information via Crib messages, Isologs and Chatter. Crib messages assume a partial knowledge of the underlying plain text through recognition of the external characteristics. Command reports, up and down German channels, were especially easy for American crypees. The origin, serial number range, the cryptonet id, report type, the file date and time, message length and error messages in the clear, gave a clear picture of the German command process. German order of battle, troop dispositions and movements were deduced by traffic analysis.

An Isolog exists when the underlying plain text is encrypted in two different systems. They exist because of relay repetition requirements, book messages to multiple receivers or error by the code clerk. American crypees were particularly effective in obtaining intelligence from this method.

Traffic analysis boils down to finding the contact relationships among units, tracking their movements, building up the cryptonet authorities, capitalizing on lack of randomness in their structures, and exploiting book and relay cribs.

ENIGMA

ENIGMA was the generic term for the German machine ciphers. It was both the name of the first enciphering device and the many variations used during WWII. ULTRA was the British code-name for intelligence derived from cracking the Enigma machine ciphers by an organization of about 10,000 at Bletchley Park (BP). The extent of the penetration of the German command structure was so profound and so pervasive that it is clear that BP's work changed not only the conduct but the outcome of Allied European Operations in WWII. Most brilliant of ULTRA successes was against German Afrika Korps whereby the 8th Army HQ read Enigma telegrams before Rommel himself. [ASIR] [KAH2]

There now exists a fair amount of material on Enigma. The following annotated outline should give the reader some ideas how important Enigma was in WWII and sources of information:

ENIGMA CIPHER MACHINE(S)

A: HISTORY

A1: Historical Perspective - Atlantic Theater Warfare in Eight Phases 1939 - 1945.

Enigma was central to the Battle of the Atlantic in WWII. Primary sources for the historical perspective come from Germany, Canada, UK, and USA. Professor Jurgen Rohwer's Comparative Analysis of Allied and Axis Radio-Intelligence in the Battle of the Atlantic, [ROHE] presents the ENIGMA history in 8 phases:

Phase 1 - Single U-Boats vs Independent Ships
9/39-6/40 Failure of BP on Schlussel M (Navy Machine)
Phase 2 - Wolf Pack vs Convoy
7/40-5/41 Success of B-Dienst (German Naval decryption service)

Phase 3 - Evasive Routing, US Entry
6/41-12/41 U-33 3 rotors recovered, U-110, Munchen Bombe limited success 336 settings
German 4 rotor improvement

Phase 4 - BP Successes on Enigma D, US losses
1/1-6/42

Phase 5 - Convoy Battles
7/47-12/13 Triton Broken ; Rerouting; Milch runs

Phase 6 - Bay Offensive
6/43-8/43

Phase 7 - Decreased Operations vs Convoys
9/43-5/44 Increased use of Ultra

Phase 8 - Holding Campaign with Schnorkel U-boats
6/44-end New Enigma not released in time for Germany

Professor Rohwer presents 105 primary references. [ROHE]

A2. Discussion:

>From September, 1939 to June 1940, German U-boats cruised west of the British Isles and Bay of Biscay to intercept Allied Merchant ships. U-boats found enough targets. Radio signals were as indispensable to the German Commander in Chief, U-boats (BdU = Befehlshaber der Unterseeboote - Commander in Chief of Submarines) for directing his U-boat groups or wolf packs as they were for Allied commanders directing the convoys of merchant ships and their escorts. The aim of the Axis powers was to sever the lines of communication by surface radars, aircraft and especially U-boats to attack ships in the convoys and thus sink more vessels and tonnage than the Allied shipbuilding yards could replace.

In the first two phases of the Battle of the Atlantic, there was a clear superiority with cryptanalytic success on the German side. Intelligence was of limited value to actual operations. The Germans introduced the short signal system, using a codebook to shorten communications to a few four letter groups which were superenciphered with daily settings of the Schlussel M [M Key] in the circuit of Heimische Gewasser (home waters). The Royal Navy used two crypto-systems - the first was the Naval Cypher which used 4 figure codebooks and the second was the 5 figure codebook Naval code. Both used subtractor tables of 5000 groups changed monthly. B-dienst was reading about 30 -50 % of the Naval Cypher, used by officers. The Merchant Navy Code was broken by the B-dienst in March 1940.

In the third phase BP mastered the Schlussel M- 3 and saved about 400 ships by rerouting convoys. The Schlussel M-3 used three rotors out a stock of eight rotors. BP had limited no success against VI-VIII and limited success against rotors I-IV. The boarding of the Krebs gave the British a box of five rotors. A key to Enigma is its two inner settings, the

Walzenlage, or rotor order, and the Ringstellung, the setting of the alphabet rings. In addition to these were the plugboard , the Steckerverbindungen, of ten pairs of letters and the Grundstellung, the starting positions of the rotors. The capture of U-110 gave BP a consistent set of settings and grid maps to reference. The British STR (Submarine Tracking Room) became key to rerouting ships valued at 1.5 mm GRT.

Phase 4 clearly went to the Germans because of their score of ships sunk off the Americas.

In Phase 5, near 1942, the BdU had many interceptions because the B-dienst decrypted the rerouting signals more effectively. Triton introduced and stumps BP. In March 1943, BP solves the Triton and Admiralty changes the operation patterns.

The six and seventh phases German cipher improvements broken by use of U. S. and British high speed Bombes.

Introduction of Kurier system for high speed transmissions to new U-boat type XXI was released to late to stop operation Overlord.

A3: Shipping Losses and Input Tonnage

Allied shipping losses were significant and import tonnage was reduced because of the U-boat success and communication. T. J. Runyan and Jan M. Copes "To Die Gallently" [RUNY] presents details.

A4. Enigma Chronology

David Kahn presents an Enigma chronology in terms of world events. A clearer picture of the effect of ULTRA can not be found. Timelines based on his and the honorable F. H. Hinsley books. [KAH2], [KAH3], [HINS] and [KAH3]

A5: British Perspective

The early history of the Enigma, the Polish attack and the beginnings of BP covered in [KAH3] ,[WINT] Winterbotham and Beesley give us special insights into the fray. [BEES] Other perspectives found in [ANTH] and [HYDE].

A6: Polish Perspective

The story of the Marian Rejewski, Jerzy Rozycki and Henryk Zygalski pioneering work in the Biuro Szyfrow (Cipher Bureau) and their escape to France is told in [ASIR].

B: SPECIFICATIONS

B1: Enigma Machine Classes A-E (Deavours)

Enigma was a class of machines. Cipher A. Deavours and Louis Kruh, in Chapter III of " Machine Cryptography and Modern Cryptanalysis", give detailed descriptions with pictures, rotor order, settings, plug-board and their influence on frequency distribution. [DEVO]

B2: Enigma - 3 rotor (Kahn)

David Kahn in his "Seizing the Enigma" , pp 178 ff gives good detail. Also "Codebreakers" p422. , also various articles by Kahn in Cryptologia give pictorials. [KAH3] [KAHN]

B3: Army Enigma - 3 rotor (Hinsley)

F.H. Hinsley and Alan Strip in "Codebreakers - Story of Bletchley Park", [HINS] have pictures and supporting detail for the Army version 3 rotor device.

B4: Early Variations - (Friedman)

NSA's Friedman Legacy - A Tribute to William and Elizabeth Friedman, 1992, pp 201 ff discusses the early Enigma variants. [FL]

B5: Naval Variation - Air Ministry (3 of 8 rotors)

See Ref's [ASIR]

B6: Air Force Variation - 3 rotor of five (British Air Ministry)

See section B3.

B7: University of Hamburg - WWW : Enigma pictures

Dr. Klaus Brunnstein (University of Hamburg) has provided excellent GIF Enigma pictures in their Working Groups "museum":

Address: http://www.informatik.uni-hamburg.de
Select "international homepage"

From 2nd entry "groups", select AGN
(first of the working groups)

There, select "Museum" (4th entry) where you get a list of about 40 pictures. The CDB has these also.

C: PATENTS

C1: General - (Levine)

Jack Levine presents the most comprehensive treatment of U.S. Cryptographic Patents 1861-1981 in [LEVI].

C2: Scherbius #1,657,411 [LAUE] [Geheimschrijfmachine] 1919

Rudolph F Lauer discusses the original A. Scherbius Enigma patent # 1657411 in his "Computer Simulation of Classical Substitution Cryptographic Systems" in [LAUE]. This machine was used for diplomatic communications and had ten rotors. BP broke it late in the game using the Colossus machines.

C3: Herbern # 1,683,072 [Electric Code Machine], 1917

Reference [ASIR] gives an interesting account of Herbern's efforts.

D: ENCIPHERING PROCESS

D1: Naval Enigma (Kahn)

David Kahn in his "Seizing the Enigma" Appendix presents a detailed Enciphering procedure for the Naval Enigma. Approximately 20 pages of notes, biblio, interviews and diagrams. [KAH3]

D2: ESSAYONS and LANAKI present modern PC technology applied to encipherment process in [ENIG].

E: CRYPTANALYSIS

E1: BP Analysis (Turing)

Cryptanalysis of the various Enigma variants starts with Alan Turing "The Enigma", in [ALAN]

E2: Polish Attack (Rejewski)

Perhaps the earliest and best attack, Marian Rejewski wrote the brilliant "Mathematical Solution of the Enigma Cipher" published in [REJE].

E3: Double Encipherment Flaw (Bloch)

Gilbert Bloch and Ralph Erskine exploit the double encipherment flaw in article on Enigma, in Cryptologia. [BLOC]

E4: Lauer Analysis of Classical Systems & (Deavours)

Rudolph F. Lauer presents Cipher A Deavours simulation program p73 ff in reference [LAUE]. Deavour's program reveals the German Army cipher machine simulated consisted of three rotors (of eight), rings settings, plugboard (for key super -encipherment, rotor starting positions and a reflecting rotor. The program requires the user to set "prepare the machine" by setting the rotor wirings, rotor order, rotor starting position, ringsettings, plugboard pairs and no of plugs used and the current rotor positions. It calculates the patchpanel, displacements of cylinder coding and effects of reverse rotors, and reflecting rotor. There are no error checks for singularity.

Lauer also presents ten cryptographic systems and representative cipher machines in increasing order of difficulty. He presents 72 references (including the Cipher A. Deavours simulations) on disk. Each system is not only simulated but the principles for the entire class of machines are presented. Ignoring the programming language, BASIC (I would choose FORTRAN, others would choose C, and others APL, and others ADA and..); the methods applicable to one machine apply equally well to others in the same class.

I have rearranged his classification methodology and added my own thoughts to show how ENIGMA fits into the progression of classical cryptographic / mechanical systems:

E40: Mathematical Footholds

a: Modulo 26 Arithmetic, Congruences, Matrices
b: Statistical Phi values for small distributions
c: Isomorphism - reference [CAND]
d: Optimization Theory
e: Advanced Calculus, Linear Transformations
f: Probability Theory

E41: Simple Substitution - Cipher Disk {My Lectures 1-8 }

Principles: monosubstitution, K1,K2,K3,K4, KM sequence keying, transpositional keys.

Examples: Aristocrats, Patristocrats, Xenocrypts Caesar, sliding strips, rotating disks

Attacks: Frequency analysis, word pattern, bigram, trigram, vowel spotting, letter distribution.

E42: Periodic Polyalphabetic Substitution - Viggy Devices
{My Lectures 10-13}

Principles: poly-alpha-substitution, repeat key sequence

Examples: Vigenere, Variant, Beaufort, Porta, Gronsfeld

Attack: Periodicity, Kasiski, trigraphic, traffic analysis, Kerckhoff's method.

E43: Running Key and Autokey - Kammel and Weller Devices

Principles: polyalphasubstitution, non-repeat key sequence, PT autokey, CT autokey and running key

Examples: Running key and autokey ciphers

Attack: Friedman attack - "Solution of Running Key Ciphers, probable word, known plain text.

E44: Simple Progressive

Principles: constant shift interval to employ all secondary alphabets (period = 26)

Examples: Progressive Cipher

Attacks: Friedman attacks, periodicity at 26,13,2,1 same as E42, Chi test, matching frequency distributions, decimation intervals, coherent key

E45: Irregular - KRYHA

Principles: irregular shifting of primary components non coherent key, non recognizable key, long key derived from two or more short keys, pseudo-random different interval shifts on progressive; sum of shifts be relatively prime to N in alphabet

Examples: One time pad, Vernam Key Tape

Attacks: Sacco's solution, Isomorphism, Friedmans technique

E46: Wheatstone Cryptograph

Principles: Aperiodic cipher, extra sequence shift, error control

Examples: Jefferson, Hebern machine, Vernam

Attack: Friedmans techniques [FR4] probable phrase

E47: Multiplex Systems

Principles: Wheel ciphers

Examples: Jefferson, M-138, M-94

Attack: Friedman techniques, De Viaris examination, synoptic tables, G. Mellen attack, Rohrbach method coincidences - generatrices group

E48: HAGELIN M-209

Principles: pin lug mechanism, cylindrical cage, guide arm - print wheel rotates number of positions = sum of the lugs on those key wheels which were affected by active pins. ==> key value with period of 3,120,180 letters.

Examples: C-36, M-209

Attack: Wayne Barker analysis one wheel to six wheels, statistical analysis on settings, probable word

E49: ENIGMA

Principles: electrical rotor or transfer wheel, stepping gears, maze between keyboard and indicating device producing 26 ** N different enciphering alphabets, re-entrance phenomenon, excess contacts. superencipherment

Examples: ENIGMA A-E

Attacks: Polish, BP, Turing, Deavours, Friedman IC, E1-E8 previously cited, Chi test on diagonals, isomorphs, Pohlig w/ PT, Konheim analysis, Lisicki Grille 1000x1000 rearrangements

Modern Experiments: Remove reflecting rotor.
Use re-entrance type rotor
[ACA and Install bi-directional Rotors
University of Increase entropy
Hamburg] Expand character sets

E410: HILL SYSTEM {NORTH DECODER in Lecture 8}

Principles: Polygraphic encipherment, non - linear encipherment == forerunner of "S" boxes in DES

Examples: Playfair, Hill Device

Attacks: Konheim technique, Rhee analysis, Mapping,

E5: Polish attacks (Kozaczuk)

Dr. Wladyslaw Kozaczuk discusses the Polish attacks on Enigma in [KOZA]

E6: Involution Principle (Konheim)

Involution principles are presented by Alan G. Konheim, "Cryptography -A Primer" , in [KONH]

E7: Related Machines (Barker)

Wayne G. Barker presents a related analysis in "Cryptanalysis of the Hagelin Cryptograph, in [BARK].

E8: Enigma 3 (Sassoons)

A clever treatment of the Enigma 3 wheel device can be found in George Sassoons, "Radio Hackers Code Book", [SASS]

E9: Tieman C (Schneier)

Bruce Schneier, in his "Applied Cryptography', presents Tieman's C program. [SCH1]

F: ROTOR SYSTEMS

F1: Theory (Konheim)

The general theory of rotor systems is well presented in chapter 5 of Konheim's primer. [KONH]

F2: Polish Solution

The brilliance of Marian Rejewski solution is presented in "The Mathematical Solution of the Enigma Cipher " in [REJE]

F3: Computer Crypto and Probability Analysis [A German View]

Norbert Ryska and Siegfried Herda give a fresh look at computer techniques required for Cryptography. From a German point of view, it gives the reader a look at security risks, and cryptomethodology. [RYSK]

G: ENIGMA IMPROVEMENTS

G1: Code Changes (Sassoon)

Sassoon suggests improvements to Enigma by using full ASCII set of 256. Sequence length 256 x x 256. Rotor settings in blocks of 256 8-bit bytes one to define the position of each rotor. Sassoon's Basic Enigma3 simulation 4 rotors and a reflector rotor. It simulates the movement towards the reflector or away from it. Rotor cross connections are well defined. Subroutines to test the encryption and decryption are included. Clear rotor advancement routines. Error checking subs as well. No plugboard. [SASS]

G2: Improved Security (ESSAYONS and LANAKI)

Clarence Tyner Jr. has spent significant time since 1944 on German cipher production and reduction efforts. Starting with a Model D (circa 1920's) Tyner simulated the original Enigma with wartime enhancements (plugboard, expanded rotor sets, etc.) and then improved it while staying within the original concepts of the original machine (keyboard input, data path through a plugboard, rotating rotors, reflecting rotors, and output display. Presented in detail later in this lecture.

H: ORGANIZATIONS (Kahn) (ASI)

H1:BP
H2:OSS
H3:German Navy - U Boat Command
H4:B-Dienst
H5:Bureau De Chiffer
H6:Polish Biuro Szyfrow
H7:French Service Renseignements
H8:AVA Telecomunications
H9:German Army Command
H10:SOE
H11:RAF-SLU
H12:Siemans und Halske Aktiengesellschaft
H13:AC Bridge Laboratory

David Kahn in his books "Seizing Enigma", "Codebreakers" , "Kahn on Codes" and "Hitlers Spies" presents the various people and organizations surrounding Enigma. Also the British Air Scientific Institute, chap 6 describes the relevance of each organization in the cracking of Enigma. [ASIR] [KAH1] [KAH2][KAHN]

ENIGMA 95

A simulation of an enhanced Enigma Cipher Machine on a standard personal computer

Clarence E. Tyner Jr. and Randall K. Nichols

ADDRESS : 11322 Carrollwood Drive, Tampa, Florida, 33618, USA.
5953 Long Creek Drive, Corpus Christi, Texas, 78414, USA

ABSTRACT : An exploration into the possibilities of what can be done with the operating methods of the Enigma on the personal computer. The same concept of employing keyboard input, a plugboard, rotors (both normal and reflecting), Uhr box and visual output are used, but are expanded by using 100-position rotors that intermittently rotate a prime amount after each input, allowing the number of rotors to vary from 1 to 12, in front or backwards orientation, top permit any keyboard character (including spaces) to be encrypted, and to simultaneously display cipher and clear text for editing. A rotating Character Set converts single-character input into 2-digit numbers for processing and superencipherment of numeric output into alpha bigrams is possible. Regular rotors, Reversing rotors, Character Sets and Superencipherment Tables are provided in sets of 100 for extensive variety. Visual monitor display and paper printout are employed and other controls are provided. It is a "what if" speculation that shows what could have been possible if the technology had been available.

KEYWORDS : Enigma, prime numbers, rotors, intermittent rotation, superencipherment, personal computer, QBasic, interval method, character set, random numbers, checksum, plugboard, orientation, internal settings, external settings.

Everyone is familiar with the Enigma Cipher Machine and the way it operates.

However, the more you learn about it and read about the cryptanalysis that overcame it in World War II, the more you wonder if it could be improved without becoming impossibly complicated. The personal computer provides a means to improve the concepts that made the original Enigma work, and it can make it work much better.

This project started as a simulation of the original Enigma. The pathway of the electric circuit caused by pressing a key is easy to understand. It goes from the keyboard through the plugboard to the rotors, is reflected from the reversing rotor, back through the rotors, through the plugboard and finally to a lamp that lights under a round window with an alphabet on it. At least one rotor will rotate during the pressing of the key and the pathway through the rotors will change from what it was previously. The internal wiring of the rotors is random and the cumulative circuit offset combinations produce an extensive number of substitution alphabets. The plugboard adds to this, as did the Uhr box.

Aside from administrative and operator errors, the weaknesses of the enigma were as follows:

1. The internal wiring of the rotors was fixed. It never changed except for a few specialized purposes. While the mathematical possibilities were astronomical, only a small portion of them were utilized probably because of manufacturing, cost and logistics considerations.

2. There were only eight rotors in a set and only 3 or 4 could be used at a time.

3. The rotors rotated only very restricted basis. One moved one position each time. The second moved only after the first had moved 1 to 26 positions. The 3rd moved only after the 2nd had moved 1 to 26 positions. There were notches on the rotors to accomplish this and the rotors could be set so that the movements occurred at different times, but movement of two rotors was infrequent, and movement of all rotors was limited and somewhat predictable.

4. The reversing (reflecting) rotor did not move, nor could it be moved (except on the earlier models).

5. A subtle weakness was that a given letter could never be encrypted as itself.

6. It was expensive and labor-intensive both to manufacture and to operate. Once it had been determined how to simulate the rotation of rotors and to simulate the transfer of the electrical current between rotors correctly, a major problem was solved. Then it was necessary to determine how to keep the internal wiring connections unchanged during rotation. This was followed by developing a method of selecting and installing the rotors at a given position and then how to rotate them to an initial setting. Having an old Model D Enigma (3 rotor) so that it was possible to determine what the outcome should be was helpful.

Creation of rotors presented a challenge in establishing the internal wiring and in making a set from which to choose three. Edward H. Hebern used the Interval Method of wiring his rotors, so it was decided to use that approach. For those who are not familiar with it, it involves determining the positional difference (interval) between points connected on opposite faces of the rotor. For a 26 (A - Z) position rotor, the intervals range from 0 to 25, with each interval being used only once. But the geometry of the problem prevents one interval from being used and requires one interval to be used twice. All intervals are measured in the same direction. For example, a connection from point A on one face to point C on the other has an interval of 2 (assuming opposite positions are identified with the same letter).

I don't know how Mr. Hebern did it, but it is a job perfectly suited for a computer. At any rate, "wiring" a rotor using the Interval Method can be very tedious because it involves a lot of trial and error if done manually (or, as it turned out, by computer). It would be interesting to know if there is a simple algorithm. It is supposed to produce a more secure encryption. After trying to do it manually (by diagramming on paper), programs were written to do it for both regular and reversing rotors. The programs also produce a file on a floppy disk to simulate a set of rotors and print the results for record purposes. Each rotor had to be unique from all others so use of random numbers was involved.

The plugboard was programmed so that it was possible to enter the 2-point (from -to) sets that were to be connected. Multiple sets could be created, just as it is possible to have multiple cable connections on a mechanical Enigma. A file of plugboards is not needed because the variance within fixed fields is derived from the connections, and to allow numbers of connections to be varied. It was necessary though to provide for editing to insure that each position was used only once (as in real life).

At this point, the idea of expanding the Enigma came into being in the form of introducing variability between the keyboard and the plugboard such as the Uhr Box does. It was decided to make the Enigma process the data in numerical form and expand it from a 26 to a 100 character format. This numerical format (00 -99) has the disadvantage of doubling the length of a message, but it has certain advantages. In addition to handling alphabetic letters, it can also:

1. Allow upper/lower cases, numbers, symbols, punctuations, and spaces to be encrypted.
2. Better conceal the language and individual characters being transmitted.
3. Eliminate the problem of a letter not being encrypted as itself.
4. Allow a longer period between repetitions.
5. Permit superencipherment.
6. Provide 100-position rotors and plugboard which are more difficult to analyze.
7. Facilitate masking control elements in messages. (e.g., rotor settings, etc.)

This format required a method of converting input into 2-digit form. It was done by creating what are called "Character Sets". These are randomly organized sets of 100 characters (upper and lowercase) that appear on the keyboard. The

entire 100 positions are not used and the unused are filled with a seldom-used accent mark. One hundred sets are available in a file on floppy disk. The sets are used in both encryption and decryption to convert from and back to cleartext.

Using 100 as a common feature, brought into use the digits 00 - 99 to identify rotors, sets, tables and plugboard positions. Sets of these components have 100 of each ("00" means "100").

The next feature was to provide for the unique rotation or non-rotation (movement of each rotor is randomly intermittent) of each regular and the reversing rotor after each input. The Character Set also rotates so that doubles (like "oo" in book) are converted differently. Rotation is by a prime amount to 100 (2 and 5 are not used). Editing prevents using other numbers. An additional feature was to provide a Rotor Display similar to the windows on the Enigma. This is primarily informational but has proven to be helpful in de-bugging the program.....and it does provide a sense of rotor movement.

Another idea was borrowed from Mr. Hebern. That was the ability to "insert" rotors into the machine either forwards or backwards which doubles the number of rotors in a given set. It was also possible to provide for a variable number of rotors. An arbitrary limit of 12 was chosen but it would be possible to have more (though that might be considered overkill). The important thing here is that it would be possible to employ from 1 to 12 rotors (from a set of 100), depending on the security desired. The rotor display automatically adjusts to the selected number.

The next feature that was added was the ability to optionally superencipher the resulting numeric ciphertext. This involves replacing a 2-digit numeric cipher with a 2-character alphabetic bigram (e.g., 36 to HK). It also permits each numeric cipher to be represented by one of 6 or 7 bigrams (e.g., 36 could be HK, UM, RY, AU, ZM or BI). The 7th bigram appears only for selected numerics because the 676 (26 x 26) possible bigrams are evenly distributed amongst the 100 numerics. In addition, the use of a given bigram in a set for each numeric is incremented sequentially so using this example, the numeric "36" would be converted to HK the first time it appears, to UM the second time, etc. The first selection can start at any of the first 6 positions and it cycles around to position 1 when position 6 or 7 is used. A SuperEnciphering Table (Figure 18) accomplishes this and there is a matching SuperDeciphering Table (Figure 19) to reverse it.

Text input requires no use of the <enter> key and the computer buffer handles rapid input so that the entry of clear or cipher text is faster than that of the original Enigma. Input is displayed on the monitor and the resulting cipher/clear text is displayed immediately below so that it is possible to visually check it. If an error occurs, a simple procedure allows you to correct it without having to re-type everything. A screenful of data consists of 6 sets of double lines (one input, one output) double spaced with the sets separated by a dotted line for clarity. There are 27 inputs per line for a total of 162. When the 159th - 161st are entered, a beep sounds to alert you to the approaching end of a screen. This allows you to make a final check of the input for errors (and easily correct them) before entering the 162nd which triggers printing that screenful to paper. During the printing you can start entering the next screenful. A limit of 1943 inputs (12 screenfuls less 1) was arbitrarily chosen for demonstration purposes (more would be possible, depending on memory available). This limit can be easily set to a shorter value to control message length to make cryptanalysis more difficult.

Printing is considered essential for the purpose of having a record of what was sent and how it was encrypted or decrypted (e.g., was the cleartext entered correctly and was the machine correctly set ?). It also eliminates the need for a second person to transcribe the output. Attached are four exhibits that are examples of the printouts that can be produced:

Exhibit A : Encryption into numeric form
Exhibit B : Decryption of Exhibit A
Exhibit C : Encryption in Superenciphered Form
Exhibit D : Decryption of Exhibit C

Each exhibit is divided into the following parts:

1. The Heading: This indicates whether it is encryption or decryption, and the date and time that the settings were entered . This does not change for repeated use of the settings for two or more consecutive messages. To enter a new date/time group or change the internal settings, the program must be completely restarted. (See A1, B1, C1 or D1)

2. The Internal Control Settings: This indicates the number of plugboard connections used, the specific plugboard connections, the number of rotors used, the specific rotor numbers in the position sequence and then each rotors orientation (frontwards or backwards). The reversing rotor number is indicated. Next, the unique rotation value for each rotor and the reversing rotor are shown, followed by the character set number and its rotation value. These constitute the internal settings that would be specified by the Signal Operating Instructions (SOI). All of these settings generate an Internal Checksum which is used to verify that the settings have been correctly entered.

This checksum is printed. If it does not agree with that provided in the SOI, then all the settings must be re-entered by restarting the program. Intermittent rotation of each rotor is a function of the installed rotors and previous entries and does not have to be specified.

3. The External Control Settings: This lists the settings that the operator selects and enters for the specific message. They consist of the Initial Settings of each rotor and optionally the Superencipherment Table number if it is used. These settings add to the Internal Checksum and produce an External Checksum in the form of a 2-digit number (mod-100 of the total sum) that is sent with the message. The superencipherment table counter setting is NOT included and is NOT sent because the recipient does not have to know it. (See A1, B1, C1, D1)

4. The Input / Output Message Text: This duplicates that which appears on the monitor screen and is provided primarily for a message audit (to insure that the message was entered correctly). Each "line" has 27 inputs with the 27 outputs below. Twenty-seven was used to provide legibility on an 80-column screen. Six such "lines" are possible for each screenful. (See A1, B1, C1 or D1)

5. The Message Control Data: A count of the input characters (message length) is provided for both superenciphered and non-superenciphered messages.

However, only non-superenciphered (numeric ciphertext) messages have the following additional data provided:

a. A Hash Total which is a Mod-100 sum of the numeric cipher text. (See A1, B1)
b. A set of Column Check Totals which is the Mod-100 sum of each of the 27 columns of cipher text. This is followed by a non-mod total of the columns. (See A2, A3, B2)
c. A total of Row Check Totals which is the Mod-100 sum of each row of cipher text. This is followed by a non-mod total of the rows. (See A2, A3, B2)

The purpose of providing column and row totals is to be able to locate transmission garbles. They would be sent only if requested. Variances in any given column and row would locate the error by intersection.

6. The Message in Transmission Form: This is what would be sent and would contain only the External Control Settings (rotor settings, superencipherment table number and external checksum) , the date and time group, the message ciphertext and the character count. The External Control Settings would be disguised by a simple manual superencipherment that would be administrative and outside the operation of the Enigma 95 (i.e., prescribed by the SOI). (See A3, C2) If it is decryption, the cleartext message is presented with normal horizontal spacing and vertically double spaced for convenient reading. (See B3, D2)

7. Following this is an optional message analysis which is simply a count of input and output characters. This can be skipped and was provided only to assist any system analysis. (See A4 and C3)

This completes the printing.

Next displayed on the monitor is an option to re-use the Internal Control Settings for another message (it was assumed that these would remain in effect for a period of time as was the case for the Enigma). If this is not selected, the program ends.

HARDWARE AND SOFTWARE REQUIREMENTS

The Enigma 95 is a program written in Microsoft QBasic. This was done so that it could be run on any standard MS DOS computer using MS DOS 5 or higher (QBasic is bundled with MS DOS) thereby eliminating the need for a specialized computer. It fits onto a 3.5 inch floppy disc, together with the necessary data files that constitute the Regular Rotors Set, Reversing Rotors Set, Character Sets and Superencipherment Tables. It is possible to also have on the same disk, the programs that create these files and the necessary documentation (.DOC) text files for each one. This makes the Enigma 95 very portable, very inexpensive and very easy to replicate.

Any computer that will run MS DOS QBasic is suitable for the Enigma 95. A color monitor is preferred but not essential. A printer is very useful, but could be eliminated if one is willing to copy output manually from the monitor screen (as the original Enigma required).

There is provided a program that produces a graphic representation of the circuit path through the Enigma 95 and a program to produce pseudo-random numbers to use in programs that produce the rotor disks. Also included are programs to analyze the Enigma 95.

OPERATIONAL OVERVIEW OF THE ENIGMA 95

The following is a run-through of the operating procedure, with the appropriate illustrations of the monitor screen at each meaningful step.

1. The computer is turned on, QBasic is selected and the Enigma95 program is loaded and run.

2. You are asked to place the data files disk in the Drive B so that they will be available.

3. You are then asked to enter the Internal Control Settings:

   a. Number of Plugboard Settings (1 to 50). 45 is optimum.
   b. The plugboard settings (from and to) (Figure 1)

SOI : ENTER THE NUMBER OF PLUGBOARD CONNECTIONS TO SET : 21

```
SET   1  :  1735   SET 11  :  2653   SET 21 :
SET   2  :  2356   SET 12  :  4899
SET   3  :  4581   SET 13  :  6250
SET   4  :  9852   SET 14  :  4069
SET   5  :  3377   SET 15  :  3180
SET   6  :  5544   SET 16  :  9402
SET   7  :  6612   SET 17  :  8437
SET   8  :  5987   SET 18  :  9307
SET   9  :  3254   SET 19  :  8843
SET  10  :  6791   SET 20  :  8514
```

Plugboard Positions not yet selected

```
01    03 04 05 06    08 09 10 11    13    15 16    18 19 20
21 22    24 25    27 28 29 30          34    36    38 39
41 42          46 47    49    51                57 58    60
61    63 64 65       68    70 71 72 73 74 75 76    78 79
82 83       86       89 90    92       95 96 97       00
```

---------- Figure 1----------

   c. Number of rotors to be used (1 to 12)
   d. The rotor number (1 to 100) for each position and its orientation (1=Fwd, 2 = Bkwd)
   e. The reversing rotor number (1 to 100) (Figure 2)

---

12 ROTORS ARE TO BE SELECTED FROM THE S.O.I.

Select Rotor (1 to 100) and Orientation (1 or 2) IN THE SAME ENTRY

For example : < RO > or < RRO > or < RRRO > <enter>
< 71 > < 232 > < 1001 >

	ROTOR	ORIENTATION
Position No. 1	32	1 - Forward
Position No. 2	49	2 - Backward
Position No. 3	42	1 - Forward
Position No. 4	98	1 - Forward
Position No. 5	63	2 - Backward
Position No. 6	94	2 - Backward
Position No. 7	62	1 - Forward
Position No. 9	4	1 - Forward
Position No. 10	33	2 - Backward
Position No. 11	25	1 - Forward
Position No. 12	11	1 - Forward

ENTER REVERSING ROTOR NUMBER (1 TO 100): 53

---------- Figure 2----------

f. The rotational shift value for each rotor (a prime number between 0 and 97 inclusive less 2 and 5) (Figure 3)

(See the current S.O.I. for the values to use)

SET ROTATIONAL SHIFT VALUES FOR EACH ROTOR POSITION

USING THE FOLLOWING PRIME NUMBERS (EACH ONLY ONCE)

0,1,3,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97

FOR ROTOR POSITION 1 : 07
FOR ROTOR POSITION 2 : 29
FOR ROTOR POSITION 3 : 01
FOR ROTOR POSITION 4 : 71
FOR ROTOR POSITION 5 : 17
FOR ROTOR POSITION 6 : 13
FOR ROTOR POSITION 7 : 11
FOR ROTOR POSITION 8 : 47
FOR ROTOR POSITION 9 : 03
FOR ROTOR POSITION 10 : 61
FOR ROTOR POSITION 11 : 23
FOR ROTOR POSITION 12 : 19

FOR REVERSING ROTOR : 31

---------- Figure 3----------

g. The Character Set number (1 to 100) (Figure 4)

(See S.O.I.)

ENTER CHARACTER SET NUMBER : 44

---------- Figure 4----------

h. The rotational value for the character set (the same range as f. above). (Figure 5)

(See the current S.O.I. for the values to use)

SET ROTATIONAL SHIFT VALUE FOR THE CHARACTER SET

USING ONE OF THE FOLLOWING PRIME NUMBERS NOT USED FOR THE ROTORS

0,1,3,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97

ROTATIONAL VALUE : 89

---------- Figure 5----------

4. You are then asked: DO YOU WANT TO (1) ENCIPHER OR (2) DECIPHER?

a. Assuming that (1) is selected, a "random number" generator is presented to select numbers for use as Internal Settings.

b. This is a sort of "spin the arrow" device to prevent bad selection of settings
but any source of random numbers may be used. It is optional. It is skipped if (2) is selected.

5. The Internal Checksum is displayed and then you are asked for the External Control Settings:

a. Initial settings for the regular rotors (1 to 100).

b. Initial setting for the reversing rotor (1 to 100).
(Figure 6)

Internal Checksum = 60354

(See your list)

SET INITIAL ROTOR SETTINGS (1 TO 100)

ROTOR 1 : 15
ROTOR 2 : 22
ROTOR 3 : 09
ROTOR 4 : 41
ROTOR 5 : 87
ROTOR 6 : 36
ROTOR 7 : 08
ROTOR 8 : 01
ROTOR 9 : 57
ROTOR 10 : 91
ROTOR 11 : 03
ROTOR 12 : 49

REVERSING ROTOR : 77

---------- Figure 6----------

c. The Superencipherment Table number (1 to 100) if used, and

d. The initial setting of the superencipherment table counter (1 to 6). (Figure 7)

(See your list)

ENTER SUPERENCIPHERMENT TABLE NUMBER : 35

SET INITIAL COUNT (1 TO 6) : 4

---------- Figure 7----------

6. The opening screen for beginning the message entry appears with: (Figure 8)
a. The External Checksum.
b. Instructions for starting and stopping text entry and making corrections.

ENTERNAL CHECKSUM = 99

To stop operations and :

1. Print text : Press \

2. Correct input : Press Shift & |

Press ENTER key to start - or - to make the next screen

---------- Figure 8----------

7. After pressing <enter>, a blank screen will appear with the initial Rotor Display at the bottom and START ENTERING MESSAGE will appear in the middle of the screen. (Figure 9)

START ENTERING MESSAGE

Rotor Display 15 22 09 41 87 36 08 01 57 91 03 49 77

---------- Figure 9----------

8. At this point you can start entering text and see it appear on the monitor, starting at the upper left corner, and filling left to right. The input and its related output will appear simultaneously. At the bottom of the screen, above the rotor display, are instructions for ending the input and for making corrections to the input. There is also a count of input at the right corner. (Figure 10)

F O U R S C O R E A N D S E V E N Y E A R S
A
FM VQ ND OU UF OF EN MX FE ZR DO YD BS YW VO RB BB HC QI UR ZD BW BZ TQ EO
WD RF

G O , O U R F
FW DP JA XW QN ZX OT DA WX

Enter '\' to end message. Press 'Shift |' to make correction. Input No. 36
Rotor Display 41 73 31 61 44 79 62 00 11 72 25 67 04

---------- Figure 10----------

Below is a listing (in columns 4 through 16) of the 13 Rotor Display windows of the above 36 inputs, to show the intermittent movement of the rotors. See Figures 11 and 12.
Col. 1 is the Input No.
Col. 2 is the cleartext input.
Col. 3 is the Character Set conversion of the cleartext.
Cols. 4 - 15 are the Regular Rotor displays.
Col. 16 is the Reversing Rotor display.
Col. 17 is the numeric cipher output.
Col. 18 is the superenciphered output.

When numbers are repeated in a rotor column, this indicates that the rotor did not rotate after that specific input. When rotation does occur, it rotates the amount previously set for that rotor. This illustration is not part of the regular operating display. It was used only as a test and to illustrate intermittent movement.

Start			15	22	09	41	87	36	08	01	57	91	03	49	77	
			--	--	--	--	--	--	--	--	--	--	--	--	--	
1	F	87	15	51	10	12	87	49	19	48	60	52	03	68	08	52
FM																
2	O	26	15	51	11	83	87	49	19	48	63	52	03	68	39	18
VQ																
3	U	64	15	51	12	54	04	62	19	48	66	52	03	68	70	06
ND																
4	R	57	15	51	13	54	21	62	30	48	69	13	26	87	01	15
OU																
5	S	79	22	80	14	25	21	62	30	95	69	13	26	06	32	03
UF																
6	C	10	29	09	15	96	21	75	41	42	69	74	49	06	32	64
OF																
7	O	81	29	09	15	96	38	75	41	42	69	35	49	06	32	69
EN																
8	R	01	36	38	15	67	38	75	52	42	69	35	72	25	32	03
MX																
9	E	65	36	38	15	38	38	75	63	42	72	96	72	44	32	92
FE																
10		06	43	67	16	09	55	88	74	89	75	96	72	63	32	37
ZR																
11	A	20	50	67	16	80	72	88	74	89	78	57	72	82	63	53
DO																
12	N	12	50	96	16	80	89	88	85	89	81	18	95	01	94	34
YD																
13	D	61	57	25	17	80	89	88	85	89	81	79	18	01	94	46
BS																
14		50	57	25	18	51	06	88	96	89	81	79	18	20	94	93
YW																
15	S	89	64	25	18	51	06	01	96	36	84	79	18	39	25	42

VO

16	E	42	64	54	19	22	23	14	96	36	84	40	18	39	25	65

RB

17	V	71	64	83	20	22	23	27	96	36	84	01	41	58	25	13

BB

18	E	64	64	83	21	93	40	40	96	83	84	62	64	77	56	66

HC

19	N	89	64	83	21	93	57	40	96	83	87	62	87	77	56	53

QI

20		16	71	12	22	64	57	53	07	30	87	62	10	96	56	20

UR

21	Y	84	71	12	22	64	74	53	07	30	90	23	10	15	56	60

ZD

22	E	8	78	12	22	35	91	66	07	77	93	23	10	34	56	93

BW

23	A	52	78	12	23	06	08	66	07	77	96	84	10	53	56	80

BZ

24	R	77	85	41	24	06	25	66	07	24	96	84	10	72	87	39

TQ

25	S	99	92	41	25	06	42	66	18	71	96	84	10	91	18	55

EO

26		82	92	70	25	06	59	66	29	18	96	84	33	10	18	20

WD

27	A	96	92	99	25	77	59	66	29	18	96	45	33	10	49	92

RF

28	G	65	99	99	26	77	76	66	29	65	99	06	33	29	49	01

FW

29	O	23	99	28	26	77	76	66	40	12	02	67	33	48	49	01

DP

30	'	36	06	57	27	77	93	66	40	59	05	28	56	67	80	65

JA

31		37	13	86	27	48	10	66	40	59	05	89	79	67	11	59

XW

32	O	56	20	15	28	19	10	66	40	06	08	50	79	67	11	18

QN

33	U	94	27	15	28	19	27	66	40	06	08	50	02	67	11	38

ZX

34	R	87	34	44	29	90	27	79	40	53	11	50	02	67	42	34

OT

35		81	34	44	30	61	27	79	51	53	11	11	02	67	73	28

DA

36	F	72	41	73	31	61	44	79	62	00	11	72	25	67	04	17

WX

---------- Figure 11----------

Figure 12 is the same as Figure 11 except that the repeated numbers in each column have been replaced by a [] to indicate no movement to emphasize the irregular movement of each rotor.

	Rotor No.		01	02	03	04	05	06	07	08	09	10	11	12	RR		
	Rotation		7	29	1	71	17	13	11	47	3	61	23	19	31		
	Start Posn		15	22	09	41	87	36	08	01	57	91	03	49	77		
			--	--	--	--	--	--	--	--	--	--	--	--	--		
1	F	87	[]	51	10	12	[]	49	19	48	60	52	[]	68	08	52	FM
2	O	26	[]	[]	11	83	[]	[]	[]	[]	63	[]	[]	[]	39	18	VQ
3	U	64	[]	[]	12	54	04	62	[]	[]	66	[]	[]	[]	70	06	ND
4	R	57	[]	[]	13	[]	21	[]	30	[]	69	13	26	87	01	15	OU
5	S	79	22	80	14	25	[]	[]	[]	95	[]	[]	[]	06	32	03	UF
6	C	10	29	09	15	96	[]	75	41	42	[]	74	49	[]	[]	64	OF
7	O	81	[]	[]	[]	[]	38	[]	[]	[]	[]	35	[]	[]	[]	69	EN
8	R	01	36	38	[]	67	[]	[]	52	[]	[]	[]	72	25	[]	03	MX
9	E	65	[]	[]	[]	38	[]	[]	63	[]	72	96	[]	44	[]	92	FE
10		06	43	67	16	09	55	88	74	89	75	[]	[]	63	[]	37	ZR
11	A	20	50	[]	[]	80	72	[]	[]	[]	78	57	[]	82	63	53	DO
12	N	12	[]	96	[]	[]	89	[]	85	[]	81	18	95	01	94	34	YD
13	D	61	57	25	17	[]	[]	[]	[]	[]	[]	79	18	[]	[]	46	BS
14		50	[]	[]	18	51	06	[]	96	[]	[]	[]	[]	20	[]	93	YW
15	S	89	64	[]	[]	[]	[]	01	[]	36	84	[]	[]	39	25	42	VO
16	E	42	[]	54	19	22	23	14	[]	[]	[]	40	[]	[]	[]	65	RB
17	V	71	[]	83	20	[]	[]	27	[]	[]	[]	01	41	58	[]	13	BB
18	E	64	[]	[]	21	93	40	40	[]	83	[]	62	64	77	56	66	HC
19	N	89	[]	[]	[]	[]	57	[]	[]	[]	87	[]	87	[]	[]	53	QI
20		16	71	12	22	64	[]	53	07	30	[]	[]	10	96	[]	20	UR

```
        21  Y  84    []  []  []  []  74  []  []  []  90  23  []  15  []    60
ZD
        22  E   8    78  []  []  35  91  66  []  77  93  []  []  34  []    93
BW
        23  A  52    []  []  23  06  08  []  []  []  96  84  []  53  []    80
BZ
        24  R  77    85  41  24  []  25  []  []  24  []  []  []  72  87    39
TQ
        25  S  99    92  []  25  []  42  []  18  71  []  []  []  91  18    55
EO
        26     82    []  70  []  []  59  []  29  18  []  []  33  10  []    20
WD
        27  A  96    []  99  []  77  []  []  []  []  []  45  []  []  49    92
RF
        28  G  65    99  []  26  []  76  []  []  65  99  06  []  29  []    01
FW
        29  O  23    []  28  []  []  []  []  40  12  02  67  []  48  []    01
DP
        30  '  36    06  57  27  []  93  []  []  59  05  28  56  67  80    65
JA
        31     37    13  86  []  48  10  []  []  []  []  89  79  []  11    59
XW
        32  O  56    20  15  28  19  []  []  []  06  08  50  []  []  []    18
QN
        33  U  94    27  []  []  []  27  []  []  []  []  []  02  []  []    38
ZX
        34  R  87    34  44  29  90  []  79  []  53  11  []  []  []  42    34
OT
        35     81    []  []  30  61  []  []  51  []  []  11  []  []  73    28
DA
        36  F  72    41  73  31  []  44  []  62  00  []  72  25  []  04    17
WX
```

[] = no movement (repeated numbers)

---------- Figure 12----------

9. Corrections are made by pressing the " shift and | " keys simultaneously.
Light magenta numbers appear between the lines of input and output so that you can identify where the error is. This position number (note 37 below) is entered (Figure 13).

```
F  O  U  R  S  C  O  R  E     A  N  D     S  E  V  E  N     Y  E  A  R  S     A
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
FM VQ ND OU UF OF EN MX FE ZR DO YD BS YW VO RB BB HC QI UR ZD BW BZ TQ EO WD RF
```

```
G  O  ,     O  U  R     F  U  R  F  A  Y  T  H  E  R  S
28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54
FW DP JA XW QN ZX OT DA WX MG LY QW KM WQ EL WM DG XB HY

55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81


82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 00 01 02 03 04 05 06 07 08


09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35


36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62

   Enter '\' to end message.   Press 'Shift |' to make correction. Input No. 46
   ENTER THE (FIRST) POSITION TO CORRECT 37
```

---------- Figure 13----------

10. The <enter> key is pressed twice. The screen will blank and then automatically refill with "good" text up to that number and stop. CONTINUE ENTERING MESSAGE will appear in the middle of the screen. Entry of correct text is then continued from that point onwards (Figure 14).

```
F  O  U  R  S  C  O  R  E     A  N  D     S  E  V  E  N     Y  E  A  R  S     A

FM VQ ND OU UF OF EN MX FE ZR DO YD BS YW VO RB BB HC QI UR ZD BW BZ TQ EO WD RF

  ---------------------------------------------------------------------------
G  O  ,     O  U  R     F

FW DP JA XW QN ZX OT DA WX


                    CONTINUE ENTERING MESSAGE

   Enter '\' to end message.   Press 'Shift |' to make correction.  Input No. 36
   Rotor Display  41  73  31  61  44  79  62  00  11  72  25  67  04
```

---------- Figure 14----------

11. When the first screen is filled (162 characters input) or is ended with a backslash (\ ), the above control settings, etc. are printed, followed by the text screen. As each subsequent screenful is completed it will be printed. This continues until the end of the message is reached and the backslash (\ ) key is pressed. This causes any partial screen to be printed before the message control data, message form and other output is printed.

If Decipherment (2) is selected, the process is essentially the same (entering control settings, etc.) except the input is ciphertext and the output is cleartext. Message Control Data is available but message analysis is not.

ROTORS, SETS AND TABLES

The term "data files" encompasses the files that constitute the 100 each groupings of Regular Rotors, Reversing Rotors, Character Sets and Superencipherment Tables that are used by Enigma 95. They have been described earlier and now they are presented for inspection. They were used in the examples discussed earlier.

```
A  From  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
         -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- - -- --
B  To   58 28 56 40 80 78 05 92 49 31 14 93 30 77 62 64 79 25 13 22 41 65 29 43 39

A  From 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
         -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- - -- --
B  To   51 19 73 02 01 42 83 94 08 69 04 07 66 57 84 26 54 44 09 68 85 52 34 03 46

A  From 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75
         -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- - -- --
B  To   27 10 17 70 37 23 06 38 59 97 91 71 95 88 96 32 45 18 82 53 61 99 81 12 16

A  From 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 00
         -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- - -- --
B  To   36 60 24 48 67 33 11 72 63 76 21 75 87 86 00 50 47 35 98 90 89 74 20 55 15
```

Figure 15 - Regular Rotor No. 32

The "To" position indicates the position on the rotor's opposite face to achieve the offset effect. (For example, position 1 on face A is connected to position 58 on face B)

```
   From  01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
         -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- - -- --
   To    48 65 34 39 86 95 82 51 12 71 17 09 90 26 43 42 11 91 67 60 59 89 87 25 24

   From  26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
         -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- - -- --
   To    14 83 78 99 72 77 61 35 03 33 53 57 97 04 50 96 16 15 93 49 62 54 01 45 40

   From  51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75
         -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- - -- --
   To    08 70 36 47 63 69 37 73 21 20 32 46 55 85 02 00 19 92 56 52 10 30 58 79 84

   From  76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 00
         -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- - -- --
   To    98 31 28 74 94 88 07 27 75 64 05 23 81 22 13 18 68 44 80 06 41 38 76 29 66
```

Figure 16 - Reversing Rotor No. 53

The "To" position indicates the connecting position on the same face to achieve the offset effect. (For example, Positions 1 and 48 are connected, 2 and 65 are connected, etc.)

Posn	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
Char	#	q	.	c	j	t		+	9	A	*	4	f	r	O	~	,	{	8	d

Posn	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Char	y	o	5	R	n	h	w	X	D	p	g	M	~	3	S	e	m	l	T	-

Posn	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
Char	[	U	1	&	@	/	z	~	~	Q	a	=	P	!	C	7	~	O	K	u

Posn	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
Char	B	'	~	Y	s	b	<	G	W	v	?	I	~	H	(	>	E	:	~	x

Posn	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00
Char	}	L	J	~	k	Z	F	~	_	)	N	~	2	;	V	i	6	]	%	$

Figure 17 - Character Set No. 44

"Posn" is the position value the Character is converted to when it is input. The characters "rotate" afterwards so that character position values change. This figure shows the set before the first input.

Letter "A" = 10 initially. After the first input, "A" = "99", then "88" (For a rotation values of 89), etc.

	01	02	03	04	05	06	07
01	HO	HI	BV	FW	DP	PX	BK
02	EF	DS	SJ	QJ	MK	BH	GS
03	BG	HD	EP	UF	MX	YB	WV
04	JG	OO	TI	QW	UJ	IQ	
05	VW	ZL	BX	LD	KF	TL	CM
06	DQ	XZ	CK	ND	AM	MH	LE
07	WO	FH	PT	FY	WN	GN	SI
08	UW	FN	RA	YU	YR	ZZ	
09	WB	DZ	OJ	LU	QL	WZ	SK
10	XG	KL	OB	RE	QP	UQ	JH
11	FU	WI	QS	MP	UX	ZH	IF
12	KP	OA	SF	IG	SO	FS	
13	CY	BJ	TJ	BB	KQ	WE	PA
14	NK	BQ	HA	HU	FG	XS	CN
15	VU	FI	UB	OU	YV	GT	PH
16	UH	PI	RU	LC	HB	NJ	
17	LQ	NM	UD	WX	WM	EH	PQ
18	CF	HM	DY	VQ	QN	HW	AS
19	JV	CX	ED	XC	OG	ID	KS
20	HH	AX	AJ	UR	WD	MY	
21	YY	KA	NF	AI	VT	ZO	TM
22	ER	DX	JF	QK	TF	MA	FT
23	HF	OH	DC	VM	VD	VG	RR
24	JX	FZ	SD	UZ	DN	FX	
25	RG	PG	HX	RM	IJ	RQ	LZ
26	KX	YA	GO	XQ	OM	FD	NC
27	IA	BP	PZ	II	KH	PP	IO
28	MM	UL	IT	DA	GQ	IB	
29	IW	CU	IC	GI	KY	BR	CL
30	KJ	PL	JE	DJ	RT	XU	PU
31	CE	JK	WS	UT	AD	AK	JJ
32	UK	XJ	PR	JY	XY	SQ	
33	WL	KV	LG	YM	NR	BA	EB
34	IP	CR	LB	YD	OT	XB	GC
35	QU	YP	JT	VB	KT	AR	VI
36	HK	UM	RY	AU	ZM	BI	
37	MZ	PD	YK	ZR	UE	JL	NA
38	OC	TZ	DF	ZX	CC	NB	IS
39	BF	XE	NH	TQ	HN	SE	JM
40	SL	LI	WF	NQ	NN	XT	
41	MF	MC	WH	OZ	VE	ZG	AG
42	HG	GD	GG	VO	OQ	UO	HS
43	HL	SM	VF	SZ	PW	HV	RL
44	KW	JQ	SN	ZB	BD	VZ	
45	WY	EZ	SB	AZ	GW	ZS	ZF
46	OP	NE	GP	BS	RS	CO	HQ
47	LK	YJ	IN	ZJ	XH	CI	PC
48	RI	WT	FF	RP	SH	EX	
49	MT	XD	ZE	WR	AF	DH	RZ
50	DK	ZK	UI	JP	VV	HT	TP

	01	02	03	04	05	06	07
51	AO	YC	JI	VC	CT	ET	IX
52	DD	NO	NL	FM	XA	EM	
53	NT	PJ	CJ	DO	QI	AN	FC
54	TD	VR	TV	QG	EE	JU	RK
55	QD	GE	MD	EO	OX	JW	IH
56	XP	BL	UN	FQ	KR	MV	
57	OL	CH	SU	NI	GX	HZ	DU
58	MS	MJ	FA	EW	TY	YX	WJ
59	VA	TO	OI	XW	ZQ	ZA	WG
60	RJ	IK	YH	ZD	SR	HJ	
61	MO	AA	NZ	AP	IV	JB	VS
62	DE	LF	FO	UP	EV	CB	GB
63	GH	UV	IM	OE	XL	ST	QF
64	GF	TX	NS	OF	NU	VY	
65	SG	KC	MN	RB	JA	KE	TE
66	VX	CW	QO	HC	BM	SC	ES
67	VJ	PF	QQ	QR	LS	XI	BE
68	LJ	LV	ZT	LY	DM	WC	
69	JN	YG	XV	EN	FL	AB	TT
70	VP	AT	GL	PO	KI	IY	WK
71	ME	UU	SX	XN	RN	HE	KD
72	YI	QA	GA	EL	KO	QH	
73	LX	CS	FK	PE	JO	YN	VK
74	WU	LT	DR	ZC	IE	BC	XK
75	XR	US	KG	EQ	JZ	QT	MB
76	CP	IU	PK	ZN	IZ	AW	
77	GU	QB	EY	ZV	LM	XF	TG
78	EC	SS	VH	NP	PS	ZI	ON
79	MR	TU	NW	AY	QM	ZY	BY
80	QC	OD	RW	BZ	CZ	SW	
81	ZP	SA	XO	YZ	NG	EU	QE
82	GJ	ZW	RX	RH	EK	AC	JC
83	TA	OS	KZ	CQ	UA	WP	AV
84	TK	OW	AH	UY	HP	DW	
85	FR	WW	PY	KM	WQ	MQ	LN
86	SY	GZ	TR	RC	BO	UC	EI
87	AQ	DV	RD	YL	RO	PM	KK
88	KU	CA	CQ	MG	QV	YS	
89	NV	BU	GK	EJ	GR	LW	MW
90	PB	OR	TB	RV	VN	CV	VL
91	DL	TN	DB	LP	YO	LH	LL
92	QZ	DI	XM	FE	RF	WA	
93	YQ	MI	NX	YW	BW	PN	GY
94	LO	JS	GV	YE	ML	YT	FP
95	OV	JD	DT	DG	QX	PV	JR
96	NY	EA	MU	AL	FJ	CD	
97	OY	KB	ZU	HY	GM	QY	TW
98	FB	TS	HR	UG	TH	BN	IL
99	EG	YF	IR	LR	SP	TC	LA
00	AE	KN	SV	FV	XX	BT	OK

Figure 18 - Superencipherment Table No. 35
The left column is the numeric cipher. The other 7 columns are the possible super

encipherments. 36 can be converted to HK , UM , RY , AU , ZM , BI in turn, depending on where the counter starts. A blank causes the counter to be reset to 1.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	61	69	82	31	00	49	41	84	21	20	31	96	06	53	51	61	87	35	18	70	36	83	76	20	79	45	A
B	33	13	74	44	67	39	03	02	36	13	01	56	66	98	86	27	14	29	46	00	89	01	93	05	79	80	B
C	88	62	38	96	31	18	88	57	47	53	06	29	05	14	46	76	83	34	73	51	29	90	66	19	13	80	C
D	28	91	23	52	62	38	95	49	92	30	50	91	68	24	53	01	06	74	02	95	57	87	84	22	18	09	D
E	96	33	78	19	54	02	99	17	86	89	82	72	52	69	55	03	75	22	66	51	81	62	58	48	77	45	E
F	58	98	53	26	92	48	14	07	15	96	73	69	52	08	62	94	56	85	12	22	11	00	01	24	07	24	F
G	72	62	34	42	55	64	42	63	29	82	89	70	97	07	26	46	28	89	02	15	77	94	45	57	93	86	G
H	14	16	66	03	71	23	42	20	01	60	36	43	18	39	01	84	46	98	42	50	14	43	18	25	97	57	H
I	27	28	29	19	74	11	12	55	27	25	60	98	63	47	27	34	04	99	38	28	76	61	29	51	70	76	I
J	65	61	82	95	30	22	04	10	51	31	31	37	39	69	73	50	44	95	94	35	54	19	55	24	32	75	J
K	21	97	65	71	65	05	75	27	70	30	87	10	85	00	72	12	13	56	19	35	88	33	44	26	29	83	K
L	99	34	16	05	06	62	33	91	40	68	47	91	77	85	94	91	17	99	67	74	09	68	89	73	68	25	L
M	22	75	41	55	71	41	88	06	93	58	02	94	28	65	61	11	85	79	58	49	96	56	89	03	20	37	M
N	37	38	26	06	46	21	81	39	57	16	14	52	17	40	52	78	40	33	64	53	64	89	79	93	96	61	N
O	12	10	38	80	63	64	19	23	59	09	00	57	26	78	04	46	42	90	83	34	15	95	84	55	97	41	O
P	13	90	47	37	73	67	25	15	16	53	76	30	87	93	70	27	17	32	78	07	30	95	43	01	85	27	P
Q	72	77	80	55	81	63	54	72	53	02	22	09	79	18	66	10	67	67	11	75	35	88	04	95	97	92	Q
R	08	65	86	87	10	92	25	82	48	60	54	43	25	71	87	48	25	23	46	30	16	90	80	82	36	49	R
S	81	45	66	24	39	12	65	48	07	02	09	40	43	44	12	99	32	60	78	63	57	00	80	71	86	43	S
T	83	90	99	54	65	22	77	98	04	13	84	05	21	91	59	50	39	86	98	69	79	54	97	64	58	38	T
U	83	15	86	17	37	03	98	16	50	04	32	28	36	56	42	62	10	20	75	31	71	63	08	11	84	24	U
V	59	35	51	23	41	43	23	78	35	67	73	90	23	90	42	70	18	54	61	21	15	50	05	66	64	44	V
W	92	09	68	20	13	40	59	41	11	58	70	33	17	07	07	83	85	49	31	48	74	03	85	17	45	09	W
X	52	34	19	49	39	77	10	47	67	32	74	63	92	71	81	56	26	75	14	40	30	69	59	00	32	06	X
Y	26	03	51	34	94	99	69	60	72	47	37	87	33	73	91	35	93	08	88	94	08	15	93	58	21	81	Y
Z	59	44	74	60	49	45	41	11	78	47	50	05	36	76	21	81	59	37	45	68	97	77	82	38	79	08	Z
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

Figure 19 - Superdecipherment Table 35
First letter at left. Second letter at top. Numeric cipher at intersection (HK, UM, RY, etc. = 36)

The Enigma rotor operation principle has probably been long superseded by much more sophisticated methods of encryption that are faster and more secure, but it will remain interesting for a long time to amateurs such as myself. It is something that is understandable and before the advent of the computer, resulted in some beautiful machines.

The Enigma 95 is not one now, but I believe that it could be "translated" into a handsome electro-mechanical device. It is something to dream about.

The only absolutely secure cipher is the One Time Pad and it has the disadvantage of requiring copies to be destroyed after one use. The Enigma 95 is an attempt to approach this holy Grail of cryptography by providing an almost unlimited supply of enhanced (both in size and method of rotation) Rotors, Character Sets, Superencipherment Tables and a lengthened Plugboard. While I cannot prove it mathematically or otherwise, I suspect that the ability to use almost unlimited expendable sets of all possible combinations of these for very limited periods (throw away feature) such as is possible in the Enigma 95, would strengthen any cipher

considerably by preventing the accumulation of sufficient material on which to base an in-depth cryptanalysis. Any comments would appreciated.

AT THE CRYPTO DROP BOX IS:

The disk accompanying this article contains ENIGMA 95 and the necessary supporting files needed in its operation. Also included are program files to create them and to analyze and test its operation. DOC files are included for each file to explain them. Start with CRYPTO.1ST, then read ENIGMA95.DOC and study ENIGMA95.FLO to gain an understanding of Enigma 95 before running it. The list of files is:

```
CRYPTO.1ST          : An outline of the files that constitute Enigma 95 system
ENIGMA95.DOC        : Detailed documentation pertaining to ENIGMA95
ENIGMA95.FLO        : A flowchart of the ENIGMA95 operation
ENIGMA95.BAS  *     : ENIGMA95

ROTORS.DAT          : Set of 100 Regular Rotors
REVROTRS.DAT        : Set of 100 Reversing Rotors
CHARS.DAT           : Set of 100 Character Sets
CODE.DAT            : Set of 100 Super Encipherment Tables

CRYPTO05.BAS  *  : Random Numbers Generator for CRYPTO27 & CRYPTO34
CRYPTO27.BAS  *  : Regular Rotor Creation using the Interval Method
CRYPTO28.BAS  *  : Super Encipherment Tables Creation
CRYPTO30.BAS  *  : Character Set Creation
CRYPTO34.BAS  *  : Reversing Rotor Creation

CRYPTO43.BAS  *  : ENIGMA95 Cipher Machine Data Paths Demonstrator
CRYPTO45.BAS  *  : Rotors Matching Analysis
CRYPTO47.BAS  *  : Check of Rotor Files for Errors
CRYPTO48.BAS  *  : Analysis of Cleartext vs. Ciphertext
CRYPTO49.BAS  *  : Rotor Intermittent Movement Test
CRYPTO51.BAS     : Plugboard Combinations

ENIGMA95.WRI     : The article about Enigma 95.  ( Created using Windows 3.1 Write )

          * = Has a matching .DOC file

    The .1st , .DOC and .FLO files are DOS files
        The .BAS and .DAT files are QBASIC or QUICKBASIC  files
        The .WRI file is a WINDOWS 3.1 Write file

ENCRYPTION                                10-31-1995  16:36:57  Hours
-------------------------------------------------------------------------------
No. of PB Connections     21
Plugboard Connections     (1735)  (2356)  (4581)  (9852)  (3377)  (5544)  (6612)
                          (5987)  (3254)  (6791)  (2653)  (4899)  (6250)  (4069)
                          (3180)  (9402)  (8437)  (9307)  (8843)  (8514)  (2176)
No. of Rotors             12
Rotors Sequence           32  49  42  98  63  94  62  60  04  33  25  11
Rotors Orientation        1   2   1   1   2   2   1   1   2   2   1   1
Reversing Rotor No.       53
Rotors Rotation Values    07  29  01  71  17  13  11  47  03  61  23  19
Rev Rotor Rotation Value  31
Character Set (CS) No.    44
CS Rotation Value         89                      Internal Checksum  60354
-------------------------------------------------------------------------------
Rotors Initial Settings   15  22  09  41  87  36  08  01  57  91  03  49
Rev Rotor Initial Setting 77
External Checksum         64
-------------------------------------------------------------------------------
```

```
F  O  U  R  S  C  O  R  E     A  N  D     S  E  V  E  N     Y  E  A  R  S     A
52 18 06 15 03 64 69 03 92 37 53 34 46 93 42 65 13 66 53 20 60 93 80 39 55 20 92
-------------------------------------------------------------------------------
G  O  ,     O  U  R     F  O  R  E  F  A  T  H  E  R  S     B  R  O  U  G  H  T
01 01 65 59 18 38 34 28 17 43 63 98 60 64 41 31 11 13 56 20 34 65 57 72 73 95 10
-------------------------------------------------------------------------------
   F  O  R  T  H     U  P  O  N     T  H  I  S     C  O  N  T  I  N  E  N  T
53 19 21 23 57 21 59 32 96 45 50 23 79 29 01 92 30 12 30 42 04 58 82 66 86 40 28
-------------------------------------------------------------------------------
A     N  E  W     N  A  T  I  O  N  .     1  2  3  4  5  6  7  8  9  0  (  *  )
27 86 23 88 28 11 26 30 91 76 90 06 96 83 85 74 48 64 96 82 80 53 00 59 25 74 73
-------------------------------------------------------------------------------
```

TOTAL INPUT CHARACTERS IS 108 HASH TOTAL OF CODE IS 02

EXHIBIT A-1

COL CHECK TOTALS
33 24 15 85 06 34 88 93 96 01 56 61 81 69 69 62 02 55 35 64 78 69 19 36 39 29 03
TOTAL COLUMNS = 5202
ROW CHECK TOTALS
83 67 78 74
TOTAL ROWS = 5202

EXHIBIT A-2

========== SEPARATE PAGE ==========

FOR TRANSMISSION AS MESSAGE No.

---

15 22 09 41 87 36 08 01 57 91 03 49 77 64 10 31 95 16 36 57

---

52 18 06 15 03 64 69 03 92 37 53 34 46 93 42 65 13 66 53 20 60 93 80 39 55 20 92
01 01 65 59 18 38 34 28 17 43 63 98 60 64 41 31 11 13 56 20 34 65 57 72 73 95 10
53 19 21 23 57 21 59 32 96 45 50 23 79 29 01 92 30 12 30 42 04 58 82 66 86 40 28
27 86 23 88 28 11 26 30 91 76 91 06 96 83 85 74 48 64 96 82 80 53 00 59 25 74 73

108 02

Column and row totals. Do not transmit unless requested.
33 24 15 85 06 34 88 93 96 01 56 61 81 69 69 62 02 55 35 64 78 69 19 36 39 29 03
83 67 78 74

EXHIBIT A-3
INPUT FREQUENCY ANALYSIS

Char	Freq	Char	Freq	Char	Freq	Char	Freq	Char	Freq
A	6	U	4	;		k		?	
B	1	V	1	'		l		(	1
C	2	W	1	=		m		)	1
D	1	X		!		n		{	
E	8	Y	1	@		o		}	
F	4	Z		#		p		<	
G	2	0	1	$		q		>	
H	4	1	1	%		r		[	
I	3	2	1	&		s		]	
J		3	1	*	1	t		~	
K		4	1	a		u		~	
L		5	1	b		v		~	
M		6	1	c		w		~	
N	9	7	1	d		x		~	
O	10	8	1	e		y		~	
P	1	9	1	f		z		~	
Q		space	15	g		_		~	
R	8	.	1	h		-		~	
S	5	,	1	i		+		~	
T	7	:		j		/		~	

Total = 108

OUTPUT FREQUENCY ANALYSIS

Code Count	Code Count	Code Count	Code Count	Code Count
1 = 3	21 = 2	41 = 1	61 =	81 =
2 =	22 =	42 = 2	62 =	82 = 2
3 = 2	23 = 3	43 = 1	63 = 1	83 = 1
4 = 1	24 =	44 =	64 = 3	84 =
5 =	25 = 1	45 = 1	65 = 3	85 = 1
6 = 2	26 = 1	46 = 1	66 = 2	86 = 2
7 =	27 = 1	47 =	67 =	87 =
8 =	28 = 3	48 = 1	68 =	88 = 1
9 =	29 = 1	49 =	69 = 1	89 =
10 = 1	30 = 3	50 = 1	70 =	90 = 1
11 = 2	31 = 1	51 =	71 =	91 = 1
12 = 1	32 = 1	52 = 1	72 = 1	92 = 3
13 = 2	33 =	53 = 4	73 = 2	93 = 2
14 =	34 = 3	54 =	74 = 2	94 =
15 = 1	35 =	55 = 1	75 =	95 = 1
16 =	36 =	56 = 1	76 = 1	96 = 3
17 = 1	37 = 1	57 = 2	77 =	97 =
18 = 2	38 = 1	58 = 1	78 =	98 = 1
19 = 1	39 = 1	59 = 3	79 = 1	99 =
20 = 3	40 = 1	60 = 2	80 = 2	00 = 1

Total = 108

EXHIBIT A-4

DECRYPTION 10-31-1995 17:00:58 Hours

No. of PB Connections 21
Plugboard Connections (1735) (2356) (4581) (9852) (3377) (5544) (6612)
(5987) (3254) (6791) (2653) (4899) (6250) (4069)
(3180) (9402) (8437) (9307) (8843) (8514) (2176)
No. of Rotors 12
Rotors Sequence 32 49 42 98 63 94 62 60 04 33 25 11
Rotors Orientation 1 2 1 1 2 2 1 1 2 2 1 1
Reversing Rotor No. 53
Rotors Rotation Values 07 29 01 71 17 13 11 47 03 61 23 19
Rev Rotor Rotation Value 31
Character Set (CS) No. 44
CS Rotation Value 89 Internal Checksum 60354

Rotors Initial Settings 15 22 09 41 87 36 08 01 57 91 03 49
Rev Rotor Initial Setting 77
External Checksum 64

```
52 18 06 15 03 64 69 03 92 37 53 34 46 93 42 65 13 66 53 20 60 93 80 39 55 20 92
F  O  U  R  S  C  O  R  E     A  N  D     S  E  V  E  N     Y  E  A  R  S     A
-------------------------------------------------------------------------------
01 01 65 59 18 38 34 28 17 43 63 98 60 64 41 31 11 13 56 20 34 65 57 72 73 95 10
G  O  ,     O  U  R     F  O  R  E  F  A  T  H  E  R  S     B  R  O  U  G  H  T
-------------------------------------------------------------------------------
53 19 21 23 57 21 59 32 96 45 50 23 79 29 01 92 30 12 30 42 04 58 82 66 86 40 28
   F  O  R  T  H     U  P  O  N     T  H  I  S     C  O  N  T  I  N  E  N  T
-------------------------------------------------------------------------------
27 86 23 88 28 11 26 30 91 76 90 06 96 83 85 74 48 64 96 82 80 53 00 59 25 74 73
A     N  E  W     N  A  T  I  O  N  .     1  2  3  4  5  6  7  8  9  0  (  *  )
-------------------------------------------------------------------------------
```

TOTAL INPUT CHARACTERS IS 108 HASH TOTAL OF CODE IS 02

EXHIBIT B-1

COL CHECK TOTALS
33 24 15 85 06 34 88 93 96 01 56 61 81 69 69 62 02 55 35 64 78 69 19 36 39 29 03
TOTAL COLUMNS = 5202
ROW CHECK TOTALS
83 67 78 74
TOTAL ROWS = 5202

EXHIBIT B-2

========== SEPARATE PAGE ==========

Messsage No.----------From----------Date/Time of Receipt

: :

: / :
: :

: / :

FOURSCORE AND SEVEN YEARS AGO, OUR FOREFATHERS BROUGHT FORTH UPON THIS CONTINENT A NEW NAT

ION. 1234567890(*)

EXHIBIT B-3

```
ENCRYPTION                                10-31-1995  16:36:57  Hours
-------------------------------------------------------------------------------
No. of PB Connections     21
Plugboard Connections     (1735)  (2356)  (4581)  (9852)  (3377)  (5544)  (6612)
                          (5987)  (3254)  (6791)  (2653)  (4899)  (6250)  (4069)
                          (3180)  (9402)  (8437)  (9307)  (8843)  (8514)  (2176)
No. of Rotors             12
Rotors Sequence           32  49  42  98  63  94  62  60  04  33  25  11
Rotors Orientation        1   2   1   1   2   2   1   1   2   2   1   1
Reversing Rotor No.       53
Rotors Rotation Values    07  29  01  71  17  13  11  47  03  61  23  19
Rev Rotor Rotation Value  31
Character Set (CS) No.    44
CS Rotation Value         89                      Internal Checksum  60354
-------------------------------------------------------------------------------
Rotors Initial Settings   15  22  09  41  87  36  08  01  57  91  03  49
Rev Rotor Initial Setting 77
Super Encipher Table No.  35
External Checksum         99
-------------------------------------------------------------------------------
F  O  U  R  S  C  O  R  E     A  N  D     S  E  V  E  N     Y  E  A  R  S     A
FM VQ ND OU UF OF EN MX FE ZR DO YD BS YW VO RB BB HC QI UR ZD BW BZ TQ EO WD RF
-------------------------------------------------------------------------------
G  O  ,     O  U  R     F  O  R  E  F  A  T  H  E  R  S     B  R  O  U  G  H  T
FW DP JA XW QN ZX OT DA WX SZ OE UG SR NU OZ UT MP KQ FQ MY XB KE NI EL PE DG RE
-------------------------------------------------------------------------------
   F  O  R  T  H     U  P  O  N     T  H  I  S     C  O  N  T  I  N  E  N  T
AN XC AI VM GX VT ZQ JY AL AZ JP VD AY GI PX WA DJ IG RT OQ QW EW RH BM RC NQ GQ
-------------------------------------------------------------------------------
A     N  E  W     N  A  T  I  O  N  .     1  2  3  4  5  6  7  8  9  0  (  *  )
II BO VG MG IB UX XQ XU LP ZN RV AM FJ CQ KM ZC RP VY CD EK CZ FC FV ZA RM IE JO
-------------------------------------------------------------------------------
TOTAL INPUT CHARACTERS IS  108
```

EXHIBIT C-1

FOR TRANSMISSION AS MESSAGE No.

---

15 22 09 41 87 36 08 01 57 91 03 49 77 35 99 10 31 95 17 00 58

FM VQ ND OU UF OF EN MX FE ZR DO YD BS YW VO RB BB HC QI UR ZD BW BZ TQ EO WD RF

FW DP JA XW QN ZX OT DA WX SZ OE UG SR NU OZ UT MP KQ FQ MY XB KE NI EL PE DG RE

AN XC AI VM GX VT ZQ JY AL AZ JP VD AY GI PX WA DJ IG RT OQ QW EW RH BM RC NQ GQ

II BO VG MG IB UX XQ XU LP ZN RV AM FJ CQ KM ZC RP VY CD EK CZ FC FV ZA RM IE JO

108

EXHIBIT C-2

INPUT FREQUENCY ANALYSIS

Char	Freq	Char	Freq	Char	Freq	Char	Freq	Char	Freq
A	6	U	4	;		k		?	
B	1	V	1	'		l		(	1
C	2	W	1	=		m		)	1
D	1	X		!		n		{	
E	8	Y	1	@		o		}	
F	4	Z		#		p		<	
G	2	0	1	$		q		>	
H	4	1	1	%		r		[	
I	3	2	1	&		s		]	
J		3	1	*	1	t		~	
K		4	1	a		u		~	
L		5	1	b		v		~	
M		6	1	c		w		~	
N	9	7	1	d		x		~	
O	10	8	1	e		y		~	
P	1	9	1	f		z		~	
Q		space	15	g		_		~	
R	8	.	1	h		-		~	
S	5	,	1	i		+		~	
T	7	:		j		/		~	

Total = 108

OUTPUT FREQUENCY ANALYSIS

\2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Total
1\	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	-----
A									1			1	1	1											1	1	6
B		1											1		1				1				1			1	6
C				1													1									1	3
D	1						1			1					1	1											5
E											1	1		1	1								1				5
F			1		1					1			1				1					1	1				7
G									1								1							1			3
H			1																								1
I		1			1		1		1																		4
J	1														1	1									1		4
K					1								1				1										3
L																1											1
M							1									1								1	1		4
N				1					1								1				1						4
O					1	1											1			1	1					1	6
P					1																			1			2
Q									1					1									1				3
R		1	1		1	1		1					1			1				1		1					9
S																		1								1	2
T																	1										1
U						1	1											1		1				1			5
V				1			1						1		1		1			1					1		7
W	1			1																				1			3
X		1	1														1				1		1				5
Y				1																			1				2
Z	1		1	1										1			1	1						1			7
	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	-----
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Total
	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	-----
	4	4	5	6	6	3	5	1	5	2	1	2	6	4	5	5	10	3	1	4	3	2	6	6	4	5	108

EXHIBIT C-3

```
DECRYPTION                                  10-31-1995  17:36:57  Hours
-------------------------------------------------------------------------------
No. of PB Connections     21
Plugboard Connections     (1735)  (2356)  (4581)  (9852)  (3377)  (5544)  (6612)
                          (5987)  (3254)  (6791)  (2653)  (4899)  (6250)  (4069)
                          (3180)  (9402)  (8437)  (9307)  (8843)  (8514)  (2176)
No. of Rotors             12
Rotors Sequence           32  49  42  98  63  94  62  60  04  33  25  11
Rotors Orientation        1   2   1   1   2   2   1   1   2   2   1   1
Reversing Rotor No.       53
Rotors Rotation Values    07  29  01  71  17  13  11  47  03  61  23  19
Rev Rotor Rotation Value  31
Character Set (CS) No.    44
CS Rotation Value         89                    Internal Checksum  60354
-------------------------------------------------------------------------------
Rotors Initial Settings   15  22  09  41  87  36  08  01  57  91  03  49
Rev Rotor Initial Setting 77
Super Encipher Table No.  35
External Checksum         99
-------------------------------------------------------------------------------
FM VQ ND OU UF OF EN MX FE ZR DO YD BS YW VO RB BB HC QI UR ZD BW BZ TQ EO WD RF
F  O  U  R  S  C  O  R  E     A  N  D     S  E  V  E  N     Y  E  A  R  S     A
-------------------------------------------------------------------------------
FW DP JA XW QN ZX OT DA WX SZ OE UG SR NU OZ UT MP KQ FQ MY XB KE NI EL PE DG RE
G  O  ,     O  U  R     F  O  R  E  F  A  T  H  E  R  S     B  R  O  U  G  H  T
-------------------------------------------------------------------------------
AN XC AI VM GX VT ZQ JY AL AZ JP VD AY GI PX WA DJ IG RT OQ QW EW RH BM RC NQ GQ
   F  O  R  T  H     U  P  O  N     T  H  I  S     C  O  N  T  I  N  E  N  T
-------------------------------------------------------------------------------
A     N  E  W     N  A  T  I  O  N  .     1  2  3  4  5  6  7  8  9  0  (  *  )
II BO VG MG IB UX XQ XU LP ZN RV AM FJ CQ KM ZC RP VY CD EK CZ FC FV ZA RM IE JO
-------------------------------------------------------------------------------
TOTAL INPUT CHARACTERS IS  108
```

EXHIBIT D-1

Messsage No.----------From----------Date/Time of Receipt

: :

: / :
: :

: / :

FOURSCORE AND SEVEN YEARS AGO, OUR FOREFATHERS BROUGHT FORTH UPON THIS CONTINENT A NEW NAT

ION. 1234567890(*)

SOLUTIONS TO LECTURE 8 PROBLEMS

Thanks to GRAPE JUICE for the quick and clear reply:

C-1 Give two solutions to: (BE)**2 = ARE

A>0 , B= 1...3, E>0, R>0

(16) ** 2 = 256 and (31) ** 2 = 961

C-2 Square root: [OKLA] [OKLI]

```
              R, A, T, S          A= E+1 +4,9
             -----------          B
            |Q  UA  RT  ET        E
            -A                   I > A
             -----               O=O
             T  UA               Q >A, T
            -T  SI               R =2,3
             -----               S
                 U  RT           T
                -A  UT           U =S+1 > A, E
                 -----           T
                 E  AO  ET       U
                -E  ES  UB
                 ---------
                      R  AR

              2   4   1   7     4=4,9
             + ------------     9> 1
             | 5  84  21  31    3
             -4                 6
             ----------------   0=0
              1  84             5>4,1
             -1  76             2=2,3
             ----------------   7
                                1
                   8  21        8=7+1 >4,3 =7,8
                  -4  81        1
             ----------------   8

                   3  40  31
                  -3  37  89
             ----------------
                      2  42
```

```
A B E I O Q R S T U            1 2 3 4 5 6 7 8 9 0
                               T R E A Q I S U B O

A B E I O Q R S T U            0 1 2 3 4 5 6 7 8 9
                               O T R E A Q I S U B

A B E I O Q R S T U            0 9 8 7 6 5 4 3 2 1
                               O B U S I Q A E R T
```

```
A B E I O Q R S T U            9 8 7 6 5 4 3 2 1 0
                               B U S I Q A E R T O
```

>From Sinkov [SINK] two Hill system problems:

Hill-1

Decipher the message: YITJP GWJOW FAQTQ XCSMA ETSQU SQAPU SQGKC PQTYJ

Use the deciphering matrix

```
| 5  1 |
| 2  7 |
```

Let A =1, B=2... Z=26

P1 = 5(C1) + 1(C2)
P2 = 2(C1) + 7(C2)

5(Y) + 1(I) = 5(25) + 1(9) = 125 + 9 =134 MOD 26 = 4 = D
2(Y) + 7(I) = 2(25) + 7(9) = 50 + 63 =113 MOD 26 = 9 = I

5(T) + 1(J) = 5(20) + 1(10) = 100 + 10=110 MOD 26 = 6 = F
2(T) + 7(J) = 2(20) + 7(10) = 40 + 70 =110 MOD 26 = 6 = F

Difficulties are things that show what men are.

Hill-2

Decipher the message:
MWALO LIAIW WTGBH JNTAK QZJKA ADAWS SKQKU AYARN CSODN IIAES OQKJY B

Use the deciphering matrix | 2 23 |

use A=1, B=2, ...Z=26

P1 = 2(C1) +23(C2)
P2 = 21(C1) +7(C2)

2(M) + 23(W) =2(13) + 23(23) =26 + 529 = 555 MOD 26 = 9 = I
21(M) +7(W) =21(13) + 7(23) =273 + 161 = 434 MOD 26 =18 = R

2(A) + 23(L) = 2(1) + 23(12) = 2 + 276 = 278 MOD 26 = 18= R
21(A) +7(L) = 21(1) + 7(12) = 21 + 84 = 105 MOD 26 = 1 = A

Irrationally held truths may be more harmful than reasoned errors.

REFERENCES / RESOURCES [updated 10 March 1996]

[ACA] ACA and You, "Handbook For Members of the American Cryptogram Association," ACA publications, 1995.

[ACA1] Anonymous, "The ACA and You - Handbook For Secure Communications", American Cryptogram Association, 1994.

[ACM] Association For Computing Machinery, "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," Report of a Special Panel of ACM U. S. Public Policy Committee (USACM), June 1994.

[AFM] AFM - 100-80, Traffic Analysis, Department of the Air Force, 1946.

[ALAN] Turing, Alan, "The Enigma", by A. Hodges. Simon and Schuster, 1983.

[ALBA] Alberti, "Treatise De Cifris," Meister Papstlichen, Princeton University Press, Princeton, N.J., 1963.

[ALKA] al-Kadi, Ibrahim A., Origins of Cryptology: The Arab Contributions, Cryptologia, Vol XVI, No. 2, April 1992, pp 97-127.

[AND1] Andree, Josephine, "Chips from the Math Log," Mu Alpha Theta, 1966.

[AND2] Andree, Josephine, "More Chips from the Math Log," Mu Alpha Theta, 1970.

[AND3] Andree, Josephine, "Lines from the O.U. Mathematics Letter," Vols I,II,III, Mu Alpha Theta, 1971,1971,1971.

[AND4] Andree, Josephine and Richard V., "RAJA Books: a Puzzle Potpourri," RAJA, 1976.

[ANDR] Andrew, Christopher, 'Secret Service', Heinemann, London 1985.

[ANNA] Anonymous., "The History of the International Code.", Proceedings of the United States Naval Institute, 1934.

[ANN1] Anonymous., " Speech and Facsimile Scrambling and Decoding," Aegean Park Press, Laguna Hills, CA, 1981.

[ANTH] Anthony - Cave Brown, "Bodyguard of Lies", Harper and Row, New York, 1975.

[ASIR] Anonymous, Enigma and Other Machines, Air Scientific Institute Report, 1976.

[AUG1] D. A. August, "Cryptography and Exploitation of Chinese Manual Cryptosystems - Part I:The Encoding Problem", Cryptologia, Vol XIII, No. 4, October 1989.

[AUG2] D. A. August, "Cryptography and Exploitation of Chinese Manual Cryptosystems - Part II:The Encrypting Problem", Cryptologia, Vol XIV, No. 1, August 1990.

[BADE] Badeau, J. S. et. al., The Genius of Arab Civilization: Source of Renaissance. Second Edition. Cambridge: MIT Press. 1983.

[BAMF] Bamford, James, "The Puzzle Palace: A Report on America's Most Secret Agency," Boston, Houghton Mifflin, 1982.

[BARB] Barber, F. J. W., "Archaeological Decipherment: A Handbook," Princeton University Press, 1974.

[B201] Barker, Wayne G., "Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Course #201, Aegean Park Press, Laguna Hills, CA. 1982.

[BALL] Ball, W. W. R., Mathematical Recreations and Essays, London, 1928.

[BAR1] Barker, Wayne G., "Course No 201, Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Aegean Park Press, Laguna Hills, CA. 1975.

[BAR2] Barker, W., ed., History of Codes and Ciphers in the U.S. During the Period between World Wars, Part II, 1930 - 1939., Aegean Park Press, 1990.

[BAR3] Barker, Wayne G., "Cryptanalysis of the Hagelin Cryptograph, Aegean Park Press, 1977.

[BAR4] Barker, Wayne G., "Cryptanalysis of the Enciphered Code Problem - Where Additive method of Encipherment Has Been Used," Aegean Park Press, 1979.

[BARK] Barker, Wayne G., "Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Aegean Park Press, Laguna Hills, CA. 1973.

[BARR] Barron, John, "'KGB: The Secret Work Of Soviet Agents," Bantom Books, New York, 1981.

[BAUD] Baudouin, Captain Roger, "Elements de Cryptographie," Paris, 1939.

[BAZE] Bazeries, M. le Capitaine, " Cryptograph a 20 rondelles-alphabets," Compte rendu de la 20e session de l' Association Francaise pour l'Advancement des Scienses, Paris: Au secretariat de l' Association, 1892.

[BEES] Beesley, P., "Very Special Intelligence", Doubleday, New York, 1977.

[BLK] Blackstock, Paul W. and Frank L Schaf, Jr., "Intelligence, Espionage, Counterespionage and Covert Operations," Gale Research Co., Detroit, MI., 1978.

[BLOC] Bloch, Gilbert and Ralph Erskine, "Exploit the Double Encipherment Flaw in Enigma", Cryptologia, vol 10, #3, July 1986, p134 ff. (29)

[BLUE] Bearden, Bill, "The Bluejacket's Manual, 20th ed., Annapolis: U.S. Naval Institute, 1978.

[BODY] Brown, Anthony - Cave, "Bodyguard of Lies", Harper and Row, New York, 1975.

[BOLI] Bolinger, D. and Sears, D., "Aspects of Language," 3rd ed., Harcourt Brace Jovanovich,Inc., New York, 1981.

[BOSW] Bosworth, Bruce, "Codes, Ciphers and Computers: An Introduction to Information Security," Hayden Books, Rochelle Park, NJ, 1990.

[BOWE] Bowers, William Maxwell, "The Bifid Cipher, Practical Cryptanalysis, II, ACA, 1960.

[BOWN] Bowen, Russell J., "Scholar's Guide to Intelligence Literature: Bibliography of the Russell J. Bowen Collection," National Intelligence Study Center, Frederick, MD, 1983.

[BP82] Beker, H., and Piper, F., " Cipher Systems, The Protection of Communications", John Wiley and Sons, NY, 1982.

[BRAS] Brasspounder, "Language Data - German," MA89, The Cryptogram, American Cryptogram Association, 1989.

[BREN] Brennecke, J., "Die Wennde im U-Boote-Krieg:Ursachen und Folgren 1939 - 1943," Herford, Koehler, 1984.

[BROO] Brook, Maxey, "150 Puzzles in Cryptarithmetic," Dover, 1963.

[BRIT] Anonymous, "British Army Manual of Cryptography", HMF, 1914.

[BROG] Broglie, Duc de, Le Secret du roi: Correspondance secrete de Louis XV avec ses agents diplomatiques 1752-1774, 3rd ed. Paris, Calmann Levy, 1879.

[BRYA] Bryan, William G., "Practical Cryptanalysis - Periodic Ciphers -Miscellaneous", Vol 5, American Cryptogram Association, 1967.

[BURL] Burling, R., "Man's Many Voices: Language in Its Cultural Context," Holt, Rinehart & Winston, New York, 1970.

[CAND] Candela, Rosario, "Isomorphism and its Application in Cryptanalytics, Cardanus Press, NYC 1946.

[CAR1] Carlisle, Sheila. Pattern Words: Three to Eight Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1986.

[CAR2] Carlisle, Sheila. Pattern Words: Nine Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1986.

[CASE] Casey, William, 'The Secret War Against Hitler', Simon & Schuster, London 1989.

[CAVE] Cave Brown, Anthony, 'Bodyguard of Lies', Harper & Row, New York 1975.

[CCF] Foster, C. C., "Cryptanalysis for Microcomputers", Hayden Books, Rochelle Park, NJ, 1990.

[CHOI] Interview with Grand Master Sin Il Choi.,9th DAN, June 25, 1995.

[CHOM] Chomsky, Norm, "Syntactic Structures," The Hague: Mouton, 1957.

[CHUN] Chungkuo Ti-erh Lishih Tangankuan, ed "K'ang-Jih chengmien chanch'ang," Chiangsu Kuchi Ch'upansheh, 1987., pp993-1026.

[CI] FM 34-60, Counterintelligence, Department of the Army, February 1990.

[COUR] Courville, Joseph B., "Manual For Cryptanalysis Of The Columnar Double Transposition Cipher, by Courville Assoc., South Gate, CA, 1986.

[CLAR] Clark, Ronald W., 'The Man who broke Purple', Weidenfeld and Nicolson, London 1977.

[COLF] Collins Gem Dictionary, "French," Collins Clear Type Press, 1979.

[COLG] Collins Gem Dictionary, "German," Collins Clear Type Press, 1984.

[COLI] Collins Gem Dictionary, "Italian," Collins Clear Type Press, 1954.

[COLL] Collins Gem Dictionary, "Latin," Collins Clear Type Press, 1980.

[COLP] Collins Gem Dictionary, "Portuguese," Collins Clear Type Press, 1981.

[COLR] Collins Gem Dictionary, "Russian," Collins Clear Type Press, 1958.

[COLS] Collins Gem Dictionary, "Spanish," Collins Clear Type Press, 1980.

[COPP] Coppersmith, Don.,"IBM Journal of Research and Development 38, 1994.

[COVT] Anonymous, "Covert Intelligence Techniques Of the Soviet Union, Aegean Park Press, Laguna Hills, Ca. 1980.

[CREM] Cremer, Peter E.," U-Boat Commander: A Periscope View of The Battle of The Atlantic," New York, Berkley, 1986.

[CULL] Cullen, Charles G., "Matrices and Linear Transformations," 2nd Ed., Dover Advanced Mathematics Books, NY, 1972.

[DAGA] D'agapeyeff, Alexander, "Codes and Ciphers," Oxford University Press, London, 1974.

[DALT] Dalton, Leroy, "Topics for Math Clubs," National Council of Teachers and Mu Alpha Theta, 1973.

[DAN] Daniel, Robert E., "Elementary Cryptanalysis: Cryptography For Fun," Cryptiquotes, Seattle, WA., 1979.

[DAVI] Da Vinci, "Solving Russian Cryptograms", The Cryptogram, September-October, Vol XLII, No 5. 1976.

[DEAC] Deacon, R., "The Chinese Secret Service," Taplinger, New York, 1974.

[DEAU] Bacon, Sir Francis, "De Augmentis Scientiarum," tr. by Gilbert Watts, (1640) or tr. by Ellis, Spedding, and Heath (1857,1870).

[DELA] Delastelle, F., Cryptographie nouvelle, Maire of Saint- Malo, P. Dubreuil, Paris, 1893.

[DENN] Denning, Dorothy E. R.," Cryptography and Data Security," Reading: Addison Wesley, 1983.

[DEVO] Deavours, Cipher A. and Louis Kruh, Machine Cryptography and Modern Cryptanalysis, Artech, New York, 1985.

[DEV1] Deavours, C. A., "Breakthrough '32: The Polish Solution of the ENIGMA," Aegean Park Press, Laguna Hills, CA, 1988.

[DEV2] Deavours, C. A. and Reeds, J.,"The ENIGMA," CRYPTOLOGIA, Vol I No 4, Oct. 1977.

[DEV3] Deavours, C. A.,"Analysis of the Herbern cryptograph using Isomorphs," CRYPTOLOGIA, Vol I No 2, April, 1977.

[DIFF] Diffie, Whitfield," The First Ten Years of Public Key Cryptography," Proceedings of the IEEE 76 (1988): 560-76.

[DIFE] Diffie, Whitfield and M.E. Hellman,"New Directions in Cryptography, IEEE Transactions on Information Theory IT-22, 1976.

[DONI] Donitz, Karl, Memoirs: Ten Years and Twenety Days, London: Weidenfeld and Nicolson, 1959.

[DOW] Dow, Don. L., "Crypto-Mania, Version 3.0", Box 1111, Nashua, NH. 03061-1111, (603) 880-6472, Cost $15 for registered version and available as shareware under CRYPTM.zip on CIS or zipnet.

[EIIC] Ei'ichi Hirose, ",Finland ni okeru tsushin joho," in Showa gunji hiwa: Dodai kurabu koenshu, Vol 1, Dodai kurabu koenshu henshu iinkai, ed., (Toyko: Dodai keizai konwakai, 1987), pp 59-60.

[ELCY] Gaines, Helen Fouche, Cryptanalysis, Dover, New York, 1956.

[ENIG] Tyner, Clarence E. Jr., and Randall K. Nichols, "ENIGMA95 - A Simulation of Enhanced Enigma Cipher Machine on A Standard Personal Computer," for publication, November, 1995.

[EPST] Epstein, Sam and Beryl, "The First Book of Codes and Ciphers," Ambassador Books, Toronto, Canada, 1956.

[ERSK] Erskine, Ralph, "Naval Enigma: The Breaking of Heimisch and Triton," Intelligence and National Security 3, Jan. 1988.

[EVES] Eves, Howard, "An Introduction to the History of Mathematics, " New York, Holt Rinehart winston, 1964.

[EYRA] Eyraud, Charles, "Precis de Cryptographie Moderne'" Paris, 1953.

[FL] Anonymous, The Friedman Legacy: A Tribute to William and Elizabeth Friedman, National Security Agency, Central Security Service, Center for Cryptological History,1995.

[FLIC] Flicke, W. F., "War Secrets in the Ether," Aegean Park Press, Laguna Hills, CA, 1994.

[FOWL] Fowler, Mark and Radhi Parekh, " Codes and Ciphers, - Advanced Level," EDC Publishing, Tulsa OK, 1994. (clever and work)

[FREB] Friedman, William F., "Cryptology," The Encyclopedia Britannica, all editions since 1929. A classic article by the greatest cryptanalyst.

[FR1] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part I - Volume 1, Aegean Park Press, Laguna Hills, CA, 1985.

[FR2] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part I - Volume 2, Aegean Park Press, Laguna Hills, CA, 1985.

[FR3] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part III, Aegean Park Press, Laguna Hills, CA, 1995.

[FR4] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part IV, Aegean Park Press, Laguna Hills, CA, 1995.

[FR5] Friedman, William F. Military Cryptanalysis - Part I, Aegean Park Press, Laguna Hills, CA, 1980.

[FR6] Friedman, William F. Military Cryptanalysis - Part II, Aegean Park Press, Laguna Hills, CA, 1980.

[FRE] Friedman, William F. , "Elements of Cryptanalysis," Aegean Park Press, Laguna Hills, CA, 1976.

[FREA] Friedman, William F. , "Advanced Military Cryptography," Aegean Park Press, Laguna Hills, CA, 1976.

[FRAA] Friedman, William F. , "American Army Field Codes in The American Expeditionary Forces During the First World War, USA 1939.

[FRAB] Friedman, W. F., Field Codes used by the German Army During World War. 1919.

[FR22] Friedman, William F., The Index of Coincidence and Its Applications In Cryptography, Publication 22, The Riverbank Publications, Aegean Park Press, Laguna Hills, CA, 1979.

[FR6] Friedman, W. F., "Six Lectures On Cryptology," National Archives, SRH-004.

[FROM] Fromkin, V and Rodman, R., "Introduction to Language," 4th ed.,Holt Reinhart & Winston, New York, 1988.

[FRS] Friedman, William F. and Elizabeth S., "The Shakespearean Ciphers Examined," Cambridge University Press, London, 1957.

[FUMI] Fumio Nakamura, Rikugun ni okeru COMINT no hoga to hatten," The Journal of National Defense, 16-1 (June 1988) pp85 - 87.

[GAJ] Gaj, Krzysztof, "Szyfr Enigmy: Metody zlamania," Warsaw Wydawnictwa Komunikacji i Lacznosci, 1989.

[GAR1] Gardner, Martin, "536 Puzzles and Curious Problems," Scribners, 1967.

[GAR2] Gardner, Martin, "Mathematics, Magic, and Mystery ," Dover, 1956.

[GAR3] Gardner, Martin, "New Mathematical Diversions from Scientific American," Simon and Schuster, 1966.

[GAR4] Gardner, Martin, "Sixth Book of Mathematical Games from Scientific American," Simon and Schuster, 1971.

[GARL] Garlinski, Jozef, 'The Swiss Corridor', Dent, London 1981.

[GAR1] Garlinski, Jozef, 'Hitler's Last Weapons', Methuen, London 1978.

[GAR2] Garlinski, Jozef, 'The Enigma War', New York, Scribner, 1979.

[GERM] "German Dictionary," Hippocrene Books, Inc., New York 1983.

[GIVI] Givierge, General Marcel, " Course In Cryptography," Aegean Park Press, Laguna Hills, CA, 1978. Also, M. Givierge, "Cours de Cryptographie," Berger-Levrault, Paris, 1925.

[GLEA] Gleason, A. M., "Elementary Course in Probability for the Cryptanalyst," Aegean Park Press, Laguna Hills, CA, 1985.

[GODD] Goddard, Eldridge and Thelma, "Cryptodyct," Marion, Iowa, 1976

[GORD] Gordon, Cyrus H., " Forgotten Scripts: Their Ongoing Discovery and Decipherment," Basic Books, New York, 1982.

[GRA1] Grandpre: "Grandpre, A. de--Cryptologist. Part 1 'Cryptographie Pratique - The Origin of the Grandpre', ISHCABIBEL, The Cryptogram, SO60, American Cryptogram Association, 1960.

[GRA2] Grandpre: "Grandpre Ciphers", ROGUE, The Cryptogram, SO63, American Cryptogram Association, 1963.

[GRA3] Grandpre: "Grandpre", Novice Notes, LEDGE, The Cryptogram, MJ75, American Cryptogram Association,1975

[GRAH] Graham, L. A., "Ingenious Mathematical Problems and Methods," Dover, 1959.

[GREU] Greulich, Helmut, "Spion in der Streichholzschachtel: Raffinierte Methoden der Abhortechnik, Gutersloh: Bertelsmann, 1969.

[GUST] Gustave, B., "Enigma:ou, la plus grande 'enigme de la guerre 1939-1945." Paris:Plon, 1973.

[HA] Hahn, Karl, " Frequency of Letters", English Letter Usage Statistics using as a sample, "A Tale of Two Cities" by Charles Dickens, Usenet SCI.Crypt, 4 Aug 1994.

[HAWA] Hitchcock, H. R., "Hawaiian," Charles E. Tuttle, Co., Toyko, 1968.

[HAWC] Hawcock, David and MacAllister, Patrick, "Puzzle Power! Multidimensional Codes, Illusions, Numbers, and Brainteasers," Little, Brown and Co., New York, 1994.

[HELD] Held, Gilbert, "Top Secret Data Encryption Techniques," Prentice Hall, 1993. (great title..limited use)

[HEMP] Hempfner, Philip and Tania, "Pattern Word List For Divided and Undivided Cryptograms," unpublished manuscript, 1984.

[HEPP] Hepp, Leo, "Die Chiffriermaschine 'ENIGMA'", F-Flagge, 1978.

[HIDE] Hideo Kubota, " Zai-shi dai-go kokugun tokushu joho senshi." unpublished manuscript, NIDS.

[HILL] Hill, Lester, S., "Cryptography in an Algebraic Alphabet", The American Mathematical Monthly, June-July 1929.

[HIL1] Hill, L. S. 1929. Cryptography in an Algebraic Alphabet. American Mathematical Monthly. 36:306-312.

[HIL2] Hill, L. S. 1931. Concerning the Linear Transformation Apparatus in Cryptography. American Mathematical Monthly. 38:135-154.

[HINS] Hinsley, F. H., "History of British Intelligence in the Second World War", Cambridge University Press, Cambridge, 1979-1988.

[HIN2] Hinsley, F. H. and Alan Strip in "Codebreakers -Story of Bletchley Park", Oxford University Press, 1994.

[HIN3] Hinsley, F. H., et. al., "British Intilligence in The Second World War: Its Influence on Strategy and Operations," London, HMSO vol I, 1979, vol II 1981, vol III, 1984 and 1988.

[HISA] Hisashi Takahashi, "Military Friction, Diplomatic Suasion in China, 1937 - 1938," The Journal of International Studies, Sophia Univ, Vol 19, July, 1987.

[HIS1] Barker, Wayne G., "History of Codes and Ciphers in the U.S. Prior to World War I," Aegean Park Press, Laguna Hills, CA, 1978.

[HITT] Hitt, Parker, Col. " Manual for the Solution of Military Ciphers," Aegean Park Press, Laguna Hills, CA, 1976.

[HODG] Hodges, Andrew, "Alan Turing: The Enigma," New York, Simon and Schuster, 1983.

[HOFF] Hoffman, Lance J., editor, "Building In Big Brother: The Cryptographic Policy Debate," Springer-Verlag, N.Y.C., 1995. (A useful and well balanced book of cryptographic resource materials.)

[HOF1] Hoffman, Lance. J., et. al.," Cryptography Policy," Communications of the ACM 37, 1994, pp. 109-17.

[HOLM Holmes, W. J., "Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific During WWII", Annapolis, MD: Naval Institute Press, 1979.

[HOM1] Homophonic: A Multiple Substitution Number Cipher", S-TUCK, The Cryptogram, DJ45, American Cryptogram Association, 1945.

[HOM2] Homophonic: Bilinear Substitution Cipher, Straddling," ISHCABIBEL, The Cryptogram, AS48, American Cryptogram Association, 1948.

[HOM3] Homophonic: Computer Column:"Homophonic Solving," PHOENIX, The Cryptogram, MA84, American Cryptogram Association, 1984.

[HOM4] Homophonic: Hocheck Cipher,", SI SI, The Cryptogram, JA90, American Cryptogram Association, 1990.

[HOM5] Homophonic: "Homophonic Checkerboard," GEMINATOR, The Cryptogram, MA90, American Cryptogram Association, 1990.

[HOM6] Homophonic: "Homophonic Number Cipher," (Novice Notes) LEDGE, The Cryptogram, SO71, American Cryptogram Association, 1971.

[HUNG] Rip Van Winkel, "Hungarian," The Cryptogram, March - April, American Cryptogram Association, 1956.

[HYDE] H. Montgomery Hyde, "Room 3603, The Story of British Intelligence Center in New York During World War II", New York, Farrar, Straus, 1963.

[IBM1] IBM Research Reports, Vol 7., No 4, IBM Research, Yorktown Heights, N.Y., 1971.

[INDE] PHOENIX, Index to the Cryptogram: 1932-1993, ACA, 1994.

[ITAL] Italian - English Dictionary, compiled by Vittore E. Bocchetta, Fawcett Premier, New York, 1965.

[JAPA] Martin, S.E., "Basic Japanese Coversation Dictionary," Charles E. Tuttle Co., Toyko, 1981.

[JOHN] Johnson, Brian, 'The Secret War', Arrow Books, London 1979.

[KADI] al-Kadi, Ibrahim A., Cryptography and Data Security: Cryptographic Properties of Arabic, Proceedings of the Third Saudi Engineering Conference. Riyadh, Saudi Arabia: Nov 24-27, Vol 2:910-921., 1991.

[KAHN] Kahn, David, "The Codebreakers", Macmillian Publishing Co. , 1967.

[KAH1] Kahn, David, "Kahn On Codes - Secrets of the New Cryptology," MacMillan Co., New York, 1983.

[KAH2] Kahn, David, "An Enigma Chronology", Cryptologia Vol XVII,Number 3, July 1993.

[KAH3] Kahn, David, "Seizing The Enigma: The Race to Break the German U-Boat Codes 1939-1943 ", Houghton Mifflin, New York, 1991.

[KERC] Kerckhoffs, "la Cryptographie Militaire, " Journel des Sciences militaires, 9th series, IX, (January and February, 1883, Libraire Militaire de L. Baudoin &Co., Paris. English trans. by Warren T, McCready of the University of Toronto, 1964

[KOBL] Koblitz, Neal, " A Course in Number Theory and Cryptography, 2nd Ed, Springer-Verlag, New York, 1994.

[KONH] Konheim, Alan G., "Cryptography -A Primer" , John Wiley, 1981, pp 212 ff.

[KORD] Kordemsky, B., "The Moscow Puzzles," Schribners, 1972.

[KOTT] Kottack, Phillip Conrad, "Anthropology: The Exploration Of Human Diversity," 6th ed., McGraw-Hill, Inc., New York, N.Y. 1994.

[KOZA] Kozaczuk, Dr. Wladyslaw, "Enigma: How the German Machine Cipher was Broken and How it Was Read by the Allies in WWI", University Pub, 1984.

[KRAI] Kraitchek, "Mathematical Recreations," Norton, 1942, and Dover, 1963.

[KULL] Kullback, Solomon, Statistical Methods in Cryptanalysis, Aegean Park Press, Laguna Hills, Ca. 1976

[LAFF] Laffin, John, "Codes and Ciphers: Secret Writing Through The Ages," Abelard-Schuman, London, 1973.

[LAI] Lai, Xuejia, "On the Design and Security of Block Ciphers," ETH Series in Information Processing 1, 1992. (Article defines the IDEA Cipher)

[LAIM] Lai, Xuejia, and James L. Massey, "A Proposal for a New Block Encryption Standard," Advances in Cryptology - Eurocrypt 90 Proceedings, 1992, pp. 55-70.

[LAKE] Lakoff, R., "Language and the Women's Place," Harper & Row, New York, 1975.

[LANG] Langie, Andre, "Cryptography," translated from French by J.C.H. Macbeth, Constable and Co., London, 1922.

[LATI] BRASSPOUNDER, "Latin Language Data, "The Cryptogram," July-August 1993.

[LAUE] Lauer, Rudolph F., "Computer Simulation of Classical Substitution Cryptographic Systems" Aegean Park Press, 1981, p72 ff.

[LEAR] Leary, Penn, " The Second Cryptographic Shakespeare," Omaha, NE [from author] 1994.

[LEA1] Leary, Penn, " Supplement to The Second Cryptographic Shakespeare," Omaha, NE [from author] 1994.

[LEAU] Leaute, H., "Sur les Mecanismes Cryptographiques de M. de Viaris," Le Genie Civil, XIII, Sept 1, 1888.

[LEDG] LEDGE, "NOVICE NOTES," American Cryptogram Association, 1994. [One of the best introductory texts on ciphers written by an expert in the field. Not only well written, clear to understand but as authoritative as they come!]

[LENS] Lenstra, A.K. et. al. "The Number Field Sieve," Proceedings of the 22 ACM Symposium on the Theory of Computing," Baltimore, ACM Press, 1990, pp 564-72.

[LEN1] Lenstra, A.K. et. al. "The Factorization of the Ninth Fermat Number," Mathematics of Computation 61 1993, pp. 319-50.

[LEWI] Lewin, Ronald, 'Ultra goes to War', Hutchinson, London 1978.

[LEWY] Lewy, Guenter, "America In Vietnam", Oxford University Press, New York, 1978.

[LEVI] Levine, J., U.S. Cryptographic Patents 1861-1981, Cryptologia, Terre Haute, In 1983.

[LEV1] Levine, J. 1961. Some Elementary Cryptanalysis of Algebraic Cryptography. American Mathematical Monthly. 68:411-418

[LEV2] Levine, J. 1961. Some Applications of High-Speed Computers to the Case n =2 of Algebraic Cryptography. Mathematics of Computation. 15:254-260

[LEV3] Levine, J. 1963. Analysis of the Case n =3 in Algebraic Cryptography With Involuntary Key Matrix With Known Alphabet. Journal fuer die Reine und Angewante Mathematik. 213:1-30.

[LISI] Lisicki, Tadeusz, 'Dzialania Enigmy', Orzet Biaty London July-August, 1975; 'Enigma i Lacida', Przeglad lacznosci, London 1974- 4; 'Pogromcy Enigmy we Francji', Orzet Biaty, London, Sept. 1975.'

[LYNC] Lynch, Frederick D., "Pattern Word List, Vol 1.," Aegean Park Press, Laguna Hills, CA, 1977.

[LYSI] Lysing, Henry, aka John Leonard Nanovic, "Secret Writing," David Kemp Co., NY 1936.

[MACI] Macintyre, D., "The Battle of the Atlantic," New York, Macmillan, 1961.

[MADA] Madachy, J. S., "Mathematics on Vacation," Scribners, 1972.

[MAGN] Magne, Emile, Le plaisant Abbe de Boisrobert, Paris, Mecure de France, 1909.

[MANN] Mann, B.,"Cryptography with Matrices," The Pentagon, Vol 21, Fall 1961.

[MANS] Mansfield, Louis C. S., "The Solution of Codes and Ciphers", Alexander Maclehose & Co., London, 1936.

[MARO] Marotta, Michael, E. "The Code Book - All About Unbreakable Codes and How To Use Them," Loompanics Unlimited, 1979. [This is a terrible book. Badly written, without proper authority, unprofessional, and prejudicial to boot. And, it has one of the better illustrations of the Soviet one-time pad with example, with three errors in cipher text, that I have corrected for the author.]

[MARS] Marshall, Alan, "Intelligence and Espionage in the Reign of Charles II," 1660-1665, Cambridge University, New York, N.Y., 1994.

[MART] Martin, James, "Security, Accuracy and Privacy in Computer Systems," Prentice Hall, Englewood Cliffs, N.J., 1973.

[MAVE] Mavenel, Denis L., Lettres, Instructions Diplomatiques et Papiers d' Etat du Cardinal Richelieu, Historie Politique, Paris 1853-1877 Collection.

[MAYA] Coe, M. D., "Breaking The Maya Code," Thames and Hudson, New York, 1992.

[MAZU] Mazur, Barry, "Questions On Decidability and Undecidability in Number Theory," Journal of Symbolic Logic, Volume 54, Number 9, June, 1994.

[MELL] Mellen G. 1981. Graphic Solution of a Linear Transformation Cipher. Cryptologia. 5:1-19.

[MEND] Mendelsohn, Capt. C. J., Studies in German Diplomatic Codes Employed During World War, GPO, 1937.

[MERK] Merkle, Ralph, "Secrecy, Authentication and Public Key Systems," Ann Arbor, UMI Research Press, 1982.

[MER1] Merkle, Ralph, "Secure Communications Over Insecure Channels," Communications of the ACM 21, 1978, pp. 294- 99.

[MER2] Merkle, Ralph and Martin E. Hellman, "On the Security of Multiple Encryption ," Communications of the ACM 24, 1981, pp. 465-67.

[MER3] Merkle, Ralph and Martin E. Hellman, "Hiding Information and Signatures in Trap Door Knapsacks," IEEE Transactions on Information Theory 24, 1978, pp. 525-30.

[MILL] Millikin, Donald, " Elementary Cryptography ", NYU Bookstore, NY, 1943.

[MM] Meyer, C. H., and Matyas, S. M., " CRYPTOGRAPHY - A New Dimension in Computer Data Security, " Wiley Interscience, New York, 1982.

[MODE] Modelski, Tadeusz, 'The Polish Contribution to the Ultimate Allied Victory in the Second World War', Worthing (Sussex) 1986.

[MRAY] Mrayati, Mohammad, Yahya Meer Alam and Hassan al- Tayyan., Ilm at-Ta'miyah wa Istikhraj al-Mu,amma Ind al-Arab. Vol 1. Damascus: The Arab Academy of Damascus., 1987.

[MULL] Mulligan, Timothy," The German Navy Examines its Cryptographic Security, Oct. 1941, Military affairs, vol 49, no 2, April 1985.

[MYER] Myer, Albert, "Manual of Signals," Washington, D.C., USGPO, 1879.

[NBS] National Bureau of Standards, "Data Encryption Standard," FIPS PUB 46-1, 1987.

[NIBL] Niblack, A. P., "Proposed Day, Night and Fog Signals for the Navy with Brief Description of the Ardois Hight System," In Proceedings of the United States Naval Institute, Annapolis: U. S. Naval Institute, 1891.

[NIC1] Nichols, Randall K., "Xeno Data on 10 Different Languages," ACA-L, August 18, 1995.

[NIC2] Nichols, Randall K., "Chinese Cryptography Parts 1-3," ACA-L, August 24, 1995.

[NIC3] Nichols, Randall K., "German Reduction Ciphers Parts 1-4," ACA-L, September 15, 1995.

[NIC4] Nichols, Randall K., "Russian Cryptography Parts 1-3," ACA-L, September 05, 1995.

[NIC5] Nichols, Randall K., "A Tribute to William F. Friedman", NCSA FORUM, August 20, 1995.

[NIC6] Nichols, Randall K., "Wallis and Rossignol," NCSA FORUM, September 25, 1995.

[NIC7] Nichols, Randall K., "Arabic Contributions to Cryptography,", in The Cryptogram, ND95, ACA, 1995.

[NIC8] Nichols, Randall K., "U.S. Coast Guard Shuts Down Morse Code System," The Cryptogram, SO95, ACA publications, 1995.

[NIC9] Nichols, Randall K., "PCP Cipher," NCSA FORUM, March 10, 1995.

[NICX] Nichols, R. K., Keynote Speech to A.C.A. Convention, "Breaking Ciphers in Other Languages.," New Orleans, La., 1993.

[NICK] Nickels, Hamilton, "Codemaster: Secrets of Making and Breaking Codes," Paladin Press, Boulder, CO., 1990.

[NORM] Norman, Bruce, 'Secret Warfare', David & Charles, Newton Abbot (Devon) 1973.

[NORW] Marm, Ingvald and Sommerfelt, Alf, "Norwegian," Teach Yourself Books, Hodder and Stoughton, London, 1967.

[NSA] NSA's Friedman Legacy - A Tribute to William and Elizabeth Friedman, NSA Center for Cryptological History, 1992, pp 201 ff.

[OKLA] Andre, Josephine and Richard V. Andree, "Cryptarithms," Unit One, Problem Solving and Logical Thinking, University of Oklahoma, Norman, Ok. Copy No: 486, 1976.

[OKLI] Andre, Josephine and Richard V. Andree, " Instructors Manual For Cryptarithms," Unit One, Problem Solving and Logical Thinking, University of Oklahoma, Norman, Ok. Copy No: 486, 1976.

[OP20] "Course in Cryptanalysis," OP-20-G', Navy Department, Office of Chief of Naval Operations, Washington, 1941.

[PERR] Perrault, Charles, Tallement des Reaux, Les Historiettes, Bibliotheque del La Pleiade, Paris 1960, pp 256-258.

[PGP] Garfinkel, Simson, "PGP: Pretty Good Privacy," O'reilly and Associates, Inc. Sebastopol, CA. 1995.

[PHIL] Phillips, H., "My Best Puzzles in Logic and Reasoning," Dover, 1961.

[PIER] Pierce, Clayton C., "Cryptoprivacy", 325 Carol Drive, Ventura, Ca. 93003.

[POLY] Polya, G., "Mathematics and Plausible Reasoning," Princeton Press, 1954.

[POL1] Polya, G., "How To Solve It.," Princeton Press, 1948.

[POPE] Pope, Maurice, "The Story of Decipherment: From Egyptian Hieroglyphic to Linear B., Thames and Hudson Ltd., 1975.

[PORT] Barker, Wayne G. "Cryptograms in Portuguese," Aegean Park Press, Laguna Hills, CA., 1986.

[POR1] Aliandro, Hygino, "The Portuguese-English Dictionary," Pocket Books, New York, N.Y., 1960.

[PRIC] Price, A.,"Instruments of Darkness: the History of Electronic Warfare, London, Macdonalds and Janes, 1977.

[RAJ1] "Pattern and Non Pattern Words of 2 to 6 Letters," G & C. Merriam Co., Norman, OK. 1977.

[RAJ2] "Pattern and Non Pattern Words of 7 to 8 Letters," G & C. Merriam Co., Norman, OK. 1980.

[RAJ3] "Pattern and Non Pattern Words of 9 to 10 Letters," G & C. Merriam Co., Norman, OK. 1981.

[RAJ4] "Non Pattern Words of 3 to 14 Letters," RAJA Books, Norman, OK. 1982.

[RAJ5] "Pattern and Non Pattern Words of 10 Letters," G & C Merriam Co., Norman, OK. 1982.

[REJE] Rejewski, Marian, "Mathematical Solution of the Enigm Cipher" published in vol 6, #1, Jan 1982 Cryptologia pp 1-37.

[RENA] Renauld, P. "La Machine a' chiffrer 'Enigma'", Bulletin Trimestriel de l'association des Amis de L'Ecole superieure de guerre no 78, 1978.

[RHEE] Rhee, Man Young, "Cryptography and Secure Communications," McGraw Hill Co, 1994

[RIVE] Rivest, Ron, "Ciphertext: The RSA Newsletter 1, 1993.

[RIV1] Rivest, Ron, Shamir, A and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM 21, 1978.

[ROAC] Roach, T., "Hobbyist's Guide To COMINT Collection and Analysis," 1330 Copper Peak Lane, San Jose, Ca. 95120-4271, 1994.

[ROBO] NYPHO, The Cryptogram, Dec 1940, Feb, 1941.

[ROHE] Jurgen Rohwer's Comparative Analysis of Allied and Axis Radio-Intelligence in the Battle of the Atlantic, Proceedings of the 13th Military History Symposium, USAF Academy, 1988, pp 77-109.

[ROHW] Rohwer Jurgen, "Critical Convoy Battles of March 1943," London, Ian Allan, 1977.

[ROH1] Rohwer Jurgen, "Nachwort: Die Schlacht im Atlantik in der Historischen Forschung, Munchen: Bernard and Graefe, 1980.

[ROH2] Rohwer Jurgen, et. al. , "Chronology of the War at Sea, Vol I, 1939-1942, London, Ian Allan, 1972.

[ROH3] Rohwer Jurgen, "U-Boote, Eine Chronik in Bildern, Oldenburs, Stalling, 1962. Skizzen der 8 Phasen.

[ROOM] Hyde, H. Montgomery, "Room 3603, The Story of British Intelligence Center in New York During World War II", New York, Farrar, Straus, 1963.

[ROSE] Budge, E. A. Wallis, "The Rosetta Stone," British Museum Press, London, 1927.

[RSA] RSA Data Security, Inc., "Mailsafe: Public Key Encryption Software Users Manual, Version 5.0, Redwood City, CA, 1994

[RUNY] Runyan, T. J. and Jan M. Copes "To Die Gallently", Westview Press 1994, p85-86 ff.

[RYSK] Norbert Ryska and Siegfried Herda, "Kryptographische Verfahren in der Datenverarbeitung," Gesellschaft fur Informatik, Berlin, Springer-Verlag1980.

[SADL] Sadler, A. L., "The Code of the Samurai," Rutland and Tokyo: Charles E. Tuttle Co., 1969.

[SACC] Sacco, Generale Luigi, " Manuale di Crittografia", 3rd ed., Rome, 1947.

[SALE] Salewski, Michael, "Die Deutscher Seekriegsleitung, 1938- 1945, Frankfurt/Main: Bernard and Graefe, 1970-1974. 3 volumes.

[SANB] Sanbohonbu, ed., "Sanbohonbu kotokan shokuinhyo." NIDS Archives.

[SAPR] Sapir, E., "Conceptual Categories in Primitive Language," Science: 74: 578-584., 1931.

[SASS] Sassoons, George, "Radio Hackers Code Book", Duckworth, London, 1986.

[SCHN] Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code C," John Wiley and Sons, 1994.

[SCH2] Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code C," 2nd ed., John Wiley and Sons, 1995.

[SCHU] Schuh, fred, "Master Book of Mathematical Recreation," Dover, 1968.

[SCHW] Schwab, Charles, "The Equalizer," Charles Schwab, San Francisco, 1994.

[SEBE] Seberry, Jennifer and Joseph Pieprzyk, "Cryptography: An Introduction to Computer Security," Prentice Hall, 1989. [CAREFUL! Lots of Errors - Basic research efforts may be flawed - see Appendix A pg 307 for example.]

[SHAN] Shannon, C. E., "The Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol 28 (October 1949).

[SHIN] Shinsaku Tamura, "Myohin kosaku," San'ei Shuppansha, Toyko, 1953.

[SIG1] "International Code Of Signals For Visual, Sound, and Radio Communications," Defense Mapping Agency, Hydrographic/Topographic Center, United States Ed. Revised 1981

[SIG2] "International Code Of Signals For Visual, Sound, and Radio Communications," U. S. Naval Oceanographic Office, United States Ed., Pub. 102, 1969.

[SIMM] Simmons, G. J., "How To Insure that Data Acquired to Verify Treaty Compliance are Trustworthy, " in "Authentication without secrecy: A secure communications problem uniquely solvable by asymmetric encryption techniques.", IEEE EASCON 79, Washington, 1979, pp. 661- 62.

[SINK] Sinkov, Abraham, "Elementary Cryptanalysis", The Mathematical Association of America, NYU, 1966.

[SISI] Pierce, C.C., "Cryptoprivacy," Author/Publisher, Ventura Ca., 1995. (XOR Logic and SIGTOT teleprinters)

[SMIH] Smith, David E., "John Wallis as Cryptographer", Bulletin of American Mathematical Society, XXIV, 1917.

[SMIT] Smith, Laurence D., "Cryptography, the Science of Secret Writing," Dover, NY, 1943.

[SOLZ] Solzhenitsyn, Aleksandr I. , "The Gulag Archipelago I- III, " Harper and Row, New York, N.Y., 1975.

[SPAN] Barker, Wayne G. "Cryptograms in Spanish," Aegean Park Press, Laguna Hills, CA., 1986.

[STEV] Stevenson, William, 'A Man Called INTREPID', Macmillan, London 1976.

[STIN] Stinson, D. R., "Cryptography, Theory and Practice," CRC Press, London, 1995.

[STIX] Stix, F., Zur Geschicte und Organisation der Wiener Geheimen Ziffernkanzlei, Mitteilungen des Osterreichischen Instituts fir Geschichtsforschung, LI 1937.

[STUR] Sturtevant, E. H. and Bechtel, G., "A Hittite Chrestomathy," Linguistic Society of American and University of Pennsylvania, Philadelphia, 1935.

[SUVO] Suvorov, Viktor "Inside Soviet Military Intelligence," Berkley Press, New York, 1985.

[TERR] Terrett, D., "The Signal Corps: The Emergency (to December 1941); G. R. Thompson, et. al, The Test (December 1941 - July 1943); D. Harris and G. Thompson, The Outcome;(Mid 1943 to 1945), Department of the Army, Office of the Chief of Military History, USGPO, Washington,1956 -1966.

[THEO] Theodore White and Annalee Jacoby, "Thunder Out Of China," William Sloane Assoc., New York, 1946.

[THOM] Thompson, Ken, "Reflections on Trusting Trust," Communications of the ACM 27, 1984.

[TILD] Glover, D. Beaird, Secret Ciphers of The 1876 Presidential Election, Aegean Park Press, Laguna Hills, Ca. 1991.

[TM32] TM 32-250, Fundamentals of Traffic Analysis (Radio Telegraph) Department of the Army, 1948.

[TRAD] U. S. Army Military History Institute, "Traditions of The Signal Corps., Washington, D.C., USGPO, 1959.

[TRAI] Lange, Andre and Soudart, E. A., "Treatise On Cryptography," Aegean Park Press, Laguna Hills, Ca. 1981.

[TRIB] Anonymous, New York Tribune, Extra No. 44, "The Cipher Dispatches, New York, 1879.

[TRIT] Trithemius:Paul Chacornac, "Grandeur et Adversite de Jean Tritheme ,Paris: Editions Traditionelles, 1963.

[TUCK] Harris, Frances A., "Solving Simple Substitution Ciphers," ACA, 1959.

[TUKK] Tuckerman, B., "A Study of The Vigenere-Vernam Single and Multiple Loop Enciphering Systems," IBM Report RC2879, Thomas J. Watson Research Center, Yorktown Heights, N.Y. 1970.

[TUCM] Tuckerman, B., "A Study of The Vigenere-Vernam Single and Multiple Loop Enciphering Systems," IBM Report RC2879, Thomas J. Watson Research Center, Yorktown Heights, N.Y. 1970.

[UBAL] Ubaldino Mori Ubaldini, "I Sommergibili begli Oceani: La Marina Italian nella Seconda Guerra Mondiale," vol XII, Roma, Ufficio Storico della Marina Militare, 1963.

[USAA] U. S. Army, Office of Chief Signal Officer, "Instructions for Using the Cipher Device Type M-94, February, 1922," USGPO, Washington, 1922.

[VAIL] Vaille, Euggene, Le Cabinet Noir, Paris Presses Universitaires de Frances, 1950.

[VALE] Valerio, "De La Cryptographie," Journal des Scienses militares, 9th series, Dec 1892 - May 1895, Paris.

[VAND] Van de Rhoer, E., "Deadly Magic: A personal Account of Communications Intilligence in WWII in the Pacific, New York, Scriber, 1978.

[VERN] Vernam, A. S., "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," J. of the IEEE, Vol 45, 109-115 (1926).

[VIAR] de Viaris in Genie Civil: "Cryptographie", Publications du Journal Le Genie Civil, 1888.

[VIA1] de Viaris, "L'art de chiffre et dechiffre les depeches secretes," Gauthier-Villars, Paris, 1893.

[VOGE] Vogel, Donald S., "Inside a KGB Cipher," Cryptologia, Vol XIV, Number 1, January 1990.

[WALL] Wallis, John, "A Collection of Letters and other Papers in Cipher" , Oxford University, Bodleian Library, 1653.

[WAL1] Wallace, Robert W. Pattern Words: Ten Letters and Eleven Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1993.

[WAL2] Wallace, Robert W. Pattern Words: Twelve Letters and Greater in Length, Aegean Park Press, Laguna Hills, CA 92654, 1993.

[WATS] Watson, R. W. Seton-, ed, "The Abbot Trithemius," in Tudor Studies, Longmans and Green, London, 1924.

[WEBE] Weber, Ralph Edward, "United States Diplomatic Codes and Ciphers, 1175-1938, Chicago, Precedent Publishing, 1979.

[WEL] Welsh, Dominic, "Codes and Cryptography," Oxford Science Publications, New York, 1993.

[WELC] Welchman, Gordon, 'The Hut Six Story', McGraw-Hill, New York 1982.

[WHOR] Whorf, B. L., "A Linguistic Consideration of Thinking In Primitive Communities," In Language, Thought, and Reality: Selected Writings of Benjamin Lee Whorf, ed. J. B. Carroll, Cambridge, MA: MIT Press, pp. 65-86., 1956.

[WINT] Winton, J., " Ultra at Sea: How Breaking the Nazi Code Affected Allied Naval Strategy During WWII," New Uork, William Morror, 1988.

[WINK] Winkle, Rip Van, "Hungarian: The Cryptogram,", March - April 1956.

[WINT] Winterbotham, F.W., 'The Ultra Secret', Weidenfeld and Nicolson, London 1974.

[WOLE] Wolfe, Ramond W., "Secret Writing," McGraw Hill Books, NY, 1970.

[WOLF] Wolfe, Jack M., " A First Course in Cryptanalysis," Brooklin College Press, NY, 1943.

[WRIX] Wrixon, Fred B. "Codes, Ciphers and Secret Languages," Crown Publishers, New York, 1990.

[XEN1] PHOENIX, "Xenocrypt Handbook," American Cryptogram Association, 1 Pidgeon Dr., Wilbraham, MA., 01095-2603, for publication March, 1996.

[YARD] Yardley, Herbert, O., "The American Black Chamber," Bobbs-Merrill, NY, 1931.

[YAR1] Yardley, H. O., "The Chinese Black Chamber," Houghton Mifflin, Boston, 1983.

[YOKO] Yukio Yokoyama, "Tokushu joho kaisoka," unpublished handwritten manuscript.

[YOUS] Youshkevitch, A. P., Geschichte der Mathematik im Mittelatter, Liepzig, Germany: Teubner, 1964.

[YUKI] Yukio Nishihara, "Kantogan tai-So Sakusenshi," Vol 17., unpublished manuscript, National Institute for Defense Studies Military Archives, Tokyo.,(hereafter NIDS Archives)

[ZIM] Zim, Herbert S., "Codes and Secret Writing." William Morrow Co., New York, 1948.

[ZEND] Callimahos, L. D., Traffic Analysis and the Zendian Problem, Agean Park Press, 1984. (also available through NSA Center for Cryptologic History)