Bibliography

Codebreakers. Hinsley, F.H. Stripp, Alan. Oxford University Press, New York. 1993.

"Cryptologia." Volume 6, Number 1, January 1982. Khan, David. Kruh, Louis. Deavours, Cipher. Winkel, Brian. Mellen, Greg.

Kahn on Codes. Kahn, David. Macmillan Publishing Company. New York, NY. 1983.

Machine Cryptography and Modern Cryptanalysis. Deavours, Cipher. Kruh, Louis. Artech House, Inc. Dedham, MA. 1985.

Alan Turing: the enigma. Hodges, Andrew. Simon and Schuster. New York, NY. 1983.

Lively debate continues as to whether the breaking of the Enigma cipher won the war. It is not, however, contested that the Polish work contributed to winning. When the Naval Enigma was broken, specific shipments were targeted such that munitions and fuel convoys were attacked, while food and medical supplies could continue through. By listening to the German troop mobilization plans, the Allies determined that their efforts to mislead the *wehrmacht* about the location of the D-day offensive had been successful. In a longer-term perspective, the success with Enigma brought cryptology into the world as a legitimate scientific field, incorporating – in the words of Rejewski – "protracted trials, imagination, and sometimes the proverbial ounce of luck."[8]

There also remains an important lesson from the German work on Enigma. Although the system itself was relatively secure, the way in which it was used was deficient. The efficacy of an otherwise excellent cipher was sabotaged by the soldiers using it. Rejewski's summation of the situation cannot be improved upon or overemphasized:

> They [made] the mistake [of] favoring keys such as AAA, or BBB, or CCC, and so on. This made things easier [for us]. But after a few months they were forbidden [to do this]. Hm! [. . .] [T]hey would pick three letters [. . .] that [stood] next to each other. Or [. . .] diagonally [from each other]. [. . .] But by then [. . .] it availed them nothing that they forbade them. [. . .] When they were forbidden [to use] three letters according to [the lay of] the keyboard, [. . .] we found another characteristic again. [. . .] There's no avoiding it… [W]henever there is arbitrariness, there is also a certain regularity. There's no avoiding it.
>
> (Woytak, Richard. "A conversation with Marian Rejewski.")

This issue is of substantial importance to those attempting to implement security in any context, but one rarely granted any attention whatsoever. The *wehrmacht* was busily improving upon the security of a system inherently flawed due to lack of education on the part of the end-users. Had Germany focused their efforts further upon how to improve the use of Enigma, rather than how to improve Enigma itself, the Polish mathematicians might not have broken it with such relative ease.

[8] Ibid. p. 7.

identify rotor positions could be rotated with respect to the wired rotor. Additionally, an entry ring performed an additional permutation which Rejewski comments "made the breaking of the cipher much more difficult."[6]

The Germans regularly implemented minor operational modifications to Enigma, most of which did no more than inconvenience Polish intelligence for brief intervals. The number of possible rotors grew from three to five, and the plugboards increased in complexity; these modifications were easily overcome by reworking the presented equations, since the majority of the previously unknown values could be eliminated at an early stage.

The most effective branch of the *wehrmacht* to use Enigma was, by far, the Navy. There were several reasons for this; firstly, they were the last branch to distribute the Enigma machines, and thus had five rotors in simultaneous use, rather than the Army's three. Second, the navy communications were far more sporadic, and with under sixty messages per day it is difficult to build up sufficient data. The daily changes of base rotor settings contributed to making that task more challenging. Furthermore, the Enigma was weighted, and the naval officers were under instructions to heave the Enigma overboard if boarding was imminent. Needless to say, no equivalently easy method of disposal existed for the German army. The breakthrough occurred with the U-110, a German submarine captured in May of 1941, with much of the Enigma machine still intact.

The most efficient solution of the Enigma cipher derived from Turing's bombe, a mechanical device that could search the key space with astonishing efficiency, finding keys in approximately twenty minutes. Turing's work was derived in part from the Polish bombe, which Rejewski assisted in. Preceding Turing's bombe by approximately three years, the Polish bombe took on the order of two hours to find starting rotor positions for a given string of ciphertext.[7] The bombes themselves were among the first electronic machines, and certainly sparked the interest of several governments in the field of computing and cryptanalysis.

[6] Cryptologia. Volume 6, Number 1, Jan. 1982. Rejewski, Marian. "Mathematical solution of the Enigma Cipher." p. 12.

[7] It should be noted that Cryptologia published Rejewski's response to one of Hinsley's books, wherein Rejewski disagrees with a number of Hinsley's purported facts about the timing of various events. In short, it is not at all clear precisely when certain events took place, and how long some projects took. I have tried to cite dates only when agreed upon by more than one source.

This set is soluble, although Rejewski chose to undertake certain other transformations, in order to account for the possibility of other rotor movements. Once we have solved this set of equations, we have Q – which is of relatively little use, since it encompasses the permutations of three rotors – and N. N is of greater interest, as it represents the permutations of a single rotor. From that data, the wiring of rotor N can be calculated and used on a daily basis to decipher Enigma intercept.

Although the Germans were unaware of the Allies' success in penetrating Enigma, they were conscious of security issues associated with their enciphering mechanism. The first effort undertaken to ensure security was ordering that rotors should be rearranged on a monthly basis. The net effect was a complete compromise of Enigma over the course of two months; with a new rotor N, he had acquired the wiring for two rotors of the rotors via the above described method. Since the previously known rotor was now a part of Q, he was able to reduce the number of unknowns in Q to two, and ultimately solve them. The Poles built a working model of Enigma, with the German rotor connections – a feat made possible only by the 'added security' that the *wehrmacht* had introduced!

The German command introduced several measures based upon the encipherer's habits of using repeated characters as keys. First, it was required that all the characters in the new rotor settings be different. This order was useless, as the German soldiers simply started using patterns made easy by the keyboard, such as 'qwe'. Once again, a frequency analysis showed those habitual keys; it was not a substantial increase in security, given that the code had already been penetrated.

By far the most sophisticated upgrade was a methodological one, wherein the entire process for using Enigma was changed. Instead of specific rotor settings for a given day, only plugboard settings would be dictated. The encipherer would transmit initial settings in plaintext, then set the rotors and encipher the message. This new methodology caused a six to eight day interruption in Poland's ability to read Enigma traffic.

In many ways, the challenge was the precise reverse of the previous. Whereas before, the effort was centered on reconstructing the machine, given keys, the challenge in this case was one of reconstructing the keys given the machine. Initially, this may seem like a pointless exercise, given that the machine has been reconstructed. Nothing could be farther from the truth, since the solution presented thus far has been for a rather simplistic version of the genuine Enigma. In reality, the alphabet ring used to problem. Choosing an arbitrary element of one 4-cycle, we must compare it with 4! arrangements – three times, one for each remaining candidate cycle. Once that cycle has been paired, we must try another 4! arrangements, in order to correctly align the last pair of 4-cycles, for a total of 5!+4(4!) combinations. So, although we have made substantial progress from the initial field of 5 x 10^{92}, further refinements would be desirable – although a mechanical effort to test these combinations was the basis of Turing's bombe.

Looking back at the message intercepts, one particular possibility advances itself. HIU ZMY is repeated four times, an unlikely event given a random distribution of keys. Other characters are repeated as well, more than sheer chance would dictate. This is due to habit, on the part of those doing the enciphering. The German soldiers commonly used repeated characters, such as 'aaa', as keys. By recognizing the most frequently occurring keys, cycle combinations which yield the common keys can be tested first. Through this method, and a certain amount of trial and error, we can regard the disjunctive transpositions α, β, χ, δ, ε, and ϕ as known. It should be noted that although it is easy to recognize certain enciphered keys as occurring on a regular basis, the cipher must be cracked once before the plaintext can be recovered. This does, however, greatly facilitate the efforts for the next day.

Thereby, the system of equations has been reduced to:

$$\begin{gathered}
\alpha = SPNP^{-1}QPN^{-1}P^{-1}S^{-1} \\
\beta = SP^{2}NP^{-2}QP^{2}N^{-1}P^{-2}S^{-1} \\
\chi = SP^{3}NP^{-3}QP^{3}N^{-1}P^{-3}S^{-1} \\
\delta = SP^{4}NP^{-4}QP^{4}N^{-1}P^{-4}S^{-1} \\
\varepsilon = SP^{5}NP^{-5}QP^{5}N^{-1}P^{-5}S^{-1} \\
\phi = SP^{6}NP^{-6}QP^{6}N^{-1}P^{-6}S^{-1}
\end{gathered}$$

An equation with a total of three unknowns (S, N, Q) could likely be solved, given a large number of intercepts over a long period of time. Fortunately, the need for such long-term analysis was obviated when Asche, a spy for the French, delivered the codebooks which contained the plugboard connections for given days. This information made S a known quantity, reducing the number of unknowns to two, N and Q:

$$\begin{gathered}
S^{-1}\alpha S = PNP^{-1}QPN^{-1}P^{-1} \\
S^{-1}\beta S = P^{2}NP^{-2}QP^{2}N^{-1}P^{-2} \\
S^{-1}\chi S = P^{3}NP^{-3}QP^{3}N^{-1}P^{-3} \\
S^{-1}\delta S = P^{4}NP^{-4}QP^{4}N^{-1}P^{-4} \\
S^{-1}\varepsilon S = P^{5}NP^{-5}QP^{5}N^{-1}P^{-5} \\
S^{-1}\phi S = P^{6}NP^{-6}QP^{6}N^{-1}P^{-6}
\end{gathered}$$

The converse is important in an attempt to break $\alpha\delta$ into the constituent permutations α and δ, and proving it is a useful exercise. Given the disjunctive cycles of the same length in even numbers, they can certainly be arranged as outlined above, in columns of transpositions Ω and Ψ. It is also clear that only a small subset of the possible arrangements will yield α and δ.[5]

Let us consider a case where the product $\Omega\Psi$ yields two cycles of length 5, and four cycles of length 4, for a total of (2*5)+(4*4)=26 elements. It is possible to present this as two permutations, by matching each cycle with another cycle of the same length.

We designate the two cycles of length five as X and Y, with $X_1 \dots X_5$ representing the five elements of cycle X. X_1 must be associated with some element in Y, and without loss of generality we may assume it is Y_1. From this, we may develop a new table as follows:

In Ω there might occur:	In Ψ there might occur:
(X_1, Y_1)	(Y_1, X_2)
(X_2, Y_2)	(Y_2, X_3)
(X_3, Y_3)	(Y_3, X_4)
(X_4, Y_4)	(Y_4, X_5)
(X_5, Y_5)	(Y_5, X_1)

This serves to prove the theorem, since it will certainly always be possible to match an element X_n with Y_n for any arbitrary ordering of X and Y in order to create one permutation, then utilize that same ordering and match element Y_n with X_{n+1} for all $0 < n < |X|$, creating tuple (Y_n, X_1) for $n = |X|$.

The difficulty is that we desire a specific permutation, not some arbitrary solution. From Rejewski's work, if two characters in different cycles belong to the same transposition, then the two cycles are part of the same permutation. Our task is therefore to determine which characters belong to the same transposition. This can be determined through trial and error: we know that element X_1 must be associated with some element of Y, and we can test every possibility until we find the correct one. Having found that first connection, we continue trying combinations until we have exhausted all possibilities.

Since every element in X is associated with exactly one element in Y, there are 5! ways to arrange the two cycles, giving 125 total arrangements. The four cycles of length 4 pose a considerably greater

[5] There are multiple arrangements of cycles that would yield α and δ, since cycles (abc) and (bca) are equivalent. The important issue is lining up both cycles correctly, from an arbitrary starting point.

disjunctive cycles of identical length. Disregarding identical transpositions, we find that Ω and Ψ must take on the following form:

In Ω there will occur	In Ψ there will occur
(a_1,a_2)	(a_2,a_3)
(a_3,a_4)	(a_4,a_5)
...	…
(a_{k-3},a_{k-2})	(a_{k-2},a_{k-1})
(a_{k-1},a_k)	(a_k,a_1)

It is clear that in transposition Ω, a_1 cannot map to a_1, by the definition of a disjunctive transposition. We can therefore without prejudice state that it maps to some other character, a_2. In the case where a_2 maps to a_1 in Ψ we have identical transpositions in Ω and Ψ, a previously solved possibility. Ψ must contain a_2 in some transposition; we may assume it is (a_2, a_3). Ω must contain a_3 in some position. Clearly it is impossible for a_3 to be associated with either a_2 or a_1, as they are already involved in transpositions. We may designate the associate of a_3 as a_4. Further inspection makes it clear that (a_k, a_1) must appear in the Ψ column and therefore k must be an even number. Were (a_k, a_1) in the Ω column, then the combination (a_1, a_2) and (a_k, a_2) would violate the assumption that the permutation consisted of disjunctive transpositions.

When the product $\Omega\Psi$ is calculated, they will generate two cycles, one being $(a_1, a_3, \ldots, a_{k-3}, a_{k-1})$ and the other $(a_2, a_4, \ldots, a_{k-2}, a_k)$. These must be of the same length, as k is an even number. Furthermore, we observe that for any $0 < i < k$, a_i and a_{i+1} enter into different cycles. From this it follows that if two characters in different cycles of $\Omega\Psi$ belong to the same transposition, then the entirety of the two cycles belong to the same collection of transpositions.

Although there is no tuple of the above ciphertext where M appears in the fourth position, it can be asserted that such a tuple would take the form Fxx Mxx, as we have already generated a complete 11-cycle. Once the first 11-cycle has been fully documented, any remaining cycle of size greater than 2 must be the other 11-cycle in order to generate a complete alphabet, therefore $\alpha\delta$ is demonstrably complete and correct.

Although Rejewski proves the theorem, he does not prove the converse:

> Theorem: If a permutation of even-numbered degree includes disjunctive cycles of
> the same length in even numbers, then this permutation may be regarded as the product
> of two permutations, each consisting solely of disjunctive transpositions.

repeated three-letter sequence and a regular one-to-one transformation enacted upon that plaintext sequence. The same holds true for a second-fifth relationship, and a third-sixth. An exception to this rule is PGW OCQ, as P is associated with D in all other cases.[3]

Given this information, we have sufficient data to calculate the products of the permutations, i.e. $\alpha\delta$, $\beta\varepsilon$, and $\chi\phi$. Generating the products can be viewed as determining the cycles apparent in the ciphertext. In this example, calculating $\alpha\delta$ would involve starting with the first and fourth characters. From the ABW BFO pair, we observe that A is associated with B. We now continue building upon this by looking at the case where the second character is in position one: BAS QIA. Thus, B is associated with Q, giving a partial cycle of ABQ. Continuing this process, we find a complete cycle of (ABQHZUIWOXL); L leads back to A. This is obviously not a complete alphabet, so the process is repeated from an arbitrary new starting letter not in a previously deduced cycle, such as C. We arrive at the following:

$$\alpha\delta\text{=(ABQHZUIWOXL)(MNJRVTGCKEF)(DP)(SY)}$$

In the process, we encounter the problem where E yields F, and F does not appear in the intercept. It would be hoped that a larger sample would avoid such problems, but in this case we can work backwards, looking for tuples where C is the fourth character and building up the chain. We are assured of the association between F and M through the theorem of transpositions, which Rejewski states as follows:

> Theorem: If two permutations of the same degree consist solely of disjunctive transpositions, then their product will include disjunctive cycles of the same length in even numbers.

It should be noted that degree, in this case, indicates the number of elements on which the permutation acts. In the case of Enigma, their degrees will always be identical, as they remap an alphabet of twenty-six characters. Take two arbitrary disjunctive transpositions, Ω and Ψ. If there appears an identical transposition in each permutation, e.g., (ab), the intercept product would show something of the form Axx Axx, and Bxx Bxx[4], giving the product $\Omega\Psi$ two cycles, (a) and (b). Clearly, this is a pair of

[3] This is a typographical error in the original source used for this example. If any middle rotors turned in any of our inputs, we would find it had repercussions throughout the rest of the tuple as well. There are other typos in the text as well – they are left as an exercise, either to the reader or in sadism, depending on inclination.

[4] Depending on which permutation, of course, it could be xAx xAx, or xxA xxA.

rotor setting is entered twice, there is a direct relationship between α and δ, β and ε, and χ and ϕ. By combining the above equations, we can look at the conjunction of permutations, the effects of following the first by the second:

$$\alpha\delta = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{3}NP^{-4}MLRL^{-1}M^{-1}P^{4}N^{-1}P^{-4}S^{-1}$$
$$\beta\varepsilon = SP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{3}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}S^{-1}$$
$$\chi\phi = SP^{3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{3}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}S^{-1}$$

Between the equations, we place a P^3 – necessary to compensate for the additional rotor turns accrued between the repeated characters. This set of equations, with five unknowns, is not soluble. The number of unknowns can be reduced, by observing that M, L, and R (along with their inverses) are all composed of disjunctive transpositions. It is therefore possible to express them as a single disjunctive permutation, $Q=MLRL^{-1}M^{-1}$:

$$\alpha\delta = SPNP^{-1}QPN^{-1}P^{3}NP^{-4}QP^{4}N^{-1}P^{-4}S^{-1}$$
$$\beta\varepsilon = SP^{2}NP^{-2}QP^{2}N^{-1}P^{3}NP^{-5}QP^{5}N^{-1}P^{-5}S^{-1}$$
$$\chi\phi = SP^{3}NP^{-3}QP^{3}N^{-1}P^{3}NP^{-6}QP^{6}N^{-1}P^{-6}S^{-1}$$

This substitution is only possible if rotor M and L do not rotate at all within the first six characters. Since M rotates every twenty-six rotations of N, if N starts at some arbitrary point there are 6/26 settings that will trigger a rotation of M. Given the hundred-plus messages intercepted on any given day, those messages where M had rotated were readily identifiable. To illustrate, let us consider the following series of possible intercepts, examining only the first six characters in each case:

ABW BFO ACC BIS AKI BTB ARS BXA AWB BCL BAS QIA
BIQ QMV CCB KIL CKP KTG CNZ KYC CPB KDL CVC KAC
DDH PKW DMB POL DUE PPO EEH FQW EHZ FNC EOH FBQ
EUR FPE GCS CIA GHG CNK GJN CVD GMX COJ GSG CWK
HDL ZKR HIU ZMY HIU ZMY HIU ZMY HIU ZMY HXU ZEY
IAM WJF IHE WNO IQR WUE IVB WAL IXJ WEB JKI RTU
JKZ RTC JZA RSX KOG EBK LIH AMW LOX ABJ LPK ADI
LQJ AUB MBZ NFC MLW NRQ MLW NRQ MLW NRQ MLW NRQ
MSQ NWV NWJ JOB NTA JLX NYM JHF NYM JHF OHZ XNC
PGW OCQ PHA DNX PXA DEX QAP HJG QFR HZE QGZ HCJ
QIE HMW QMS HOA QYZ HHC RAA VJX RFQ VZX RRN VXD
RSD VWZ RWZ VGC SRO YXN SUP YPG TLB GRL TMV GOM
TQO GUN UGU ICY UQT IUP UQT IUP UQT IUP VIY TMH
WLL ORR WNT OYP WWP OGG WZY OSH XFF LZT XQK LUI
XQR LUE YAP SJG YFV SZM YQQ SUV YSG SWK YSG SWK
YSG SWK ZMD UOZ ZPZ UDC

Several things leap out which suggest that our understanding of the problem is good. Any given leading character is associated with a consistent fourth character, which we would expect of a twice-

Walking through this morass of permutations may help clarify the reasoning behind this particular approach. The evaluation takes place left to right; the product of multiple permutations in this case represents the order in which manipulations are performed on the alphabet by the Enigma machine.

First, the plugboard's setting (S) is taken into account. Current then flows through rotor N, which has rotated once; thus, PN. To explain the utility of P^{-1}, we must view N from a mechanical perspective. The rotor is a collection of wires, set to connect one character to another character. By representing each character as a number, with 'a'=1, 'b'=2, …, 'z'=26, we can measure distance, such that (a, b) has distance (b-a)=(2-1)=1.[2] If N has, at a base state of P=0, transposition (b, d), we may conclude that the transposition has distance 2. Without loss of generality, we may imagine that P contains transposition (a, b) upon the first rotor turn. But now (a, b) and (b, d) together yield (a, d), a transposition of distance 3! This necessarily implies a change in the wiring of rotor N, which cannot be. P^{-1} describes the change in output that follows from the consistent internal wiring of the rotor.

Next are the other two rotors, M and L, which are assumed to be stationary. This is a reasonable assumption for the course of the exercise, because of the infrequency in their rotations. Over the first few characters, it is very unlikely that they will move, so that possibility can be discarded for the moment. The reflecting disk, R, then causes current to go back through the inverses of the various permutations (L^{-1}, etc.).

We can describe the permutations that generate the next five characters of ciphertext in a similar fashion, thus:

$$\beta = SP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{-2}S^{-1}$$
$$\chi = SP^{3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{-3}S^{-1}$$
$$\delta = SP^{4}NP^{-4}MLRL^{-1}M^{-1}P^{4}N^{-1}P^{-4}S^{-1}$$
$$\varepsilon = SP^{5}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}S^{-1}$$
$$\phi = SP^{6}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}S^{-1}$$

At this point, however, the only information possessed by the cryptanalyst is a few letters of enciphered text, which does not readily lend itself to this sort of analysis. Rejewski did have a few weeks of actual intercept, and being aware of the enciphering mechanism presented a new potential direction from which to attack the problem. Because the initial rotor settings for any given day are identical, and the new

[2] We may without loss of generality assume linearity of the internal wiring. If this can be shown impractical in any particular case, the need for permutation P^{-1} is illustrated.

The enciphering process relies almost exclusively upon the internal wiring of the rotors. Current from a circuit completed by pressing a key travels through each rotor in turn, then passes through a reflecting disk, which sends it back through all the rotors once again. Additionally, every key pressed will advance the leftmost rotor. Much like an odometer, the middle and rightmost rotor turn at increasingly less frequent intervals. Each rotor has a different set of connections, and each one functions in a way very similar to a plugboard with some plug in every hole. An important characteristic of the rotor wiring is that at no point did any character map to itself; there was some change in the plaintext that would take place at each step. Every connection must also be one-to-one; it would be highly undesirable for a plaintext to encrypt to multiple ciphertexts, from the same starting position. Decryption would be something of an unpleasant challenge. To fulfill the previously observed property that $F(F(M))=M$, the wiring must also be symmetric.

A one-to-one set of connections must therefore map all twenty-six characters of the potential input alphabet to a different arrangement of twenty-six characters, with no character mapping to itself. Thus, each rotor must be a collection of disjunctive (non-overlapping) transpositions of the alphabet. Due to the symmetric wiring, $F(M)$ can be described as a set of thirteen two-tuples, each indicating the appropriate transposition for a specific letter:

e.g. $F(M)=(ad)(bn)(cx)(eq)(fo)(gl)(hm)(ip)(jv)(kw)(ru)(sz)(ty)$

A series of transpositions such as that expressed above, where no character is repeated, is termed an ‘involution’. Rejewski started by generating a system of equations to describe the workings of the Enigma machine, by assigning permutations L, M, and N to the three rotors. S indicates the permutations induced by the plugboard, and R represents the action of the reflecting disk. Because the first rotor (N) rotates with every keypress, we can describe the movement of the N rotor by another permutation, P, where P^x equates to the Xth rotation of the rotor N. α denotes an involution, the previously observed outcome of an enciphered Enigma message. The reason for this somewhat convoluted notation will become clear.

We can therefore describe a new permutation as the net effect of those permutations taking place inside the Enigma machine:

$$\alpha=SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$$

The Enigma variant upon which Rejewski based his work was in common use by the German army, prior to the start of World War II. The front of the machine had a plugboard – a series of holes, one for each letter of the alphabet -- into which cables could be plugged. This would swap various characters, such that if A and H were plugged, every A would be treated as an H, and vice versa, prior to any other operations that the Enigma performed.

The top of the Enigma was composed of a keyboard of twenty-six letters, which the typist would use to enter a message. Above the keys was a display of twenty-six lights, each with a letter painted atop. Every time a key was pressed on the keyboard, a light would illuminate to indicate the next letter of the ciphertext. Finally, above the lights were three rotors, each of which had twenty-six settings, identifiable by a letter. Over the course of typing, the rotors turned themselves at varying rates. The Enigma machine was itself stored in a wooden carrying case, with a front panel that could be unfolded to permit access to the plugboard.

Training soldiers to use the Enigma was fast and easy. Sets of codebooks were distributed among the *wehrmact*, which specified given plugboard and rotor settings for every day. The operator of the Enigma would start from those settings, and choose an arbitrary, new rotor setting. This new setting would be distinguishable by the letters on each rotor – three letters in all. To help with detecting errors, the operator would type in the new setting twice, generating six letters of ciphertext. Then the rotors would be set to the new setting, and the entire message of plaintext would be encrypted.

The receiver would start with the daily rotor settings, type in the first six letters, and verify that they deciphered to the same three-letter group, repeated twice. The rotors would be reset to the deciphered setting, and the ciphertext entered. By transcribing which lights lit, the original message would be deciphered.

At this point, an interesting observation about the Enigma machine can be made: trying to encipher text twice in a row, with the same initial rotor settings, yields the starting plaintext. In more precise language, given an encryption function F which results from rotor settings *f*, and some plaintext M, F(F(M))=M. This property permits the use of Enigma for both encryption and decryption, without any further adaptation.

Unraveling Enigma

In 1923, Chiffrienmaschinen Aktien Gesellschaft (a German company specializing in cipher devices) unveiled the first Enigma at the International Postal Congress in Bern, Switzerland. The device itself was unimpressive, resembling nothing so much as a typewriter. Indeed, it could be pressed into service as a typewriter, if so desired. The internals of the machine were, however, dramatically different from that of a conventional typewriter. An enciphering machine with potential for over "500 million million million … million [the word "million" being written a total of 15 times – and the whole number thus being 5 x 10^{92}]" combinations.[1] The Enigma was employed extensively by all branches of the *wehrmacht* in World War II, and became the first widely used electronic enciphering device of any complexity to receive commercial success.

Throughout World War II, under conditions of great secrecy, the Allies managed to develop ways to break the Enigma cipher through mathematical means. At the start of the war, this process required analysis of all messages for a given day. By the end of the war, electronic means sped the process to the degree where messages could be broken within twenty minutes of interception. The electronic method was, however, predicated upon the mathematical solution to Enigma. In popular literature prior to the 1970's, the British were acclaimed with having solved the cipher. In 1973, Gustave Bertrand revealed the involvement of Polish mathematicians in that solution and most particularly the contribution of Marian Rejewski, who had calculated the internal wiring of Enigma as employed by the *wehrmacht*.

In a series of subsequent articles, Rejewski spoke at length about the process he used to solve Enigma, and spent a great deal of his time debunking myths which had grown out of the secrecy surrounding the war effort. The Germans never believed the Enigma cipher was solved, although they were cognizant of weaknesses within their implementation. Over time, various refinements were added to the cipher. The initial breakthroughs with the first variations of Enigma gave the Polish mathematicians a sufficient foothold in subsequent alterations that the Allies continued to read Enigma message traffic through the end of the war.

[1] Cryptologia. Volume VI, No. 1, January 1982. Rejewski, Marian.

Unraveling Enigma

Tom Walcott
Beloit College