Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

THE CRYPTOGRAPHIC MATHEMATICS OF ENIGMA

A. Ray Miller [a]

[a] Mail Stop J1, National Security Agency, 9800 Savage Road, Fort George Meade MD 20755-6000 USA.

Available online: 04 Jun 2010

To cite this article: A. Ray Miller (1995): THE CRYPTOGRAPHIC MATHEMATICS OF ENIGMA, Cryptologia, 19:1, 65-80

To link to this article: http://dx.doi.org/10.1080/0161-119591883773

THE CRYPTOGRAPHIC MATHEMATICS OF ENIGMA

A. Ray Miller

ADDRESS: Mail Stop J1, National Security Agency, 9800 Savage Road, Fort George Meade MD 20755-6000 USA.

ABSTRACT: The Enigma cipher machine had the confidence of German forces who depended upon its security. This misplaced confidence was due in part to the large key space the machine provided. This paper derives for the first time the exact number of theoretical cryptographic key settings and machine configurations for the Enigma cipher machine. It also calculates the number of practical key settings Allied cryptanalysts were faced with on a daily basis throughout World War II. Finally, it shows the relative contribution each component of the Enigma added to the overall strength of the machine.

KEYWORDS: Cryptography, mathematics, Enigma, World War II.

Dedicated to the memory of the Allied Polish cryptanalysts:

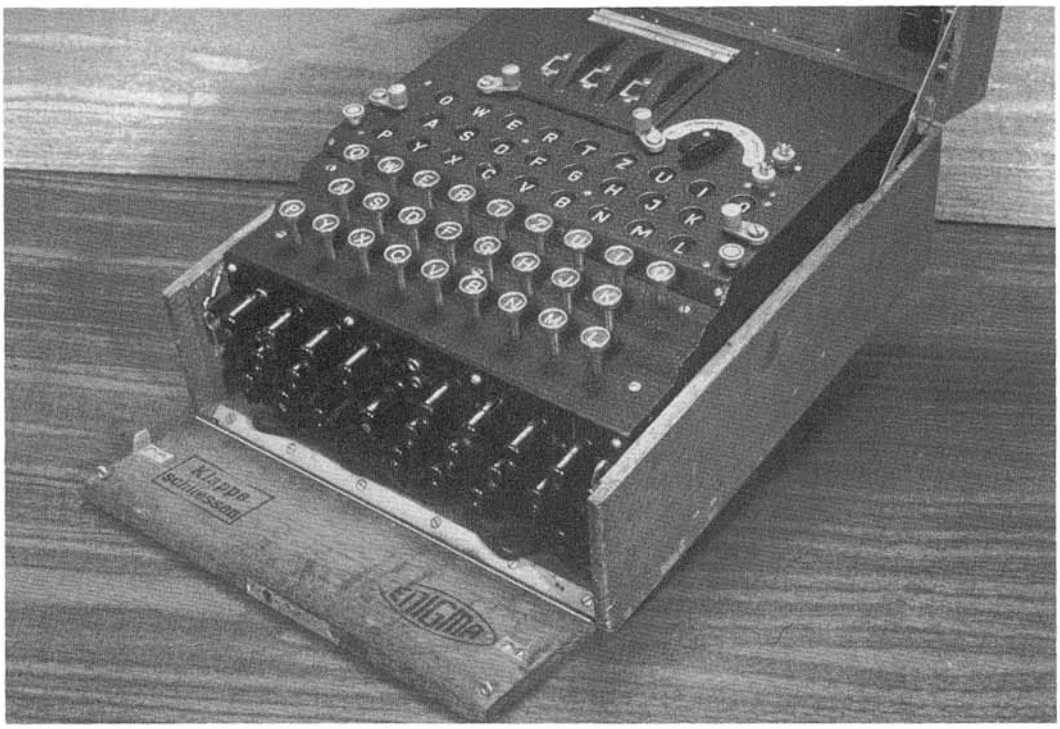
Marian Rejewski

Jerzy Rozycki

Henryk Zygalski

"ULTRA was the greatest secret of World War II after the atom bomb. With the exception of knowledge about that weapon and the probable exception of the time and place of major operations, such as the Normandy invasion, no information was held more tightly. ... The security implies ULTRA's significance. ULTRA furnished intelligence better than any in the whole long history of humankind. It was more precise, more trustworthy, more voluminous, more continuous, longer lasting, and available faster, at a higher level, and from more commands than any other form of intelligence - spies or scouts or aerial reconnaissance or prisoner interrogations. ... It may be concluded that ULTRA saved the world two years of war, billions of dollars, and millions of lives."

David Kahn, *Seizing the Enigma*[3]



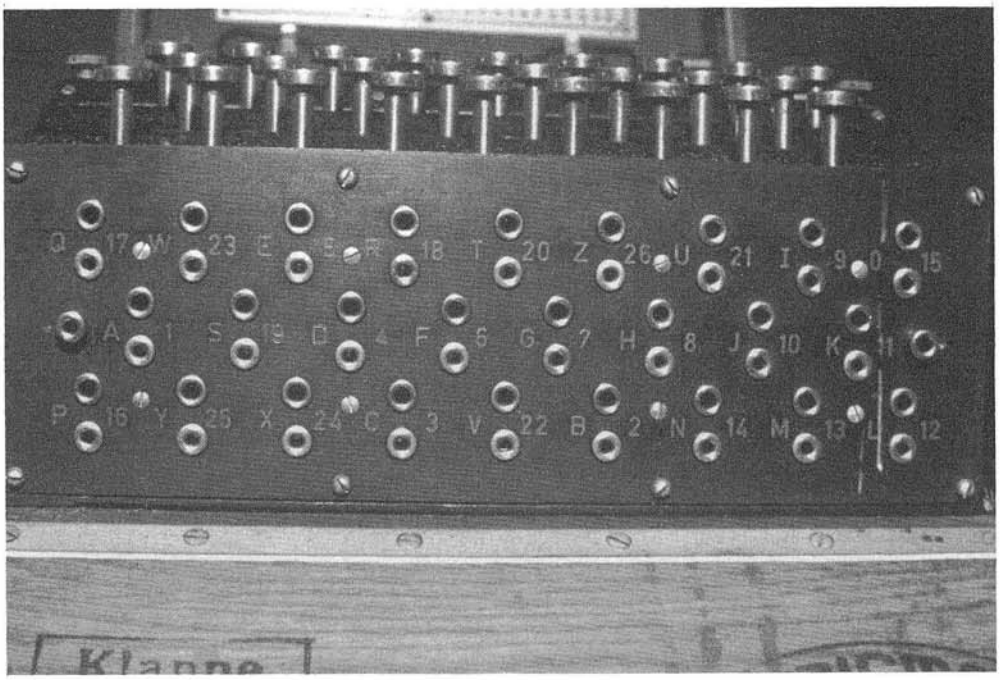
Exterior view of Enigma showing front plugboard with cables.

The Enigma cipher machine is one of the best known cipher machines in the world. Initially broken by Polish cryptanalysts, Enigma decrypts from British and later American efforts were given the cover name ULTRA to reflect the value of the information. Today the Enigma stands as a silent sentinel to the folly of those who placed their absolute confidence in its security. But it also stands in renowned tribute to the cryptanalysts who pitted their minds against a problem of seemingly invincible odds, and who scaled its lofty heights.

Just how difficult was the Enigma cipher machine? Much has been written in recent years about the attacks against Enigma or the intelligence value of the ULTRA decrypts. However little has been said about the defenses of the machine itself and why it was so trusted by its German designers. This paper sheds some light on that topic by calculating the incredible number of possible key settings and machine configurations, a number which led German forces to place undeserved confidence in Enigma's security.[1] Both the theoretical and

[1]For example after analysis of this very topic one German cryptographer wrote "From a mathematical standpoint we cannot speak of a theoretically absolute unsolvability of a cryptogram, but due to the special procedures performed by the Enigma machine, the solvability is so far removed from practical possibility, that the cipher system of the machine, when the distribution of keys is correctly handled, must be regarded as

the practical strength of the machine is calculated. The paper also provides an in-depth discussion of Enigma's construction.



Close-up of plugboard with cables removed.

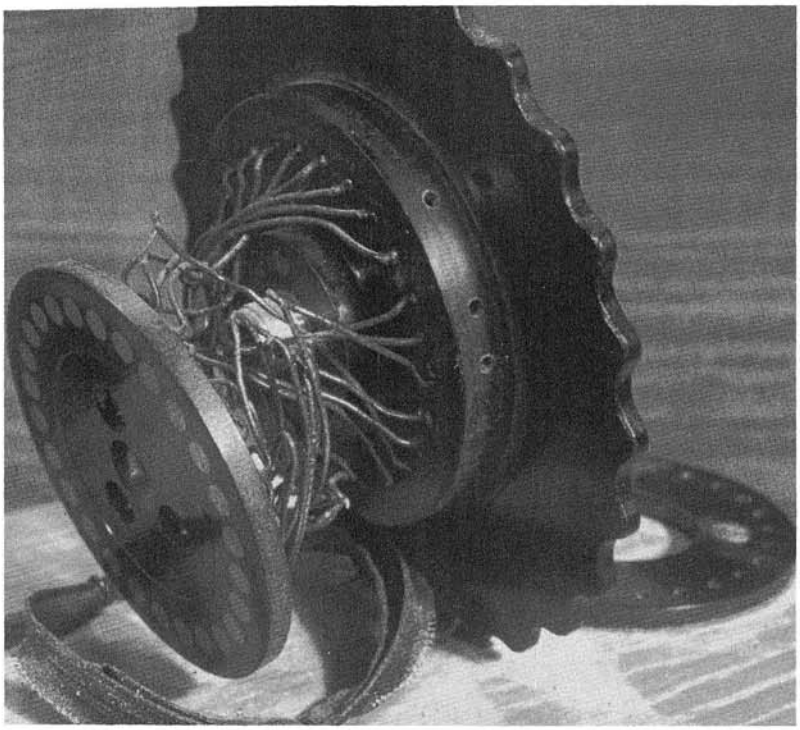
An Enigma cipher machine consisted of five variable components:[2]

1. a plugboard which could contain from zero to thirteen dual-wired cables,
2. three ordered (left to right) rotors which wired 26 input contact points to 26 output contact points positioned on alternate faces of a disc,
3. twenty-six serrations around the periphery of the rotors which allowed the operator to specify an initial rotational position for the rotors,
4. a moveable ring on each of the rotors which controlled the rotational behavior of the rotor immediately to the left by means of a notch, and[3]
5. a reflector half-rotor (which did not in fact rotate) to fold inputs and outputs back onto the same face of contact points.

virtually incapable of solution."

[2]Additional detailed descriptions on Enigma internals can be found in some of the references at the end of this paper. See also the attached diagram and photos.

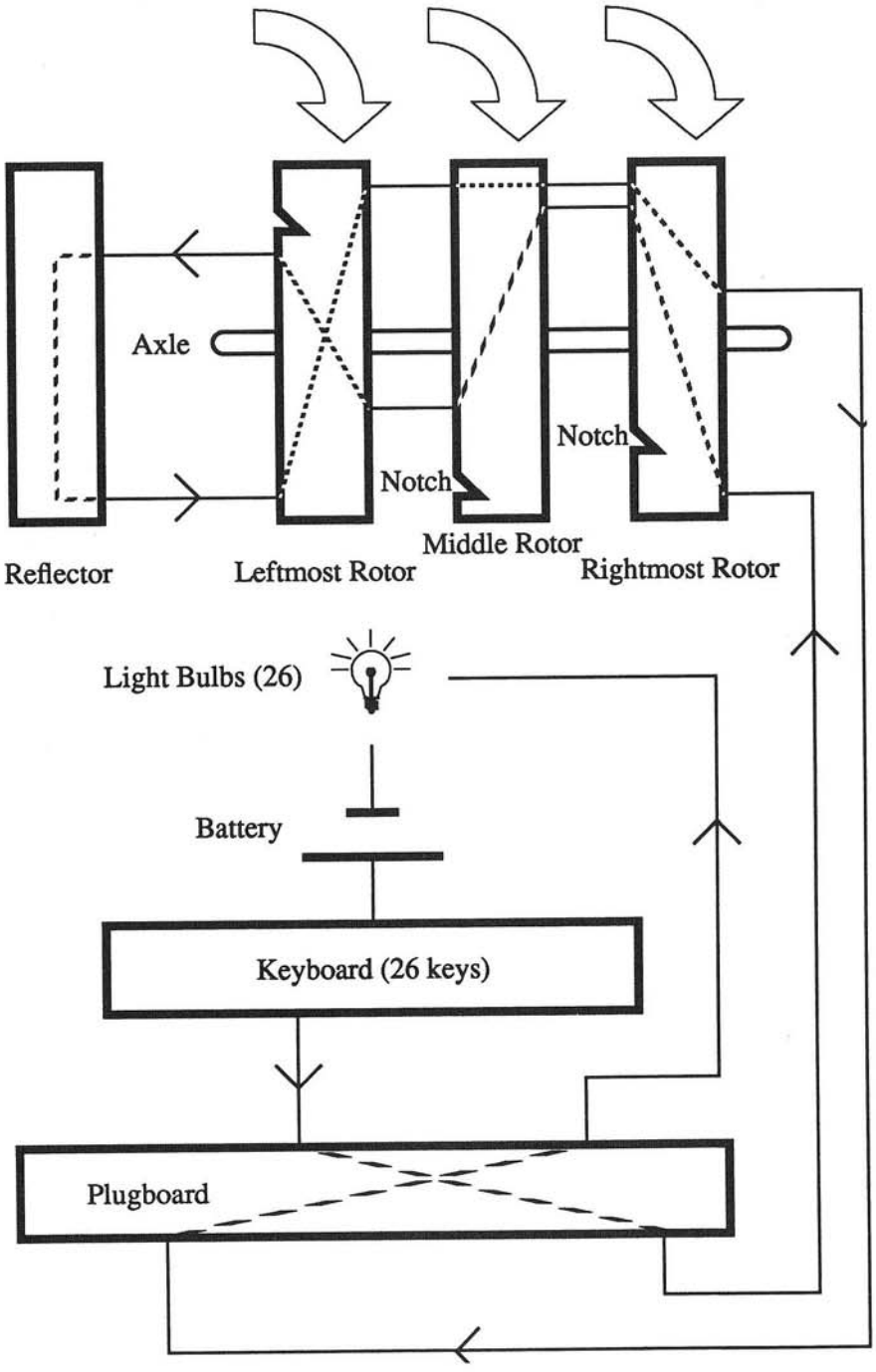
[3]Subsequent Naval Enigmas contained four rotors and up to two notches per ring.



Disassembled rotor. 26 input contact points wired to 26 output contact points on alternate faces of disc.

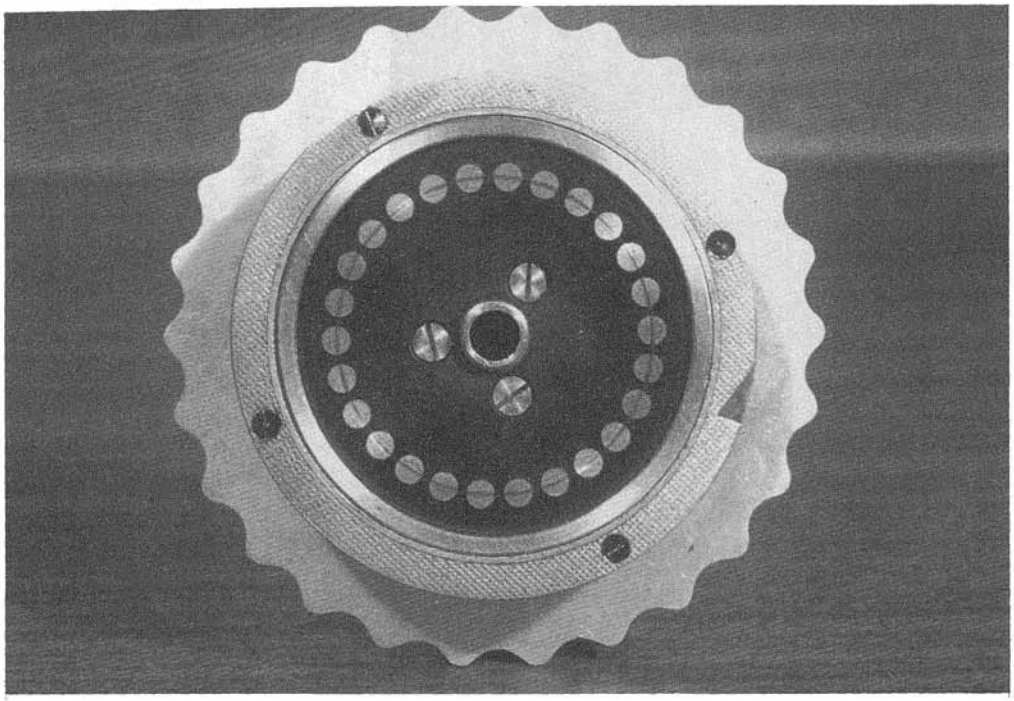
Nothing else on the machine which could be used to set the initial state of the cryptologic was variable. Additional necessary equipment included a mechanical system (stepping levers and ratchets) for forcing rotor rotation, a 26 letter keyboard, 26 light bulbs for the output letters, and a battery for powering the light bulbs. What we wish to determine is the number of different ways of configuring the variable components in the system which contributed to the cryptographic strength of the machine. Although in practice the Germans did not use Enigma to its fullest potential, Allied cryptanalysts could not *a priori* rule out any valid theoretical configuration.

The first variable component was the plugboard. Twenty-six (for A - Z) dual-holed sockets were on the front panel of Enigma. A dual-wired plugboard cable could be inserted making a connection between any pair of letters. Enigma cryptographers had a choice of how many different cables could be inserted (from zero to thirteen) and which letters were connected together. The plugboard functioned like an easily modifiable stationary rotor positioned to the right of



Internal wiring of Enigma showing one connection.

the three rotating rotors.[4]



Close-up of rotor 26 contact points, notch, and serrations.

There were three elements which must be considered when calculating the number of possible plugboard connections: the number of cables used, which group of sockets were selected to receive those cables, and the interconnections within that group of sockets (i.e., the specific letter-pairs created by each cable). We will consider socket selection first. There were 26 sockets on the plugboard. Each individual cable consumed 2 sockets (one for each end of the cable). Given the choice of p plugboard cables ($0 \leq p \leq 13$) inserted into the plugboard, there were therefore $\begin{pmatrix} 26 \\ 2p \end{pmatrix}$ different combinations of sockets which could have been selected.

Having calculated the number of different groups of sockets, we will now determine how many ways in which those p cables could have been inserted into

[4]If a letter's plugboard socket was left unconnected, e.g. the letter **A**, then **A** on the keyboard was wired directly to the **A** input position feeding the rotors. On output a wire coming from the rotors' output **A** position was wired directly to the light bulb **A**. If on the other hand **A** was plugged to **X**, then on input the **A** key was fed to the rotors as **X**, the **X** key was fed to the rotors as **A**, and on output what would have normally illuminated the **A** light bulb now connected to the **X** light bulb, and what before would have gone to **X** instead lit up as **A**.

the $2p$ selected sockets. After inserting the first end of cable #1 into a socket, the second end of the first cable had $2p - 1$ free sockets from which to choose (within that group). After inserting the first end of cable #2 into a socket, the second end of the second cable had $2p - 3$ free sockets from which to choose. This pattern continues down to cable $\#p$; when its second end needed to be inserted into the plugboard only 1 free socket was left open. It should be clear at this point that the total number of ways in which p cables[5] could have been inserted into $2p$ open sockets (with each cable consuming two sockets) is given by $(2p - 1)!!$.

Therefore, given p cables inserted into the plugboard, the number of different connections which could have been made by an Enigma operator is given by the combination of the above two elements or

$$\binom{26}{2p} \times (2p - 1)!! = \frac{26!}{(26 - 2p)! \times p! \times 2^p}.$$

The third and final element which must be factored in is the number of cables used, or p. Using the equation just calculated, the number of plugboard combinations for all possible values of p are given in the following table. One interesting characteristic of the machine is that the maximum number of combinations did not occur at 13 as you might expect, but rather when the operators used 11 plugboard cables.[6]

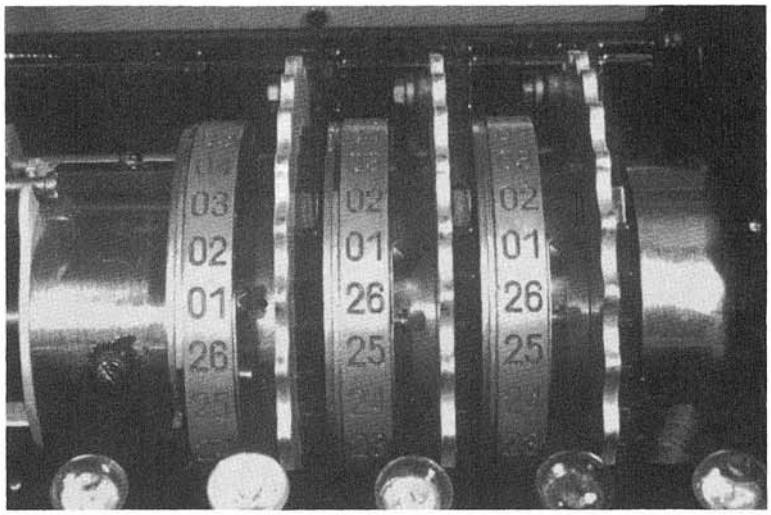
p	combinations	p	combinations
0	1	7	1,305,093,289,500
1	325	8	10,767,019,638,375
2	44,850	9	53,835,098,191,875
3	3,453,450	10	150,738,274,937,250
4	164,038,875	11	205,552,193,096,250
5	5,019,589,575	12	102,776,096,548,125
6	100,391,791,500	13	7,905,853,580,625

Since the combinations possible for each value of p were mutually exclusive, the total number of possible plugboard combinations is given by the sum of the above numbers, or

[5]The boundary condition of $p = 0$ has one interconnection possibility.

[6]The Germans used a variety of connections. In 1940, for example, keys were recovered that used from 6 to 11 plugboard cables. In 1941 they standardized on 10 plugboard cables for all traffic.

$$\sum_{p=0}^{13} \frac{26!}{(26-2p)! \times p! \times 2^p} = 532,985,208,200,576.$$



Close-up of rotors inside of machine. Reflector is to the left.

The second variable component was the three ordered (left to right) rotors which wired 26 input contact points to 26 output contact points positioned on alternate faces of a disc. This equation is straightforward. There are of course 26! unique discs which could have been constructed.[7] Of those 26! any one of them could have been selected by the cryptographers to occupy the leftmost position. The middle position could have been occupied by one of the $26! - 1$ discs which were left. And the rightmost disc could have been selected from any one of the $26! - 2$ discs still remaining. The total number of ways of ordering all possible disc combinations in the machine is therefore $26! \times (26! - 1) \times (26! - 2)$.[8]

[7] $26! = 403,291,461,126,605,635,584,000,000$. Since the rotor discs were hardwired such a vast number would have been impossible in practice to construct. Indeed, only a very small handful of rotor discs were ever constructed since they were limited to what troops could physically carry with them. Also the Germans never changed the disc wirings during the war. They did, however, create several different groups of rotor disc wirings for special purpose machines. (For example the High Command had specially wired Enigmas to communicate with Hitler's Headquarters.) Additionally even if the practical rotor disc wirings were compromised the rotor ordering was still an unknown, although of course the equation is much smaller under those conditions. Furthermore, German cryptographers knew attacking cryptanalysts would have to initially sift through all possible combinations. Finally they could have deployed "pluggable rotor discs" which could have been changed by the operators in the field and thus would have restored the number of practical combinations back to the number of theoretical combinations. ("Pluggable reflectors" were in fact deployed later in the war; see below.) See the final section of the paper for a practical and not a theoretical example.

[8] It was known that the German troops carried individually numbered and unique sets of rotors. Hence

The third variable component of Enigma was the initial rotational position of the three rotors containing the wired discs. This was specified by the cryptographers and set by the machine operators by means of 26 serrations around the rotor periphery. Since each of the three rotors could be initially set into one of 26 different positions the total number of combinations of rotor key settings was 26^3 or 17,576.

The fourth variable component of the machine was a moveable ring on each of the rotors; each ring contained a notch in a specific location.[9] The purpose of the notch was to force a rotation of the rotor immediately to the left when the notch was in a particular position. The rightmost rotor rotated every time a key was pressed. The rightmost rotor's notch forced a rotation of the middle rotor once every 26 keystrokes. The middle rotor's notch forced a rotation of the leftmost rotor once every 26×26 keystrokes. Since there were no more rotors, the leftmost rotor's notch had absolutely no effect whatsoever. (The reflector, positioned to the left of all rotors, did not move.)

Therefore, only two notches contributed to the cryptographic strength of the machine. Since each of them could have been positioned in any one of 26 possible locations, 26^2 combinations were possible or 676.

The fifth and final variable component of Enigma was the reflector. The reflector had 26 contact points like a rotor, but only on one face. Thirteen wires internally connected the 26 contact points together in a series of pairs so that a connection coming in to the reflector from the rotors was sent back through the rotors a second time by a different route. The internal wiring could be constructed in the following fashion. Connecting one end of the first wire to contact point#1, the other side of the wire had 25 different contact points to which it could be connected. Thus the first wire consumed two contact points and had 25 different possibilities. The second wire also consumed two contact points, and had only 23 different connection possibilities remaining from the unconsumed contact points. The third wire consumed two more contact points and had 21 possibilities for connection. The pattern should be apparent by now; the number of distinct reflectors which could have been placed into Enigma was[10]

---

selecting a rotor reduced the number of possibilities by one. So $26!^3$ is not the correct value.

[9]The ring also held the A-Z indicators specified by the cryptographers as part of the key setting. The operators used this as a guide when setting the rotor in step 3. Moving the notched ring against the wired disc also had the secondary effect of moving the A-Z indicators against the disc as well. This technically linked the rotational position in step 3 with the notch position in step 4. However, since it was possible to place the internal wired disc in any one of the 26 positions and the notched ring separately in any one of the 26 positions these were, in fact, independent variables when counting initial cryptographic machine states.

[10]In practice the operators did not frequently change the reflector in the Enigma. Only a handful of hard wired reflectors ever saw service. Additionally, reflectors were created that also had different internal wiring for the special purpose Enigmas. However, just as with the rotors, German cryptographers knew that initially

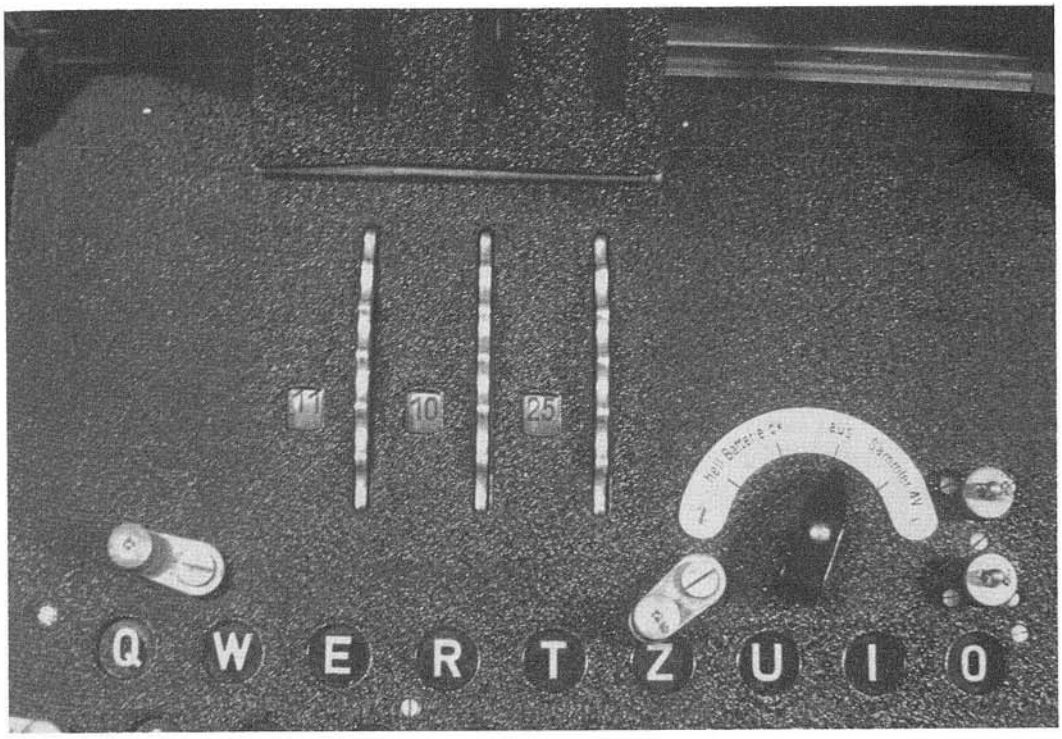
$$25!! = \frac{26!}{(13! \times 2^{13})} = 7,905,853,580,625.$$

Reflector with rotors removed.

(It is interesting to notice that the number of different reflector combinations is also the same as the number of possible plugboard combinations when $p = 13$ cables were used. This should not be surprising; in both cases the value represents the number of possible pair-wise combinations which can be made given 26 choices and 13 connecting wires.)

We now have everything we need in order to calculate the theoretical number of possible Enigma configurations. It is simply the product of all five values calculated above which is approximately 3×10^{114}. To see just how large that number is, consider that it is estimated that there are only about 10^{80} atoms in the entire observable universe. No wonder the German cryptographers had confidence in their machine!

Allied cryptanalysts would have to sift through all possible combinations. It was not until later that some four rotor Naval machines gained easily selectable interchangeable reflectors. Even later, German cryptographers developed and deployed pluggable reflectors which could be rewired by the operators in the field. This restored the number of practical reflector combinations back to the theoretical value.



Initial rotational position of a three rotor Enigma.

The three rotor, single notched Enigma was by far the most common model in use by German forces. Later in the war, however, the German Navy adopted a variant version of the Enigma cipher machine which used four rotors, and rings which contained either a single or a dual notch. Let's recalculate the theoretical number of key settings and machine configurations for a Naval Enigma to see how those modifications increased the strength of the machine.

Step 1 is the number of plugboard combinations. Obviously the fourth rotor and the extra notches had absolutely no affect on this value; it is unchanged at 532,985,208,200,576.

Step 2 is the selection and the ordering, left to right, of the wired rotor discs. The previous value calculated was $26! \times (26! - 1) \times (26! - 2)$. It is tempting to simply add in the factor $(26! - 3)$. However, the new fourth rotor was not interchangeable with the other rotors; it could only be placed in one location.[11]

[11] The Germans did not want to retool their equipment and change the internal mechanics of the Enigma. Hence there was no fourth stepping lever to cause rotation of that rotor during a message. Since no stepping lever was present, the ratchets the lever interacted with were not added to the fourth rotor. This meant the fourth rotor (positioned on the extreme left next to the reflector) was incompatible, and could not be used in the other three rotor locations.

This meant that selection of the fourth rotor was independent, and since there were 26! ways that the rotor's disc wiring could have been constructed,[12] the new equation is given by $26! \times (26! - 1) \times (26! - 2) \times 26!$.

Step 3 is the initial rotational positions of the wired discs. As all four could have been in any one of 26 possible positions the number of combinations is 26^4 or 456,976.

Step 4 is the initial positions of the moveable notched rings. The German Navy added a second notch to some rings in order to increase the irregularity of the rotational behavior of the rotors. We will therefore calculate all possible combinations of single or dual notched rings in each of the rotor positions. For a ring containing a single notch we've already seen that the notch could have been placed in one of 26 possible orientations. A ring containing two notches, on the other hand, had 26×25 possible orientations. Since these two cases were mutually exclusive of each other, the total number of combinations is expressed as the sum of the two values or $26 + (26 \times 25) = 26^2$. Now on the three rotor Enigmas, as previously stated, the notch locations only mattered for the rotors placed into the rightmost and middle positions. As it turns out, that is also true for the four rotor Naval Enigmas as well. Since the fourth rotor had no ratchets and the Enigma had no fourth stepping lever the fourth rotor did not move; once the Enigma operator had set the initial rotational position by hand, it remained constant for the duration of the message.[13] So then the total number of possible single or dual notched ring positions on the rightmost and middle two rotors is given by 26^4 or 456,976.

Step 5 is the reflector wiring. Due to cramped conditions on board ship, the Germans did not want to add the extra space required for the fourth rotor, thereby making the Enigma wider than it was before. Instead, they made a special half-width reflector so that the machine could continue to fit into the same sized space. However, the total number of possible wiring configurations does not change from what we calculated above, or 7,905,853,580,625.[14]

We are now ready to determine the theoretical number of possible Naval Enigma configurations assuming four rotors and single or dual notches in the

[12] In practice, the Navy initially deployed only one new fourth rotor disc. Later they added a second disc. But as before, Allied cryptanalysts were initially faced with determining which wiring configuration was used from all possible combinations.

[13] This had a nice side effect, however. In practice, the fourth rotor and its new reflector had wiring chosen such that in one particular orientation the combination had exactly the same effective wiring as reflectors built for three rotor Enigmas. This gave the four rotor machines the ability to still communicate with the older three rotor machines.

[14] In practice, the Navy introduced just one half-width reflector at the same time they introduced their first fourth rotor. A second half-width interchangeable reflector was released at the same time their second fourth rotor was released. Pluggable reflectors followed all of these events.

rings. It is the product of all five values calculated above which is approximately 2×10^{145}.

The numbers derived thus far are only theoretical values which reflect how many initial cryptographic machine states were possible. In practice once the war started Allied cryptanalysts had a much easier job. As a final exercise, we'll calculate the number of possible cryptovariables cryptanalysts were likely to encounter when trying to determine the daily keys. Some information was known by the Allies to be effectively constant.

In step 1, the plugboard, the most common value of p used was 10. Since the number of cables was known, all that needed to be determined on a daily basis was which 20 letters had a cable patch inserted and the 10 pairs created by those 20 letters. This is already given in the table under $p = 10$ as the value 150,738,274,937,250.

In step 2, the selection and ordering of the rotor discs, things changed over time. Initially only three rotor discs were created for general purpose use. (Special purpose machines, as previously stated, had their own set of wirings.) Later, two additional rotor discs were introduced making five total. The German Navy added an additional three rotor discs bringing their total to eight. And finally, one and then two extra fourth rotor discs (without rotation ratchets) were added by the Navy giving them 10 possible discs.

We will assume the general purpose case of five discs and further assume the wiring of each of the discs is known. We will also assume this is an Enigma machine with three rotors. What Allied cryptanalysts had to determine was which three of the five possible discs were chosen, and in which order they were placed into the machine. This is simply $\begin{pmatrix} 5 \\ 3 \end{pmatrix}$ or $5 \times 4 \times 3 = 60$ possible combinations which needed to be checked.

In step 3, the initial rotational position of the rotors was an unknown key setting for which there were 26^3 or 17,576 possible values.

In step 4, the position of the notched rings, we will assume single notches on all of the rings. (Dual notched rings were not introduced until the Navy added their extra three rotor discs.) This is 26^2 or 676.[15]

[15] Some may choose to add another factor of 26 at this point, since the daily key was formally given by three positions for the rings (step 4) followed by rotational orientation of the three rotors (step 3). As previously stated, moving the rings containing the notches had the side effect of moving the indicators used as a guide by the operators used in step 3. So although the notch was unimportant in the leftmost rotor due to the reflector, the ring position was very important to ensure the disc wiring was oriented correctly given an indicator for step 3. However, since there are 26 ways to specify the combination of ring position and indicator selection which will yield the exact same disc wiring orientation in the leftmost rotor, we can factor the 26 back out of the

In step 5 we will assume the operators are using a single reflector in which the wiring is already known so the number of combinations here is simply 1.

Enigma being used in the field. Panzer General Heinz Guderian and Enigma operators in command vehicle in France, 1940.

Thus the possible cryptovariable space Allied cryptanalysts were typically faced with during the Second World War when attempting to read Enigma traffic is the product of the above five values which is approximately 1×10^{23}, or stated

equation again.

another way about one hundred thousand billion billion.[16] Although that value is much smaller than the total number of atoms in the entire observable universe it is still quite an impressive number! This is all the more true considering Allied cryptanalysts were faced with continually changing message keys on at least a daily basis - for every different radio network the Germans constructed.

With such daunting odds facing any cryptanalyst, it is not surprising that the German cryptographers felt secure using the Enigma. The strength of the large numbers, numbers so vast they are really beyond true comprehension, led the Germans to have absolute and complete confidence in the integrity of the Enigma cipher machine. And in that misplaced confidence, the Germans were absolutely, completely, and fatally wrong.

REFERENCES

1. Erskine, Ralph and Frode Weierud. 1987. Naval Enigma: M4 and its Rotors. *Cryptologia*. 4(3): 235-244.

2. Hinsley, F. H. 1979, 1981. *British Intelligence in the Second World War. 2 Volumes*. London: Her Majesty's Stationery Office.

3. Kahn, David. 1991. *Seizing the Enigma*. Boston: Houghton Mifflin Company.

4. Kozaczuk, Wladyslaw. 1984. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*. Edited and Translated by Christopher Kasparek. Frederick, Maryland: University Publications of America, Inc.

5. Office of the Chief of Naval Operations CNC-OP-20. 1980. *Enigma Series: Volume 1. Click Process*. On file at the Smithsonian American History Museum. RIP 603, Reg. No. 9, Communications Intelligence Technical Paper TS-10/E-1, Filed 2 December 1980.

6. Woytak, Richard. 1982. A Conversation with Marian Rejewski. Transcribed and Translated by Christopher Kasparek. *Cryptologia*. 6(1): 50-60.

BIOGRAPHICAL SKETCH

A. Ray Miller received a BS in Computer Science from the University of Central Florida in 1979. He received an MS and a PhD in Computer Science from the

[16] Billion is to be understood in the American and not in the European sense.

University of Illinois in 1984 and 1987, respectively. While in school, he worked at the Naval Experimental Computer Simulation Laboratory, the Department of Computer Science at the University of Illinois, and the Center for Supercomputing Research and Development. Dr. Miller has been employed at the National Security Agency since 1987, and has taken a tour at the Supercomputing Research Center. He has received 19 awards and commendations during his seven years at the NSA. Dr. Miller is the author of several papers.