# ENIGMA: AN ANALYSIS AND MAPLET SIMULATOR

Rick Klima
Department of Mathematical Sciences
Appalachian State University
342 Walker Hall
Boone, North Carolina 28608
klimare@appstate.edu

Neil Sigmon
Department of Mathematics
Radford University
212 Walker Hall
Radford, Virginia 24142
npsigmon@radford.edu

A *cipher* is a method for disguising information so that ideally it cannot be understood by anyone but the intended recipient. *Cryptanalysis* refers to the process of an unintended recipient of disguised information attempting to remove the disguise and understand the information. Successful cryptanalysis is called *breaking* a cipher.

When a cipher is used to exchange information, the undisguised information is called the *plaintext*, and the disguised information the *ciphertext*. The process of converting from plaintext to ciphertext is called *encryption*. Upon receiving a ciphertext, the recipient must remove the disguise, a process called *decryption*. To be able to effectively encrypt and decrypt messages, correspondents must typically share knowledge of a secret *key*, which is used in applying the cipher. More specifically, the key for a cipher is information usually known only to the originator and intended recipient of a message, which is used by the originator to encrypt the plaintext, and the recipient to decrypt the ciphertext.

**The Enigma Cipher Machine**

In 1918, German electrical engineer Arthur Scherbius applied for a patent for a mechanical cipher machine. This machine, later marketed commercially under the name *Enigma*, was designed with electric current running through revolving wired wheels, called *rotors*. Scherbius offered his machine to the German military, and while they did not find any deficiencies in it, they did not choose at that time to purchase any. Only years later, after learning that their World War I ciphers had routinely been broken, did the Germans adopt various models of the Enigma, which they used as their primary resource for encrypted communications throughout World War II. In this section, we will present some technical details of two of these models, the *Wehrmacht* Enigma, used by the German army, and the *Kriegsmarine M4* Enigma, used by the German navy.

An Enigma consisted of four components: a 26-letter keyboard for entering input letters (either plaintext or ciphertext), a plugboard resembling a miniature old telephone switchboard, a system of rotors, and a 26-letter lampboard for displaying output letters. Pressing an input letter on the keyboard sent electric current through the plugboard and rotors, where the encryption or decryption took place, and the current ended at the lampboard where a small bulb was illuminated to indicate the output letter. The layout of letters on the keyboard and lampboard was similar to the layout on a modern keyboard.

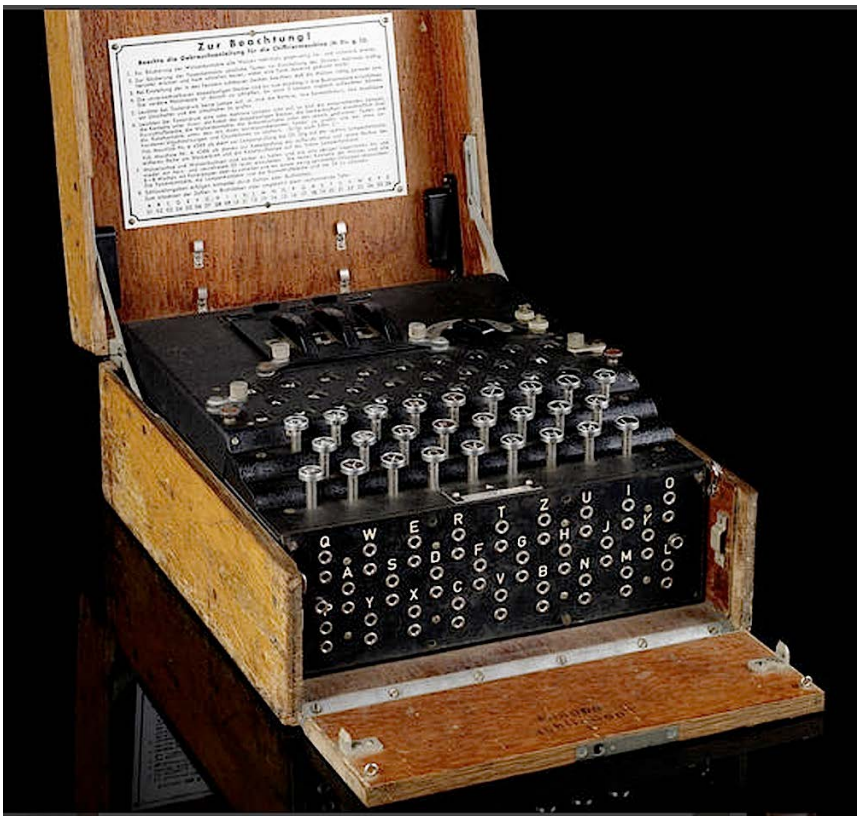


**Figure 1: Enigma Cipher Machine, Front View**

Pressing an input letter on an Enigma keyboard sent current designating the letter first to the plugboard. The plugboard was situated in the front of an Enigma, and had 26 open sockets, one to represent each possible letter. The plugboard sockets could either be left open or connected in pairs by short cables. If a pair of plugboard sockets were connected by a cable, then current designating either letter represented by the sockets would be converted at the plugboard to designate the other letter. If a plugboard socket were left open, then current designating the letter represented by the socket would leave the plugboard still designating the same letter.

There were many different choices for which plugboard sockets could be connected in an Enigma, with anywhere from zero to 13 cables used, and usually a very large number of possibilities for which pair of sockets could be connected by each cable. Varying the number of cables would have maximized security, but standard German operating procedure was to use a fixed number of cables. With a fixed number of cables, 11 cables would have maximized security (as is shown in [1]), but for most of the war standard German operating procedure was to use 10 cables. Each Enigma provided for use in the field came with 12 cables, with two held in reserve in case any of the 10 in use became faulty.

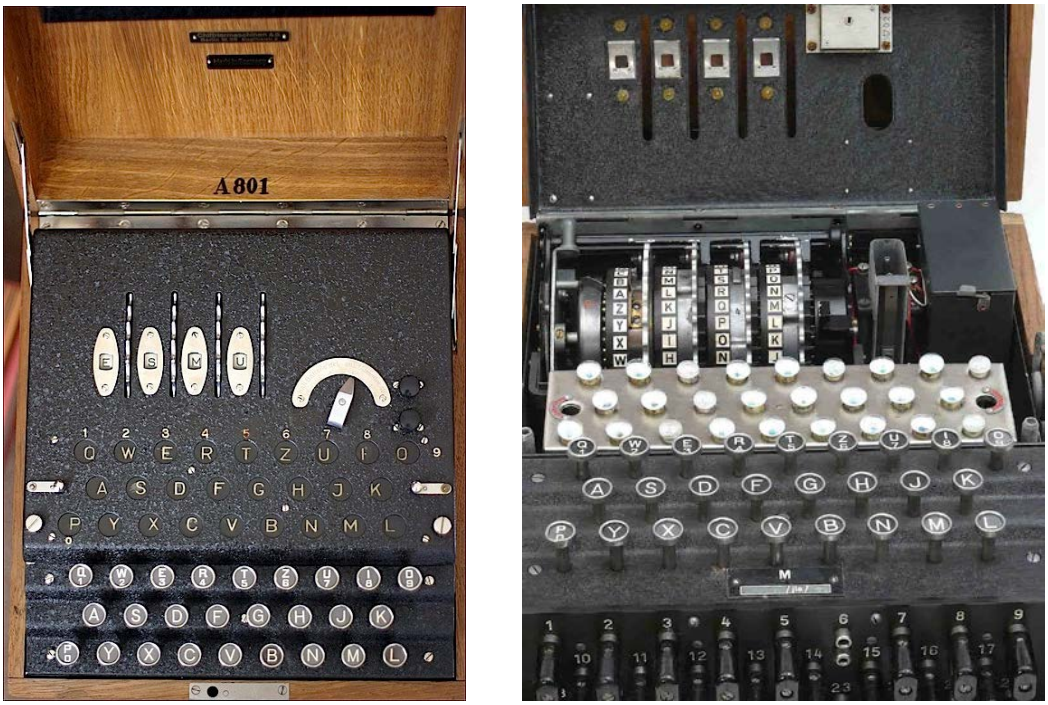


**Figure 2: Enigma Cipher Machine, Top View**

After leaving the plugboard, current went through a system of rotors situated in the back of an Enigma. Each individual rotor was a circular disk about the size of a hockey puck. We will call the flat sides of a rotor the *right* and *left* sides, since rotors could only be placed in an Enigma standing on end with either side facing in a particular direction. Both flat sides of a rotor contained 26 contact points, one to represent each letter, with the letters listed in alphabetical order around both sides of the rotor clockwise (when the rotor is viewed from the right). The contacts on the right side of a rotor were wired to the contact points on the left, but not necessarily straight across. The idea was that current could enter one side of a rotor at one of the contact positions, representing a letter, and pass through and exit the rotor on the other side at a different contact position, representing a different letter.

Wehrmacht Enigmas could accommodate three rotors side-by-side, while Kriegsmarine M4 Enigmas could accommodate four. Although rotors could only be situated with each side facing in a particular direction, current could pass through the rotors in either direction. The reason for this is that while current always initially passed through the rotors from right to left, to the left of the rotor slots a reflector sent the current back through the rotors from left to right. In addition, the reflector was itself like half a rotor in the sense that on its right side were 26 contact points, one to represent each letter, but on its left side were no contacts. The contacts on the right side of a reflector were wired to each other in 13 pairs. Unlike plugboard sockets, reflector contacts were always fully connected. Also, unlike rotor contacts, reflector contacts could not be connected in a way such that a letter was connected to itself.

There were many different choices for how rotor and reflector contacts could be connected in an Enigma, but because rotors and reflectors had to be hard-wired and changing the wiring was very difficult, rotors and reflectors with only a very small number of different wirings were ever produced and used in the field. Rotors with only five different wirings were produced for Wehrmacht Enigmas. These rotors were labeled with the Roman numerals **I–V**, and the contacts connected in each are listed in [1]. Of these five rotors, three were used at a time in Wehrmacht Enigmas. Any three could be used, and they could be arranged in any order.

Kriegsmarine M4 Enigmas could hold four rotors in the same space that Wehrmacht Enigmas had for three. This was accomplished by using a thinner reflector, which allowed for a thinner fourth rotor to be inserted between the leftmost full-size rotor and the reflector. For the three full-size rotors in Kriegsmarine M4 Enigmas, any of the Wehrmacht rotors **I–V** could be used, as well as any of three additional rotors with different wirings. These three additional full-size rotors were labeled with the Roman numerals **VI–VIII**, and the contacts connected in each are listed in [1]. The eight full-size rotors **I–VIII** were too wide to fit into the space available for the thinner fourth rotor in Kriegsmarine M4 Enigmas. For this thinner fourth rotor, rotors with only two different wirings were produced. These rotors were labeled with the Greek letters β (beta) and γ (gamma), and the contacts connected in each are listed in [1].

Reflectors with only two different wirings were produced for Wehrmacht Enigmas. These reflectors were labeled with the letters **B** and **C**, and the contacts connected in each are listed in [1]. Because Kriegsmarine M4 Enigmas were modified to hold four rotors instead of three, reflectors produced for Wehrmacht Enigmas were too wide to fit in them. As a result, different thinner reflectors had to be produced for Kriegsmarine M4 Enigmas. Reflectors with only two different wirings were produced for Kriegsmarine M4 Enigmas. These thinner reflectors were also labeled with the letters **B** and **C**, and the contacts connected in each are listed in [1].

As we have noted, pressing an input letter on an Enigma keyboard sent electric current through the plugboard and rotors, and the current ended at the lampboard where a small bulb was illuminated to indicate the output letter. To be more precise, pressing an input letter sent electric current first through the plugboard, then through the rotors (either three or four depending on the Enigma model) from right to left, through the reflector, back through the rotors from left to right, and then through the plugboard a second time. After leaving the plugboard the second time, the current went to the lampboard where a bulb was illuminated to indicate the output letter. This clearly gives a very large number of possible configurations for an Enigma. However, we are not done. Before a rotor was placed in an Enigma, it could be rotated into any of 26 possible orientations. The orientation of a rotor in an Enigma dictates the path that current follows through the rotor.

To assist Enigma operators with orienting rotors correctly, etched in a ring around the edge of each rotor were the letters A–Z (or sometimes the numbers 01–26), listed in order

clockwise (when the rotor was viewed from the right). For each rotor slot in an Enigma, a small window was cut to show the letter (or number) at a particular location on the ring. We will call this letter the *window letter*. The window letter for a rotor indicates the orientation of the rotor.

A number called the *rotor offset* also indicates the orientation of a rotor in an Enigma. The rotor offset for a rotor is a whole number between 0 and 25, with 0 meaning the rotor is in its original orientation (for which the window letter will be A), 1 meaning the rotor has been rotated 1 position counterclockwise (when viewed from the right), 2 meaning the rotor has been rotated 2 positions counterclockwise, and so on, through 25 meaning the rotor has been rotated 25 positions counterclockwise. There is no need to consider rotor offsets larger than 25, since rotating a rotor 26 positions counterclockwise will take the rotor back to its original orientation with rotor offset 0.

The etched ring around the edge of an Enigma rotor was also movable, and could be rotated into any of 26 different positions while the wired part of the rotor was held fixed. This is a complication, because rotating the ring changes the window letter without changing the rotor offset. A number called the *ring setting* indicates the position of the ring on a rotor. The ring setting for a rotor is a whole number between 1 and 26, with 1 meaning the ring is in its original position (for which with rotor offset 0 the window letter is A), 2 meaning the ring has been rotated 1 position counterclockwise (when the rotor is viewed from the right), 3 meaning the ring has been rotated 2 positions counterclockwise, and so on, through 26 meaning the ring has been rotated 25 positions counterclockwise. There is no need to consider ring settings larger than 26, since rotating a ring 26 positions counterclockwise will take the ring back to its original position with ring setting 1.

The various rotor offsets and ring settings increase the number of possible configurations for an Enigma to an astronomically large number. Even so, everything we have presented so far would have ultimately made for nothing more than a glorified substitution cipher had it not been for one final feature that we have not yet mentioned—the rotors revolved within the machine during the actual encryption and decryption processes.

Encrypting and decrypting with an Enigma was done one letter at a time, and each time an input letter was pressed on the keyboard, the rightmost rotor would immediately (before current reached the rotors) rotate one position counterclockwise (when the rotor was viewed from the right). In addition, for each Enigma rotor **I–VIII**, there was either one or two notches on the ring around the rotor. Since each notch was on the ring, its position in the rotor slot at any time could be identified solely by the window letter. For each notch, there was one particular position in the rotor slot, identified by a window letter called the *notch letter*, for which if the rotor rotated one position counterclockwise, the notch would cause the rotor to the left, if it were one of the rotors **I–VIII**, to also rotate one position counterclockwise. That is, for each notch on the ring on the rightmost rotor, once every 26 times the rotor rotated one position counterclockwise the notch would cause the middle full-size rotor to also rotate one position counterclockwise, and for each notch on the ring on the middle full-size rotor, once every 26 times the rotor

rotated one position counterclockwise the notch would cause the leftmost full-size rotor to also rotate one position counterclockwise. Additionally, for the middle full-size rotor only, if a notch letter was showing in the window when an input letter was pressed, the middle full-size rotor would itself rotate one position counterclockwise, regardless of whether a notch on the ring on the rightmost rotor would have caused it to rotate. The notch letters for each of the Enigma rotors **I–VIII** are listed in [1].

To clarify, during the actual encryption and decryption processes, only Enigma rotors rotated, not the rings around the rotors. Once a ring had been set in the initial configuration of the machine, its location around its rotor was fixed, and during the encryption and decryption processes, the rotation of the rotor alone changed the window letter. Also, only the full-size rotors **I–V** used in Wehrmacht Enigmas and **I–VIII** used for the rightmost three rotors in Kriegsmarine M4 Enigmas rotated. The thinner rotors β and γ used for the leftmost rotor in Kriegsmarine M4 Enigmas never rotated, although they could be set in the initial configuration of the machine with a nonzero rotor offset. On the other hand, in both Enigma models the reflectors **B** and **C**, which also never rotated, were always set with a zero offset. Finally, after an input letter was pressed on the keyboard, all rotation of the rotors occurred before current reached the rotors, and no additional rotation occurred until the next input letter was pressed.

Finally, for current traveling through an Enigma, since the current went through the plugboard at the start of its journey and then again at the end, and through the rotors from right to left before going through the reflector and then again from left to right after, and reflector contacts were always connected in pairs, the machine would always produce input/output letters in pairs. That is, for example, for identical configurations of an Enigma, if entering input letter E yielded output letter G, then entering input letter G would yield output letter E. What is important about this is that for a ciphertext formed using an Enigma, the ciphertext could be decrypted by initially configuring the machine identically to how it had been initially configured during the encryption of the message, and then inputting the ciphertext letters.

In the field during World War II, a ciphertext formed using an Enigma was decrypted by initially configuring a different Enigma identically to how the machine used to encrypt the message had been initially configured, and then inputting the ciphertext letters. Thus, the key for an Enigma cipher was the complete initial configuration of the machine used to encrypt the message, including how the plugboard had been wired, which rotors had been used in order with ring settings and initial window letters, and which reflector had been used. Despite this, from a technical perspective the Enigma was not difficult for operators to use in the field, since they did not have to understand the encryption or decryption processes, but only how to configure the machine.

**Maplet Simulator for the Enigma Cipher Machine**

Our recent interest in cryptology at the general education level culminated with the publication of the book *Cryptology, Classical and Modern, with Maplets* [1]. In addition

to being a dynamic and enthralling subject that even the most ambivalent towards mathematics can have a natural interest in, cryptology has a rich legacy of importance throughout human history. Our book is designed not only to introduce general education students to the importance of mathematics and cryptology in their everyday lives, but also to the importance of mathematics and cryptology throughout history.

One area of emphasis in the book is our careful description, analysis of security, and Maplet simulation of the Enigma cipher machine. A screenshot of our Maplet simulator for the Enigma is given in Figure 3.

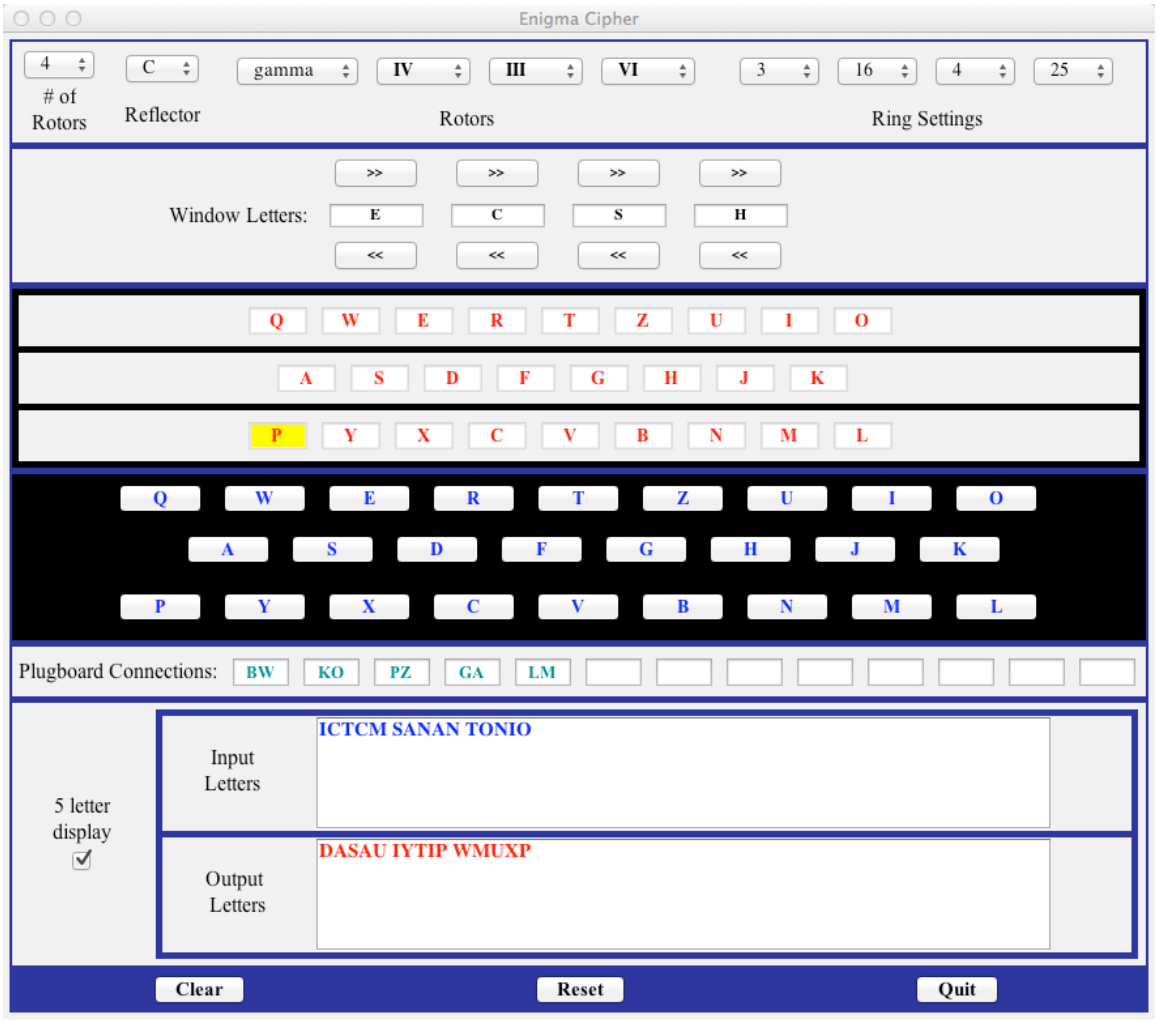


**Figure 3: Maplet Simulator for the Enigma Cipher Machine**

This Maplet can be downloaded from [2], and an example with additional screenshots and accompanying discussion can be found in [1].

A complete list of the types of ciphers and other cryptographic techniques and systems presented and supplemented with Maplets in [1] includes substitution ciphers (with

cryptanalysis), Playfair ciphers, transposition ciphers (with cryptanalysis), ADFGVX ciphers, the Enigma machine, the Navajo code, shift and affine ciphers (with cryptanalysis), Alberti ciphers, Vigenère ciphers (with cryptanalysis), the Friedman and Kasiski tests, Hill ciphers (with cryptanalysis), RSA ciphers (with cryptanalysis), the Diffie-Hellman key exchange, ElGamal ciphers (with cryptanalysis), stream ciphers, the Advanced Encryption Standard, digital signatures, hash functions, and public-key infrastructures. Also included in [1] are basic introductions to combinatorics, modular arithmetic, probability, matrices, the Euclidean algorithm, modular exponentiation, ASCII, primality testing, integer factorization, discrete logarithms, and number base conversions, some supplemented with Maplets, and all presented to a general audience.

## Calculating the Number of Initial Configurations

German cryptologists during World War II were confident that the Enigma cipher machine was unbreakable, since due to the astronomically large number of initial configurations of the machine, it would have been impossible for an Enigma cipher to be broken by trying all possible initial configurations. It is shown in [3] that the theoretical number of initial configurations of a Wehrmacht Enigma is more than $3 \times 10^{114}$, and of a Kriegsmarine M4 Enigma is more than $2 \times 10^{145}$, numbers so large that they are well beyond human comprehension. However, recall that the Germans only used rotors and reflectors with a very small number of different wirings, and for most of the war used a fixed number of plugboard cables. This dramatically reduced the actual number of possible initial configurations.

In order to determine the actual number of possible initial configurations of an Enigma, we will consider separately the five variable components of the machine—the plugboard, arrangement of rotors, ring settings, initial window letters, and choice of reflector. More specifically, we will consider separately the number of initial configurations of each of these variable components, and then combine them to find the number of possible initial configurations of the full machine.

## Plugboard

Recall that an Enigma plugboard consists of 26 open sockets, one to represent each letter, and these sockets can either be left open or connected in pairs by short cables. The number of cables used in the machine can thus range from zero to 13, with exactly twice as many sockets connected. If $p$ cables are used, then $2p$ sockets would be connected, and the number of ways to choose the $2p$ sockets to be connected can be found using the following formula.

$$ {}_{26}C_{2p} = \frac{26!}{(2p)!\,(26-2p)!} $$

For example, recall that for most of the war standard German operating procedure was to use exactly 10 cables. Using this formula, we can find the number of ways to choose 20 sockets to connect using these cables as follows.

$$_{26}C_{20} = \frac{26!}{20!\,6!} = 230{,}230$$

After the $2p$ sockets have been chosen, they must actually be connected using the $p$ cables. Suppose one end of a first cable is plugged into one of the sockets. This leaves $2p-1$ choices for the socket into which the other end of the first cable will be plugged. After this is done, suppose one end of a second cable is plugged into one of the remaining sockets. This leaves $2p-3$ choices for the socket into which the other end of the second cable will be plugged. Continuing in this manner, we find that the number of ways to connect all $2p$ sockets using $p$ cables (as long as $p$ is at least 1) is given by the quantity $S_p = (2p-1)\cdot(2p-3)\cdots 3\cdot 1$. For example, with 20 sockets to be connected using 10 cables, using this formula we find that the number of ways to connect the sockets using the cables is $S_{10} = 19\cdot 17\cdots 3\cdot 1 = 654{,}729{,}075$.

**Arrangement of Rotors**

Recall that rotors with five different wirings were produced for Wehrmacht Enigmas, with three in use in the machine at a time. Thus we can find the number of different ways in which rotors can be arranged from left to right in a Wehrmacht Enigma as follows.

$$_5P_3 = \frac{5!}{2!} = 60$$

For Kriegsmarine M4 Enigmas, rotors with eight different wirings were produced for the rightmost three rotor slots, and rotors with two different wirings for the leftmost rotor slot. Thus we can find the number of different ways in which rotors can be arranged from left to right in a Kriegsmarine M4 Enigma as follows.

$$2\cdot {}_8P_3 = 2\cdot\frac{8!}{5!} = 672$$

**Ring Settings**

Recall that around each Enigma rotor was a movable ring that could be rotated into any of 26 different positions while the wired part of the rotor was held fixed. For Wehrmacht Enigmas, with three rotors in use in the machine at a time, the number of possible ring settings for the rotors is $26^3 = 17{,}576$. For Kriegsmarine M4 Enigmas, with four rotors in use at a time, the number of possible ring settings is $26^4 = 456{,}976$.

**Initial Window Letters**

Recall that before a rotor was placed in an Enigma, it could be rotated into any of 26 possible orientations, each yielding a unique window letter. For Wehrmacht Enigmas, with three rotors in use at a time, the number of possible initial window letters is

$26^3 = 17{,}576$. For Kriegsmarine M4 Enigmas, with four rotors in use at a time, the number of possible initial window letters is $26^4 = 456{,}976$.

**Choice of Reflector**

Recall that reflectors with two different wirings were produced for Enigmas, with one in use in the machine at a time. Thus the number of different ways in which a reflector can be chosen for an Enigma is 2.

**The Full Machine**

Combining the number of initial configurations of each of the variable components of a Wehrmacht Enigma, we find the number of possible initial configurations of the full machine using exactly 10 plugboard cables as follows.

$$_{26}C_{20} \cdot S_{10} \cdot {}_5P_3 \cdot 26^3 \cdot 26^3 \cdot 2 = 5{,}587{,}851{,}741{,}017{,}032{,}206{,}720{,}000$$

For a Kriegsmarine M4 Enigma, we find the number of possible initial configurations of the full machine using exactly 10 plugboard cables as follows.

$$_{26}C_{20} \cdot S_{10} \cdot 2 \cdot {}_8P_3 \cdot 26^4 \cdot 26^4 \cdot 2 = 42{,}306{,}743{,}101{,}588{,}154{,}243{,}518{,}464{,}000$$

(From the perspective of someone actually trying to break an Enigma cipher, these numbers can be reduced by a factor of 26. Because the notch on the ring on the leftmost rotor in an Enigma has no effect on the operation of the machine, for each possible orientation of the leftmost rotor [considering both the ring setting and initial window letter], there are 26 different combinations of a ring setting and initial window letter for which the operation of the machine is identical. For someone trying to break an Enigma cipher, only one of these 26 combinations needs to be considered.)

These numbers were still much too large for an Enigma cipher to be broken during World War II by trying all possible initial configurations. However, they are also very much less than the theoretical number of initial configurations of the full machine. This fact, along with other general mistakes in the overall implementation of the Enigma by the Germans as well as specific mistakes by German operators in the field allowed the Allies to successfully break the machine during World War II.

**References**

[1] R. Klima and N. Sigmon. *Cryptology, Classical and Modern, with Maplets*. Taylor & Francis/CRC Press, Boca Raton, FL, 2012.

[2] R. Klima and N. Sigmon. Textbook homepage for *Cryptology, Classical and Modern, with Maplets*. Available at http://www.radford.edu/~npsigmon/cryptobook.html.

[3] R. Miller. *The Cryptographic Mathematics of Enigma*. Center for Cryptologic History, National Security Agency, 2004.