Math 135: The Art of Secret Writing (Summer 2006)
The Theoretically Possible Number of Enigma Configurations

We outline the calculation of the number of theoretically possible Enigma configurations. The calculation uses only simple combinatorics, and is given in full detail in the pamphlet *The Cryptographic Mathematics of Enigma* by A. Ray Miller and published Center for Cryptologic History. An incomplete version is available online at `http://www.nsa.gov/publications/publi00004.cfm`

An Enigma machine consisted of five variable components:

- a plugboard which could contain from zero to thirteen dual-wired cables;
- three ordered (left to right) rotors which wired twenty-six input contact points to twenty-six output contact points positioned on alternate faces of a disc;
- twenty-six serrations around the periphery of the rotors which allowed the operator to specify an initial rotational position for the rotors;
- 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
- a reflector half-rotor (which did not in fact rotate) to fold inputs and outputs back onto the same face of contact points.

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 operators had a choice of how many different cables could be inserted (from zero to thirteen) and which letters were connected.

Given the choice of p plugboard cables inserted into the plugboard ($0 \leq p \leq 13$) there were therefore $C(26, 2p)$ different combinations of sockets that could have been selected. Once it was decided that $2p$ sockets would be filled by the p cables, there were $(2p-1)$ free sockets for the first cable, $(2p-3)$ free sockets for the second cable, $\ldots$, $(2p-(2p-1)) = 1$ free socket for the pth cable. Hence, there were $(2p-1) \times (2p-3) \times (2p-5) \times \cdots \times 1$ possibilities.

This then gives that if p cables were inserted into the plugboard, the different number of combinations which could have been made by the Enigma operator was

$$\begin{aligned}
C(26,2p) &\times (2p-1) \times (2p-3) \times (2p-5) \times \cdots \times 1 \\
&= \frac{26!}{(26-2p)!(2p)!} \times (2p-1) \times (2p-3) \times (2p-5) \times \cdots \times 1 \\
&= \frac{26!}{(26-2p)!} \cdot \frac{(2p-1) \times (2p-3) \times (2p-5) \times \cdots \times 1}{(2p) \times (2p-1) \times (2p-2) \times \cdots \times 1} \\
&= \frac{26!}{(26-2p)!} \cdot \frac{1}{(2p) \times (2p-2) \times (2p-4) \times \cdots \times 2} \\
&= \frac{26!}{(26-2p)!} \cdot \frac{1}{2^p\, p!}
\end{aligned}$$

Since the operator could choose to use any number p of plugs from $0 \leq p \leq 13$, the total number of possible plugboard combinations was

$$\sum_{p=0}^{13} \frac{26!}{(26-2p)!} \cdot \frac{1}{2^p \, p!} = 532,985,208,200,576.$$

Ordered rotors

The second variable component was the three ordered (left to right) rotors which wired twenty-six input contact points to twenty-six output contact points positioned on alternate faces of a disc. There are of course 26! unique discs which could have been constructed. Of those 26! any one of them could have been selected 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

$$\begin{aligned} &26! \times (26! - 1) \times (26! - 2) \\ &\quad = 65,592,937,459,144,468,297,405,473,480,371,753,615,896, \\ &\qquad\qquad 841,298,988,710,328,553,805,190,043,271,168,000,000. \end{aligned}$$

Serrations

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

Moveable ring

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. 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 $26 \times 26 = 676$ keystrokes. Since there were no more rotors, the leftmost rotor's notch had absolutely no effect whatsoever.

Reflector

The fifth variable component of Enigma was the reflector. The reflector had twenty-six contact points like a rotor, but only on one face. Thirteen wires internally connected the twenty-six 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 twenty-five different contact points to which it could be connected. Thus the first wire consumed two contact points and had twenty-five different possibilities. The second wire also consumed two contact points, and had only twenty-three different connection possibilities remaining from the unconsumed contact points. The third wire consumed two more contact points and had twenty-one possibilities for connection. The number of distinct reflectors which could have been placed into Enigma was

$$25 \times 23 \times 21 \times \cdots \times 1 = \frac{26!}{2^{13} 13!} = 7,905,853,580,625.$$

Total number of possible settings

By the multiplication principle, the number of theoretical possible Enigma configurations is the product of these five numbers, which is

$$\begin{aligned}&3{,}283, 883, 513, 796, 974, 198, 700, 882, 069, 882, 752, 878, 379,\\ &\qquad 955, 261, 095, 623, 685, 444, 055, 315, 226, 006, 433, 615, 627,\\ &\qquad\qquad 409, 666, 933, 182, 371, 154, 802, 769, 920, 000, 000, 000\\ &\approx 3 \times 10^{114}.\end{aligned}$$

Number of possible settings used in practice

It is worth noting that the German cryptographers did not use the Enigma machine to its fullest potential. At a number of steps, decisions were made which drastically reduced the number of possible combinations. Allied cryptographers therefore did not face quite the daunting odds first imagined.

In step 1, the most common number of plugboard cables used was 10. Since the number of cables was known, all that needed to be determined on a daily basis was which twenty letters had a cable patch inserted and the ten pairs created by those twenty letters. We find that for $p = 10$,

$$\frac{26!}{(26-2p)!} \cdot \frac{1}{2^p \, p!} = \frac{26!}{(26-20)!} \cdot \frac{1}{2^{10} \, 10!} = 150, 738, 274, 937, 250.$$

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. Since the rotor discs were hardwired, such a vast number would have been impossible to construct in practice. Indeed, only a very small handful of rotor discs was 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.) Later, two additional rotor discs were introduced, making a total of five. 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 ten 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 $5 \times 4 \times 3 = 60$ 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 (still) $26^3 = 17, 576$ 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.) As before, this is $26^2 = 676$.

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.

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, or

$$107, 458, 687, 327, 250, 619, 360, 000 \approx 10^{23}.$$