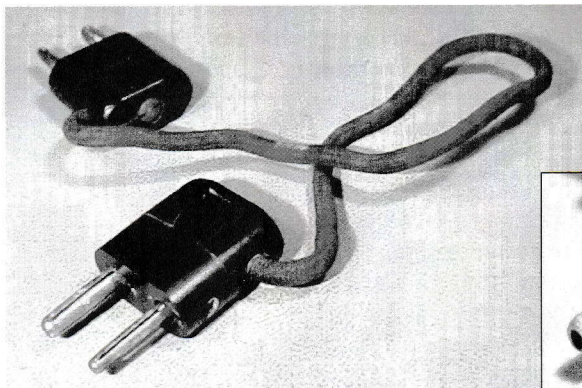




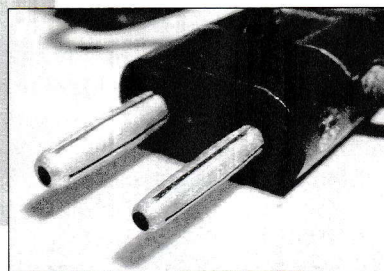
6.3 The Steckerbrett

The army variants of the Enigma (A, M3 and M4) were enhanced with a Steckerbrett (*plug board* or *patch panel*) that would allow any pair of letters to be swapped. If a patch cable was used between **G** and **P**, those two letters would be swapped. In other words: **G** would become **P** and **P** would become **G**. As the Steckerbrett is connected between the keyboard and the ETW, the encoded letter will go through stecker mappings twice. This would prevent a letter from being encoded into itself, which can be regarded as one of the weaknesses of the system. Nevertheless, the addition of the Steckerbrett greatly increased the number of possible permutations of the Enigma machine, making it much more secure than the commercial models.



A real Enigma cable in close-up

These pictures show a single patch cable of a real Enigma machine. To prevent a plug from being inserted the wrong way around, a thick and a thin pin were used. Two wires were used to cross-connect the pins of both plugs.



If no cable was used, the letter was known to be *Self-Steckered*. The diagram on page 38 shows how a contact in the socket is closed when the plug is removed.

As we have 26 characters, a theoretical maximum of 13 cables could be used. Note that any number of cables can be used, from none to 13, giving a much increased number of possible permutations. Most machines however, were supplied with only 11 cables. The reason for this is probably that the maximum number of permutations is reached when using 11 cables. Using more than 11 cables reduces, strangely enough, the maximum number of combinations. In order to understand this, we'll take a look at the mathematics behind the Steckerbrett. When using **n** cables, the maximum number of combinations is:

$$P = \frac{26!}{n! \cdot (26 - 2n)! \cdot 2^n}$$

The results are given in the table below.

Number of cables (n)	Combinations
0	1
1	325
2	44,850
3	3,453,450
4	164,038,875
5	5,019,589,575
6	100,391,791,500
7	1,305,093,290,000
8	10,767,019,640,000
9	53,835,098,190,000
10	150,738,274,900,000
11	205,552,193,100,000
12	102,776,096,500,000
13	7,905,853,580,550
0-13 cables	532,985,208,119,326

Source: Arthur O. Bauer

As you can see here, the maximum number of permutations is obtained when using 11 cables. In practice, the procedure was such that they would always use between 7 and 11 cables. According to the table this would mean a maximum number of combinations of:

422,197,679,120,000

This number has to be multiplied by the number of possible wheel orders and settings. For a Heeres Enigma (using 3 wheels from a set of 5), this number has to be multiplied by 60 (Walzenlage) x 17,576 (Grundstellung), which results in:

445,232,784,600,000,000,000

For a U-boat M4, using 3 extra wheels and two thin wheels, this would be:

129,651,786,900,000,000,000,000