Enigma – function and decryption

Seminar paper

Torben Tietgen
Informatik
100528
7. Fachsemester
7. Verwaltungssemester
2/16/2017

Table of contend

1 Historical context

Bevor Enigma and similar machines cryptographic was made by hand, which is slow and error-prone.

Since the early 1920s Enigma was used as commercial cryptographic system. At first the militaries had no interest in Enigma. After publications about decryption in WW1 Germany militaries changed their mind.

2 Construction

Enigma is an electro-mechanical rotor cipher machines. It consists of 3, later 4, slots for rotors, a reflector, a plugboard with 26 sockets, a keyboard and a lampboard. The plug-, key- and lampboard had a German typewriter layout.

2.1 Rotors

At first Enigma comes with 3 different rotors, later more models were added, for a total of 5 and later 8. Each rotor realized a simple substitution cipher by wires connecting pins with contacts. The connections differ for each model. A notch is attached to the rotors to determine the turnover of the next on. The operator can read the current position by the alphabetic ring on the outside. To set the position they have a hand-wheel.

2.2 Reflector

The Reflector returns the current flow back in the rotors and does not rotate. The 26 pins are connected in pairs. Four models were available but mostly model B was used. The Reflector was added with the goal to make encryption and decryption the same operation.

2.3 Plugboard

The plugboard realizes a one to one substitution. It has 26 sockets and was usually used with 10 cables to connect the sockets in pairs.

3 Function

Each keypress rotates the right rotor and the notch on it eventually the next one. The current flows through the pressed button to the plugboard, where it will pass eventually a cable. After that it flows through the rotors and passes the reflector, which returns it to the rotors and the plugboard. Finally a lamp will glow and indicates the corresponding letter.

4 Key

The cryptographic key of the Enigma, the setting, is the combination of:

- rotor order
  which rotors where selected for each slot
- ring settings
  the rotation of the alphabetic ring relative to the wiring
- plug connections
  the connected socket on the plugboard
- starting position of the rotors

To decrypt a message successfully the receiver has to set his Enigma the same way the sander had done to encrypt it.

4.1 Key space

To determinate the strange of the encryption the key space is the relevant information. The key space is the number of possible combinations of the settings:

- rotors: 3 out of 5
  5 * 4 * 3 = 60
- ring positions: 26 for the first two
  $26^2 = 676$
- cycle length: 26 per rotor (minus “kick”)
  26 * 25 * 26 = 16 900
- plugboard: 10 cables in 26 sockets
  $$\frac{26!}{2^{10} * 10! * (26 - 2 * 10)!} = 150\,738\,274\,937\,250$$

In combination:

60 * 676 * 16 900 * 150 738 274 937 250
= 103 325 660 891 587 134 000 000

This equals a 76 bit key, for comparison AES128 and other modern cryptographically functions has 128.

5 Decryption

The first ones who had successfully broken the Enigma were the polish. They hat a commercial version of Enigma which uses other rotors then the military version. They also got copies of manuals and 2 month of daily keys thanks to the work of a French spy. Marian Rejewski, a polish mathematician, deduced the wiring of the rotors and the reflector of the military Enigma with the use of permutation theory. After that success they know the full logical structure and were able to build replica of Enigma.

5.1 Characteristics method

At this time the Germans used just three rotors. The key for a given day was taken from a code book. For each day the rotor order, the ring setting and the plugs were given. The starting positions of the rotors, the message key, were chosen by operator. To tell the sender the message key he had to double the letters, encrypt it and send the six letters as first part of the communication. Let's say one chooses "DHI" so after doubling it, it would be "DHIDHI" and encrypted maybe "XHJKLM". So the "D" was encrypted to "X" and "K", "H" to "H" and "L" and "I" to "J" and "M".

With enough collected messages the polishes were able to construct so called *characteristics* for a given message key. They created a code book with all *characteristic.* With this information there were able to compute the message key of intercepted messages.

This method worked till 1 May 1937 when the German navy started using special code books. On 15 September 1938 the army and air force changed the way the setting for Enigma were chosen. Operators were then required to choose their own initial rotor position for the encryption of the message key for each message.

5.2 Bomba

The army and air force keep the practice of encrypting the message key twice, but now collection big numbers of messages did not revile the characteristics anymore.

After the characteristics method no longer works, Rejewski invented the bomba. The bomba is an electro-mechanical device. Each of them contains six sets of Enigma rotors, one for each letter in encrypted message key. The bomba uses females, one letter of the message key encrypted both times to the same letter. The occurrence of females in an intercepted message key caused an information leak. The bomba automated the process in finding settings in which the found female occurred.

In January 1934 Germany withdrew from the German-Polish Non-Aggression Pact. The Polish handed the information to the British and France. The British worked out sheets for every 60 rotor combinations. The sheets stopped working after the Germans change the way the message keys were transmitted.

5.3 Cribs

The British, one of them were Alan Turing, wanted an attacked which didn't rely on the way Enigma were used.

They used so called *cribs*. A *crib* is any known plaintext or suspected plaintext at some point in an encrypted message. Because of the reflector a letter can never encrypt to itself. So there are only a few positions in which the plaintext can be in the message.

With lots of practice, skill and experience it is possible to determine the key which was used to encrypt the message and to decrypt it back in plaintext. This is brute force method and often takes a long time to be successful.

5.4 Bombe

September 1939 Alan Turing designed the bombe, an electro-mechanical device emulating several Enigma machines wired together. The bombe were used to automate the process of finding promising wheel orders, initial positions of the rotors, plugs and crib positions. The final investigation must still be made by experienced cryptanalysts, but the time to decrypt messages was reduced drastically.

Thanks to the bombe the British were able to decrypt mostly every message send by the Germans. The only exception was the German navy which used a special Enigma with more rotors and special rules for the use of it.

6 Sources

Smart , Nigel P.: "Cryptography Made Simple" ISBN: 978-3-319-21935-6

https://de.wikipedia.org/wiki/Enigma_(Maschine)
https://en.wikipedia.org/wiki/Enigma_machine
https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma