MTAT.07.006 Research Seminar in Cryptography

The Enigma Cipher Machine

Kadri Hendla
University of Tartu
kadri_h@ut.ee

Overview

- Description of Enigma
- Enigma in Use
- Cryptanalysis of Enigma

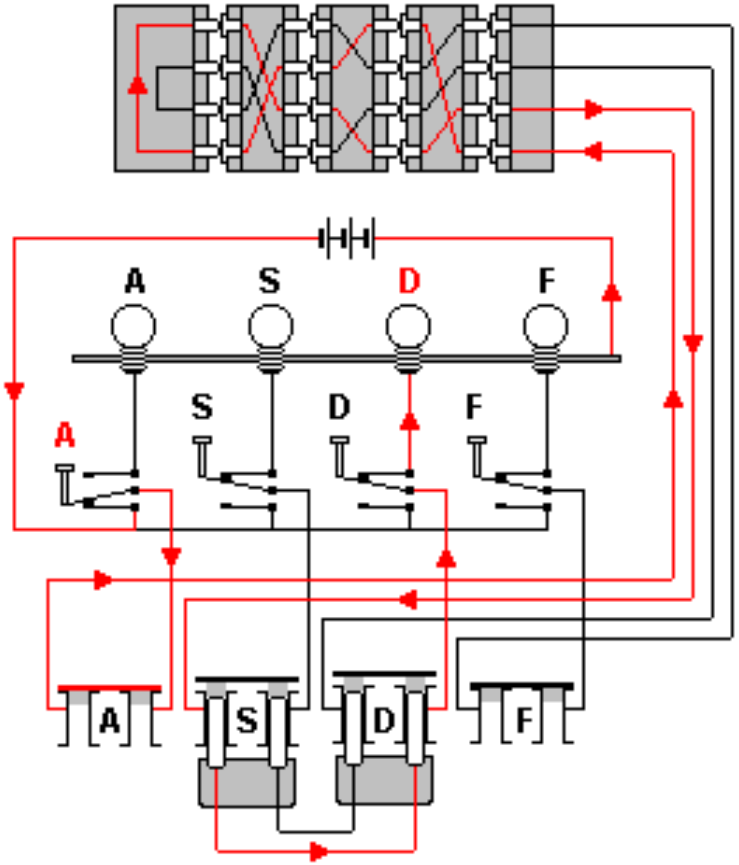
History of Enigma

- Enigma is most known for its part in World War II.
- In 1918 Arthur Scherbius applied for a patent for Enigma.
- German military adopted Enigma in 1926.
- There were many different versions of Enigma.

The Enigma Machine

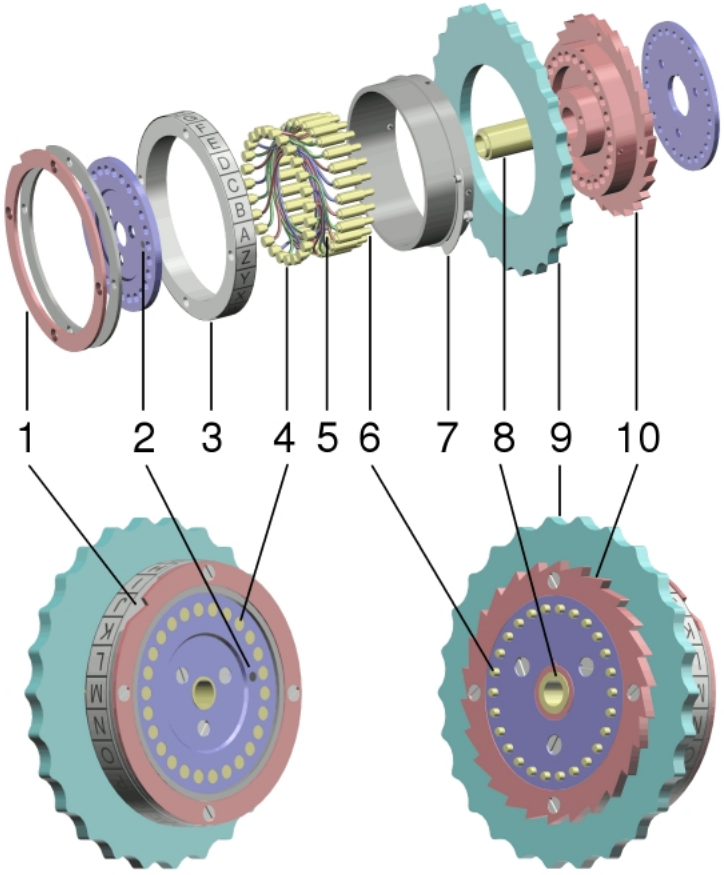
Description of Enigma: Working Principle

- Scrambler (3 rotors and a reflector)
- Lamps
- Keyboard
- Plugboard



Description of Enigma: Rotors

- 1. notched ring
- 2. marking dot for ”A” contact
- 3. alphabet ring
- 4. plate contacts
- 5. wire connections
- 6. pin contacts
- 7. spring-loaded ring adjusting lever
- 8. hub
- 9. finger wheel
- 10. ratchet wheel



Description of Enigma: Reflector

The reflector gave two important properties to Enigma:

- Encryption was the same as decryption.
- No letter could be encrypted to itself.

Enigma in Use: Cryptographic Key

Enigma cryptographic key is made up of the following parts:

- The rotor order (and selection)
- The initial position of the rotors
- The plugboard connections
- The alphabet ring settings

Enigma in Use: Indicator procedures

- Some of these settings were written in codebooks, for example:
  - ⋆ Choice and order of rotors
  - ⋆ Plugboard settings
  - ⋆ Ring settings
- Starting position was (pseudo-)randomly chosen by the Enigma operator

Enigma in Use: Indicator procedure 1

The operator

- sets up his machine according to the codebook.
- chooses his random starting position, for example GKL.
- encrypts GKL twice using the global starting position (given in a code-book).
- turns the rotors to GKL and encrypts the actual message.
- transmits the encrypted starting position and message.

Enigma in Use: Indicator procedure 1

The receiving operator:

- sets up his machine according to the codebook.
- decrypts first six letters of the ciphertext.
- sets the rotors to the indicated position.
- decrypts the rest of the message.

Enigma in Use: Indicator procedure 1

This procedure was not very secure:

- The use of a global ground setting is a bad idea. This way all the messages start from the different positions of the same machine cycle. This was changed later.

- The repetition of message key results in relation between the letters. For example, if the encrypted message key is JXDRFT, then it is known that

  ⋆ J and R (the 1,4 pair) were originally the same letter,

  ⋆ X and F (the 2,5 pair) were originally the same letter,

  ⋆ D and T (the 3,6 pair) were originally the same letter.

Enigma in Use: Indicator procedure 2

The operator:

- sets up his machine according to the codebook. Now the codebook contains information only about rotor and ring settings.
- chooses a random starting position, for example WZA.
- chooses a random message key, for example SXT.
- turns the rotors to WZA, encrypts SXT and gets, for example, UHL.

Enigma in Use: Indicator procedure 2

- turns the rotors to SXT and encrypts the rest of the message.
- transmits WZA (in the plain), UHL and the encrypted message.

Enigma in Use: Indicator procedure 2

The receiving operator:

- sets up his machine according to the codebook.
- turns the rotors to WZA, decrypts UHL and gets, SXT.
- turns the rotors to SXT and decrypts the rest of the message.

Enigma in Use: The Real World

- Enigma could have been unbreakable, but its use in practice was often careless and gave the codebreakers many valuable clues.
- The operators were lazy or untrained and chose easy message settings.
- Routine messages were sent out day after day at about the same time, from the same place, of the same length and starting in exactly the same way.

Cryptanalysis of Enigma

- Breaking of Enigma before World War II by the Poles
- Breaking of Enigma during World War II by the British
- Breaking of Naval Enigma

Cryptanalysis of Enigma: Pre-World War II

- In 1928, the German Army began using their enhanced Enigma.
- The Poles had the commercial version of Enigma.
- They managed to figure out the internal wiring of rotors.
- Now all they needed were the daily machine configurations.

Cryptanalysis of Enigma: Chains

- In 1932, Polish mathematician Marian Rejewski figured out the indicator procedure and noticed the relation between the letters of the twice encrypted message settings.

- It was possible to find *chains* of how those identical letters changed.

AXP AVC	IOV NKZ	HSA PYT	PPZ LEX
FZD YQO	IZL NQL	NNQ CMA	GUH BIS
FGT YHD	KDY GNV	NBJ COQ	GOI BKK
MIW MRI	VWG EZG	SYX SJB	TVB KFM
DJG UDG	OJN QDE	SNH SMS	TLI KPK
LNK TMF	ZAO RXJ	SXV SVZ	TYO KJJ
XKN JAE	CTL OUL	ERS XWU	WHJ WBQ
BHG DBG	CMM OTY	EAA XXT	JQR ISH
RZU ZQN	UKM HAY	YCE FGR	JEY ICV
RTC ZUW	QFF VLP	PII LRK	JCE IGP

Cryptanalysis of Enigma: Cyclometer

- In 1934, Rejewski invented *cyclometer* for preparing a card catalog of the length and number of chains for all positions of the rotors.
- Using the catalog, a daily key could be found in about 15 minutes.
- In 1937, the Germans changed the reflector wirings and the Poles had to build a new catalog.
- In 1938, the Germans stopped using the global message keys and this method turned useless. Luckily, they still transmitted encrypted message keys twice.

Cryptanalysis of Enigma: Pre-World War II

- An important observation was that sometimes the (1,4), (2,5), (3,6) pairs were identical, for example PST PWA.
- The occurrence of those pairs depended on the wheel order and the start position.
- If enough such pairs occurred during one day, then it was possible to find a unique configuration for which all those doubles could occur.
- Another Polish cryptanalyst, Henryk Zygalski, invented a method for it, known as ”Zygalski sheets” or ”perforated sheets”.

Cryptanalysis of Enigma: Zygalski sheets

- This method involved laying a series of perforated sheets over one another.
- The sheets had 26 rows and columns The rows represented the position of the middle rotor, the columns the position of the rightmost rotor. There was one such sheet for every position of the left rotor.
- If an identical pair was possible at that position, a hole would be cut into the sheet.
- When the sheets were laid over one another and a light shone through in one place, a possible key had been found.

Cryptanalysis of Enigma: The Polish *Bomby*

- For testing all those possible keys automatically, Rejewski invented a machine called *bomba*.
- It consisted of three Enigma scramblers, placed one machine cycle apart and driven by a motor.
- The *bomba* had separate terminals for input and output letters.
- The machine stepped through all the cycles until a match was found and then stopped.
- 6 *bomby* were required for each test run.

Cryptanalysis of Enigma: Pre-World War II - Conclusion

- In 1939, the Germans stopped transmitting the twice encrypted message keys.
- The Poles contracted military alliance with the British and the French and shared their work on Enigma.
- After the German invasion, the Polish cryptanalysts fled the country; some of them later ended up in Britain. Strangely enough, they were not invited to work on Enigma at Bletchley Park.

Cryptanalysis of Enigma: World War II

- The British now knew techniques for breaking Enigma, but the Germans had increased their security.
- They had added two rotors to Enigma, three of which would be used at one time.
- The Polish methods didn't work anymore.
- Alan Turing designed the British *bombe*.

Cryptanalysis of Enigma: The Turing Bombe

- The bombe relied on *cribs* - known plaintext-ciphertext fragments.
- The bombe consisted of sets of rotors, wired up according to a *menu* prepared by the codebreakers.
- The rotors stepped through all possible rotor settings. At each position a test would be conducted and if it failed, that setting could be ruled out.
- The test worked by making deductions from cribs. What made it harder was the use of a plugboard.

Cryptanalysis of Enigma: The Turing Bombe

- Lets denote the scrambler starting position by S_1 and the next position by S_2 and so on.
- We also denote the plugboard transformation by P.
- $P(P(x)) = x$
- Turing noticed that, even though the values for $P(A)$ or $P(W)$ were unknown, the crib still provided known relationships amongst these values.

Cryptanalysis of Enigma: Breaking of Naval Enigma

- The Navy variant of Enigma was much more secure.
- It used lot more rotors and the indicator procedures were more secure.
- Starting form 1937, the Navy used an entirely different coding system that involved using bigram and trigram substitutions.

Cryptanalysis of Enigma: The Navy Indicator Procedure

The operator:

- chooses a trigram from a codebook.
- encrypts it at ground settings.
- turns it into a bigram with the help of bigram tables.
- encrypts the message using this trigram.
- transmits this in the message header.

Cryptanalysis of Enigma: The Navy Indicator Procedure

The receiving operator:

- looks this bigram up from his bigram tables.
- turns it back into trigrams.
- decrypts those trigrams at ground settings.
- decrypts the message using the acquired message key.

Cryptanalysis of Enigma: Breaking of Naval Enigma

- In 1937 the Poles had managed to decrypt some Navy messages due to a fortunate incident.
- They didn't manage to work out the indicator procedure, but in 1939, Alan Turing did it, using the information from the Poles.
- He, along with Peter Twinn, started decrypting older messages that were encrypted using only 6 plugs on the plugboard.
- The EINS catalog
- Capture of *Polares* enabled them to partially reconstruct the bigram tables.

Cryptanalysis of Enigma: Banburismus

- They developed a method called Banburismus that worked on encrypted message keys.
- Banburismus required that the indicators had been encrypted using the same message settings.
- The idea of Banburismus is to guess the plaintext corresponding to those indicators by the statistical analysis of the messages.
- Two messages whose indicators differed only in the third character (for example VFG and VFX) were punched onto thin cards (banburies) and slid over each other.

Cryptanalysis of Enigma: Banburismus

- At each offset, number of overlapping holes were counted.
- Message with indicator *VFG*:
  GXCYBGDSLVWBDJLKWIPEHVYGQZWDTHRQXIKEESQSSPZXARIXEABQIRUCKHGWU
- Message with indicator *VFX*:
  NSCFCCPVIPEMSGIZWFLHESCIYSPVRXMCFQAXVXDVUQILBJUABNLKMKDJMENUNQ

```
GXCYBGDSLVWBDJLKWIPEHVYGQZWDTHRQXIKEESQSSPZXARIXEABQIRUCKHGWUEBPF
          YNSCFCCPVIPEMSGIZWFLHESCIYSPVRXMCFQAXVXDVUQILBJUABNLKMKDJMENUNQ
                          - --  -   -          -  -   --
```

Cryptanalysis of Enigma: Banburismus

- It was possible that if there was a large number of the same cipher letters at some offset, then there was the same offset between the rightmost rotor start letters.
- The principle was that the plaintext of *VFX* is 9 characters ahead of *VFG*, or that $X = G + 9$.
- This way, a chain of letters could be constructed, that could then be tried over a letter sequence of an Enigma rotor, for example G - - B - H - - - X - Q.
- Hopefully, some of those positions could then be ruled out.

Cryptanalysis of Enigma: Banburismus

- This position violates the ”self-reciprocal” property of Enigma. Letter G enciphers to B, but B enciphers to E.

  .. G ... ... B ... H ... ... X ... Q

  A B C D E F G H I J K L M N O P Q

- This position violates the ”no-self-ciphering” property of Enigma. Letter H apparently enciphers to H.

  ... .. G ... ... B ... H ... ... X ... Q

  A B C D E F G H I J K L M N O P Q

- When other, different chains are laid over the remaining possibilities, choices can be further narrowed and the rightmost rotor used can be determined.

Conclusion

- By 1945, almost all German Enigma traffic could be decrypted within a day or two.
- The Germans were still confident of its security and openly discussed their plans and movements.
- After the war it was learnt that the German cryptographers were aware that Enigma was not unbreakable, they just couldn't fathom that anyone would go to such lengths to do it.