Cryptography: Mechanical Rotor Ciphers

Alex Corner

Sheffield Hallam University

The Story So Far

- The Caesar cipher is far too limited.
- The monoalphabetic general substitution cipher has an enormous amount of keys, but are easily cracked by frequency analysis.
- The Vigenère cipher is polyalphabetic, but as we've just seen is vulnerable to frequency analysis when we know the key length.
- Something else was needed.

Origins of Enigma

- In 1917, Edward Hugh Hebern designed a rotor cipher machine, the first of its kind. A prototype was made in 1918, but sales didn't really get off the ground.
- In 1919, Hugo Alexander Koch patented designs for a rotor cipher machine, but did nothing with them. He assigned the patent rights to Arthur Scherbius in 1927.

Origins of Enigma

- Scherbius had already developed his own cipher machine designs by this point and his first **Enigma machines** (patented 1918) were commercially available from 1923, primarily for financial and diplomatic purposes. Sales didn't really get off the ground.
- Then Hitler rose to power and Germany started re-arming itself. Enigma machines were suddenly in demand.
- Many countries developed their own rotor cipher machines which proved especially lucrative if one was savvy enough to relocate their business to the neutral country of Switzerland. (See Crypto AG.)

The Enigma Machine

- From 1926 the German Navy began to use a military version of Enigma to encrypt messages, with the German Army following suit in 1928, followed by the Luftwaffe.
- About 40,000 machines were used by the Nazis in World War II (1939 - 1945).
- Again, it was thought to be unbreakable.

The Enigma Machine

- The Enigma machine utilised many different mechanical components, to create an intricate cipher.
- When a plaintext letter was typed, an electrical current would set off a scrambling system, so that a different ciphertext letter was illuminated on the lampboard.

Sending Messages

- An operator would set up the machine each day with that day's secret setting.
- As each letter was encrypted, the operator would write it down.
- When the complete message was encrypted, it was transmitted by radio.
- It was believed that any intercepted messages would be indecipherable.

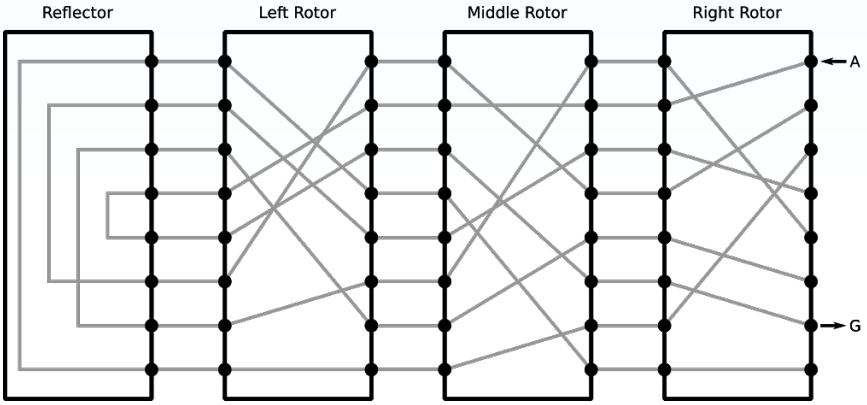
Receiving Messages

- An operator would set up the machine each day with that day's secret setting - the same settings as the operator that sent the message.
- Each ciphertext letter was typed in and would light up the plaintext equivalent on the lampboard.
- This is an example of a **symmetric cipher**, since exactly the same method, using the same key, encrypts and decrypts the messages.

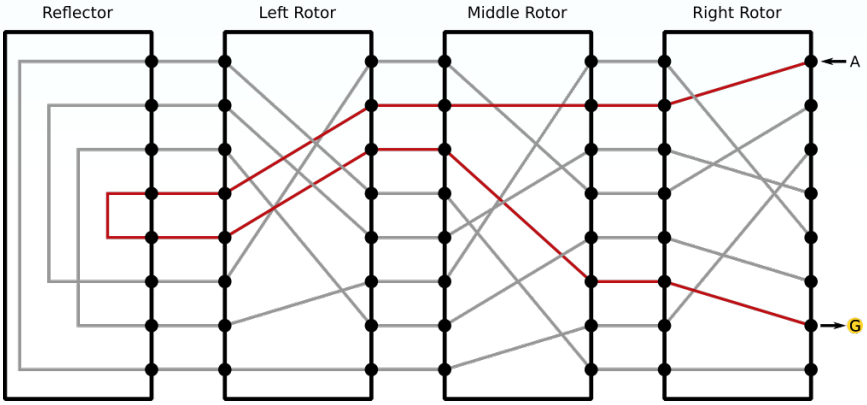
The Enigma Machine

- The design had:
  - A plugboard;
  - Three rotors, chosen from five options, each with different internal wirings;
  - A reflector.
- Each rotor is its own substitution cipher. But as each key was pressed, it 'stepped on', i.e., changed position.
- This produces a polyalphabetic cipher like the Vigenère cipher.
- The sequence passes through the three rotors and the reflector, before sending it back via a different route.

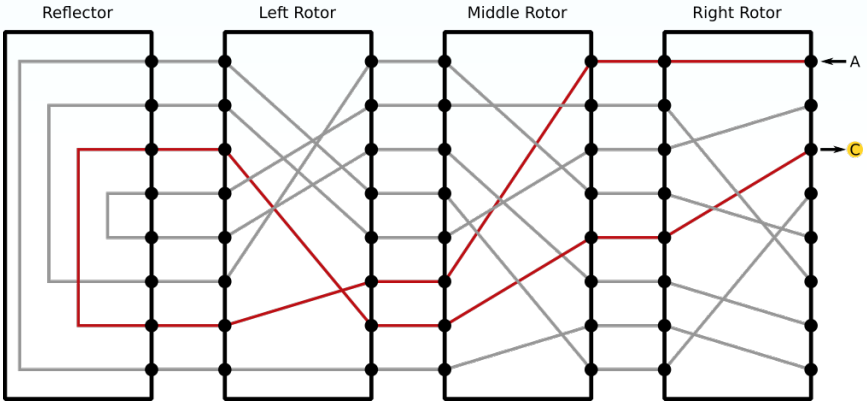
The Enigma Machine



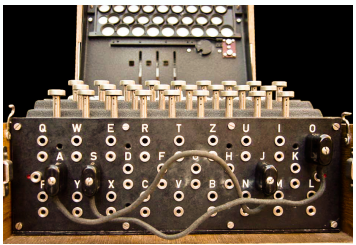
The Enigma Machine



The Enigma Machine



The Plugboard



- On the front of the machine was the **plugboard**, consisting of 26 plugs `A` – `Z`.
- One standard arrangement used 10 cables to connect pairs together on the plugboard.
- Each pair was then swapped before passing through the rest of the machine, and swapped again at the end.

The Enigma Machine

- The scrambling system made Enigma incredibly powerful as an enciphering scheme.
- For example, initially a `c` might be a `K`, but next time it might be a `P`. Each time it would be different.
- This apparent randomness made it difficult to crack because frequency analysis was not possible.
- The initial settings of the machine provided the key.

The Keys

- Every month a secret key sheet was distributed to show how the operators would set up the machine each day.
- Depending on the type of machine, the keyspace was huge. One version of Enigma had the following number of keys:

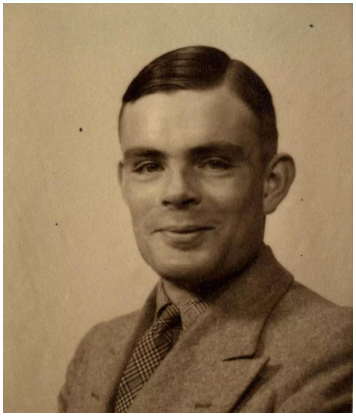
  $$753, 506, 019, 827, 465, 601, 628, 054, 269, 182, 006, 024, 455, 361, 232, 867, 996, 259,$$
  $$038, 139, 284, 671, 620, 842, 209, 198, 855, 035, 390, 656, 499, 576, 744, 406, 240, 169,$$
  $$347, 894, 791, 372, 800, 000, 000, 000, 000.$$

- This huge amount of keys is way more than sufficient to prevent any kind of brute force attack.

Cryptanalysis of Enigma

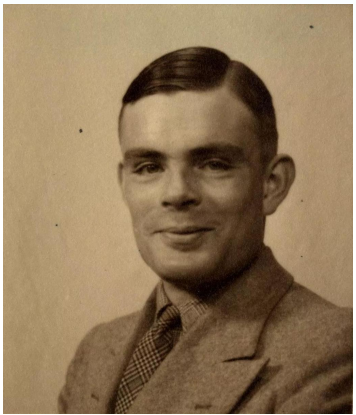
- A lot of people think the British were the first to break Enigma. But it was Polish mathematicians Marian Rejewski (R), Henryk Zygalski (M), and Jerzy Różycki (L).
- They had obtained a commercial Enigma machine and were able to decipher messages before the Second World War began.
- The commercial machine differed from the military machine in some crucial aspects, but these mathematicians were able to model the machine using mathematics from the area of 'group theory' in order to break the cipher.

Cryptanalysis of Enigma



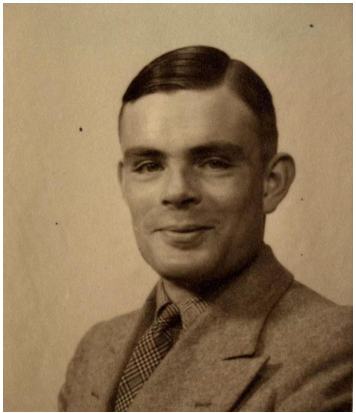
- But in September 1939 the Nazis invaded Poland. The Polish mathematicians fled to France before heading to England, where they had been passing on the keys that they had found.
- Work to break Enigma was based at Bletchley Park and the Poles weren't allowed to be involved any more.
- The man most famously associated with Enigma then got involved in the cryptanalysis efforts.
- Alan Turing (1912-1954): 'Before the war my work was in logic and my hobby was cryptanalysis and now it is the other way round.'

Cryptanalysis of Enigma



- Fundamentally, Enigma was broken through the use of 'cribs', improper use of keys by the Germans, and the subtle flaw that no letter could be encrypted as itself.
- Common cribs to look for were phrases such as 'Heil Hitler' or 'The weather today is forecast to be...'.
- Each message also started with the 'session key'. After setting the machine using the daily key, an operator would type a 'random' session key consisting of three letters (twice) - but this wasn't always done randomly.
- The machine was then reset to the session key and this was used.

Cryptanalysis of Enigma



- The recipient, with their machine set to the daily settings, would be able to decrypt the session key, and then continue in this fashion.
- But there was no reason to have typed the session key twice. Extra redundancy, but a weakness for anybody who knew what they were looking for. (The enemies knew the system, after all.)
- Even worse, the three letters for the session key were often not that random: part of a row or column from the keyboard, or even letters connected to a girlfriend's name. This lack of true randomness further hurt the security of the cipher.

The Advance of the Computer

- The development of computers in the 1950s changed cryptography forever.
- However some of the classical techniques were retained in the new designs: Substitution and Transposition.
- Together with these computer-aided ciphers could easily implement a new operation: XOR.
- All these were to be incorporated in the first worldwide standard: DES.