Cristina Nita-Rotaru

CS355: Cryptography

Lecture 4: Enigma.

Towards cryptographic engines

- How to move from pencil and paper to more automatic ways of encrypting and decrypting?
- How to design more secure ciphers
- Alberti's Disk
- Jefferson's Wheel
- Enigma

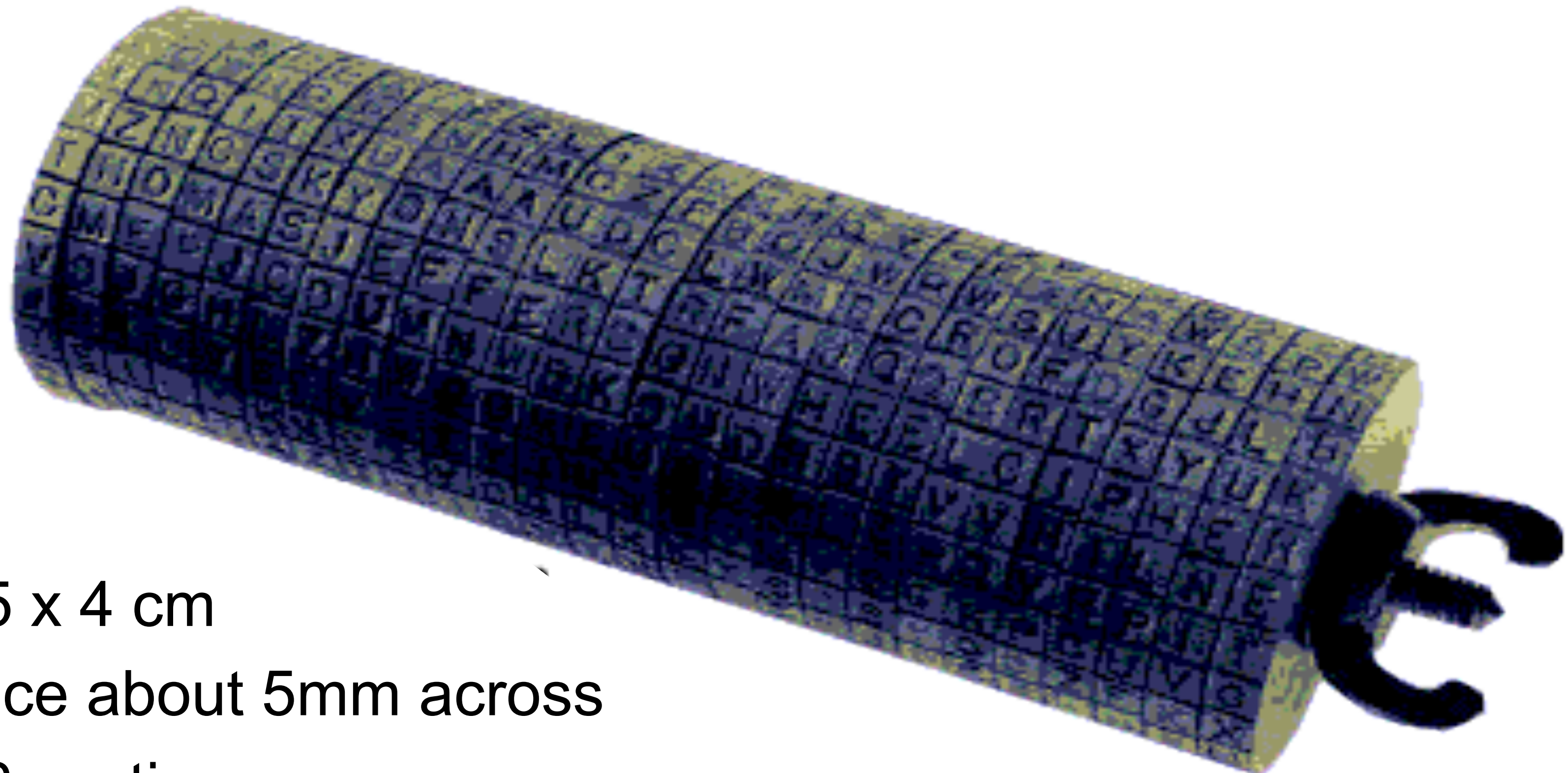
Alberti disk - 1467

- Outer is fixed
- Insider is mobile

Alberti disk

- The numbers on outer disks are used to code pre-determined passphrases
- Encode: on inner disk there is a mark which could be lined up with a letter on the outer disc as a key
- Decode:
  - Need to use a disk with a matching alphabet on the inner ring
  - Need to know the correct letter to match the mark to rotate the inner disk

Jefferson wheel cipher - 1790



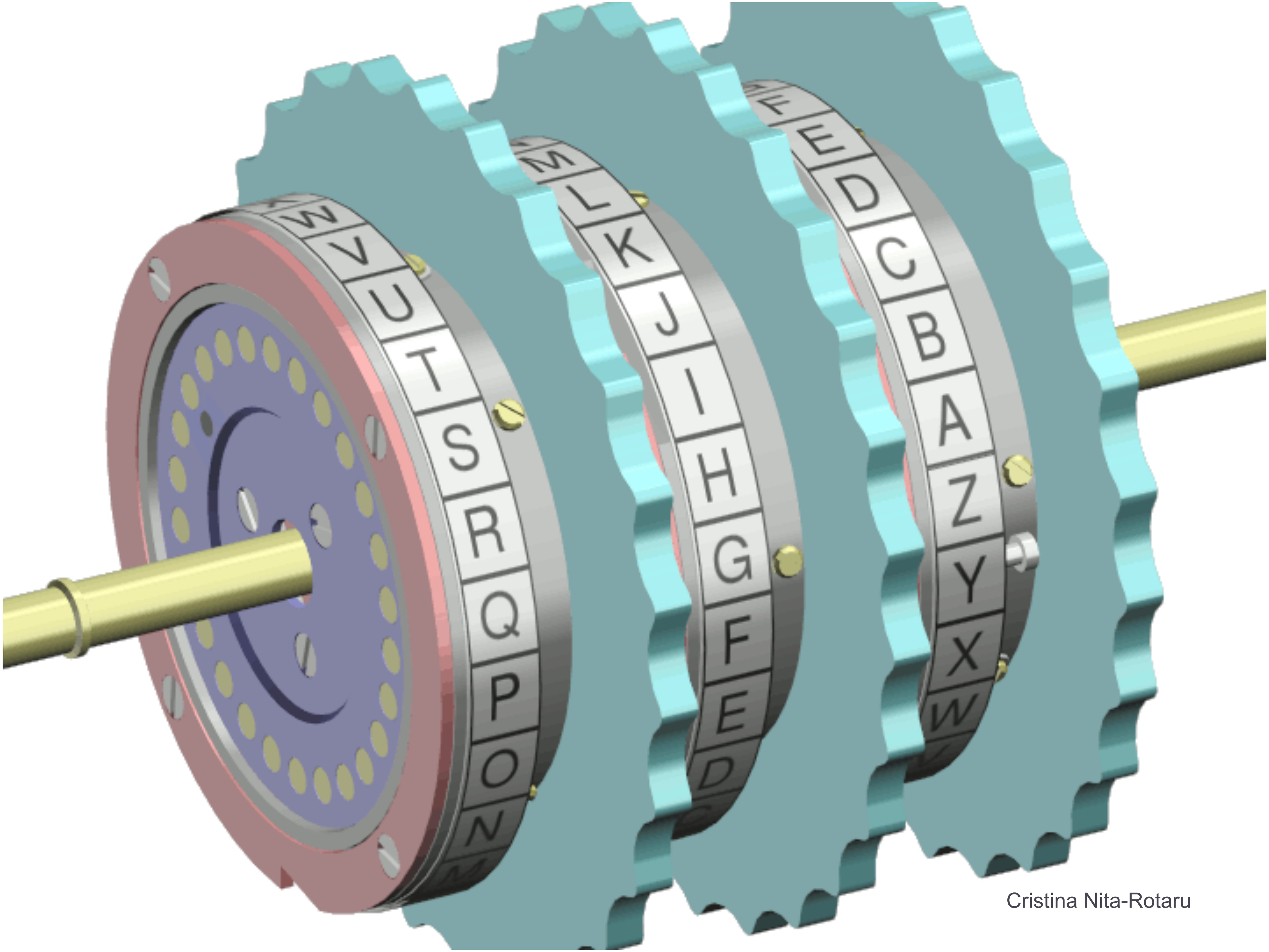
- 15 x 4 cm
- slice about 5mm across
- 26 sections
- one letter is assigned randomly to each section.

Jefferson cipher

- Encode: a fragment of the message appears along one side of the cylinder, the cylinder is then turned and another line is copied out at random
- Decode:
  - Use the cylinder to enter the ciphertext, and then turn the cylinder examining each row until the plaintext is seen.
  - Same cylinder must be used for both encryption and decryption

Rotor machines

- Vigenere can be broken once somebody finds the key length
- How to have a longer key?
- Idea:
  - Multiple rounds of substitution, encryption consists of mapping a letter many times
  - Mechanical/electrical wiring to automate the encryption/decryption process
- A machine consists of multiple cylinders (rotors) that map letters several times



Cristina Nita-Rotaru

Rotor machines

- Each rotor has 26 states (as many as the alphabet)
- At each state there is a substitution cipher: the wiring between the contacts implements a fixed substitution of letters
- Each cylinder rotates to change states according to a different schedule changing the substitution
- A m-cylinder rotor machine has 26^m different substitution ciphers
  - $26^3 = 17576$
  - $26^4 = 456{,}976$
  - $26^5 = 11{,}881{,}376$
- Most famous rotor machine is Enigma

History of the Enigma machine

- Patented by Scherius in 1918
- Widely used by the Germans from 1926 to the end of second world war
- First successfully broken by Polish in the thirties by exploiting the repetition of the message key and knowledge of the machine design (espionage)
- Then broken by the UK intelligence during the WW II

Enigma machine trivia

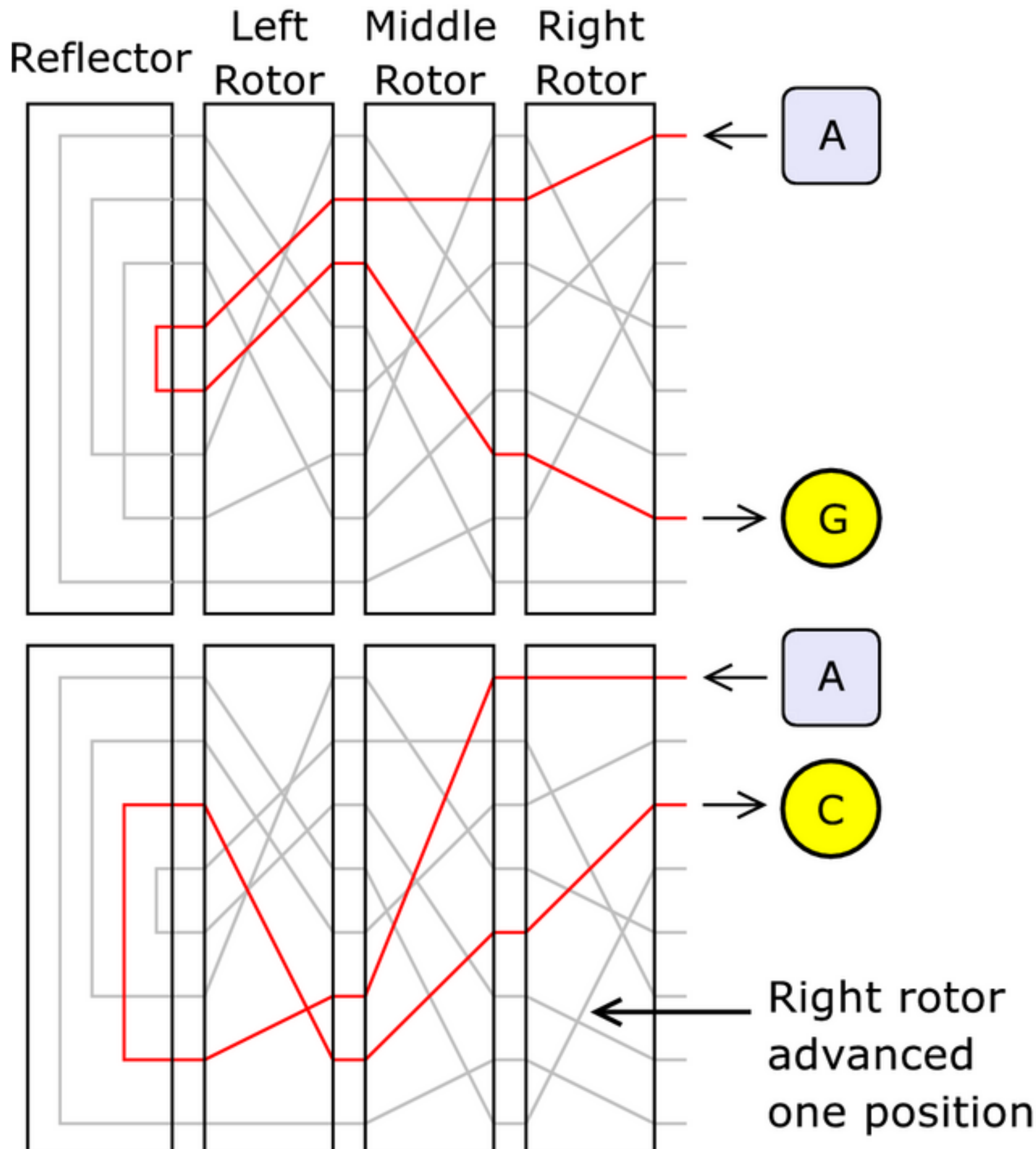
- Patented by Scherius in 1918
- Came on the market in 1923, weighted 50 kg (about 110 lbs), later cut down to 12kg (about 26 lbs)
- It cost about $30,000 in today's prices
- 34 x 28 x 15 cm

Enigma machine

- Plug board:
  - 6 pair of letters are swapped
- 3 scramblers (motors):
  - 3 scramblers can be used in any order:
- A reflector

A rotor rotates 1/6th after each map

Second rotor rotates after first had a complete revolution, and so on



Food for thought …

- What’s the purpose of the reflector????
- How would you design an Enigma without the reflector (would it be a better (more difficult to break) machine?)
- What type of cipher (encryption) does a rotor perform?
- What can you say about the result of encrypting the same letter consecutively

Enigma machine: Size of key space

- Use 3 scramblers (motors):
  17576 substitutions
- 3 scramblers can be used in any order: 6 combinations
- Plug board: allowed 6 pairs of letters to be swapped before the scramblers process started and after it ended.

$$100,391,791,500$$

- Total number of keys $\approx 10^{16}$
- Later versions of Enigma usec 5 rotors and 10 pairs of letters

Decryption

- Need the encrypted message, and know which rotors were used, the connections on the plug board and the initial settings of the rotors.
- Without the knowledge of the state of the machine when the original message was typed in, it is extremely difficult to decode a message.

Encrypting with Enigma

- **Daily key**: The settings for the rotors and plug boards changed daily according to a **codebook received by all operators**
- **Message key**: Each message was encrypted with a unique key defined by the position of the 3 rotors
- An encrypted message consists of the message key repeated twice and encrypted with the daily key, then the message encrypted with the message key

Using Enigma machine

- A day key has the form
  - Plugboard setting: A/L–P/R–T/D–B/W–K/F–O/Y
  - Scrambler arrangement: 2-3-1
  - Scrambler starting position: Q-C-W
- Sender and receiver set up the machine the same way for each message
- Message key: a new scrambler starting position, e.g., PGH

Using Enigma machine

- Several communication ``networks''
  - Each network had its own codebooks
  - Different types of enigma machines (rotors, plugboard) (naval could have up to 8 rotors, rotor was not fixed, could have also been configured)

Food for thought ...

- What type of cryptography is this? Symmetric or anti-symmetric?
- Why bother with the rotors when the enormous key space seems to be determined by the plugboard?
- What happens if the enemy got a codebook????

How to break the Enigma machine?

- Recover 3 secrets
  - Internal connections for the 3 rotors
  - Daily keys
  - Message keys
- Exploiting the repetition of message keys
  - In each ciphertext, letters in positions 1 & 4 are the same letter encrypted under the day key
  - With 2 months of day keys and Enigma usage instructions, the Polish mathematician Rejewski succeeded to reconstruct the internal wiring

How to recover the day key?

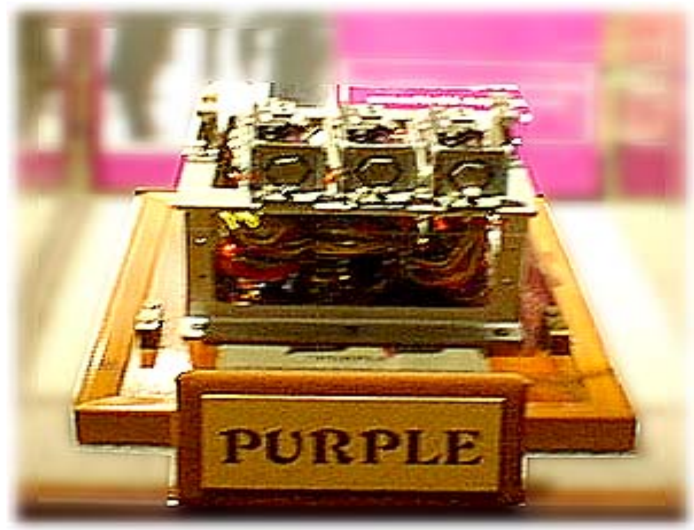
- Encryption can be mathematically expressed as a product of permutations
- Catalog of "characteristics"
  - Main idea: separating the effect of the plugboard setting from the starting position of rotors
  - Determine the rotor positions first
  - Attacking plugboard is easy
  - Plugboard does not affect chain lengths in the permutation
- Using known plaintext attack
  - Stereotypical structure of messages
  - Easy to predict standard reports
  - Retransmission of messages between multiple networks

Lessons learned from breaking Engima

- Keeping a machine (i.e., a cipher algorithm) secret does not help
  - The Kerckhoff's principle
  - Security through obscurity doesn't work
- Large number of keys are not sufficient
- Known plaintext attack was easy to mount
- Key management was the weakest link
- People were also the weakest link
- Never underestimate the opponent
- Even a strong cipher, when used incorrectly, can be broken

Japanese Purple machine

- Electromechanical stepping switch machine modeled after Enigma
- Used telephone stepping switches instead of rotors
- Pearl Harbor attack preparations encoded in Purple, decoded hours before attack



Alan Turing (1912 - 1954)

- English mathematician, logician and cryptographer
- Father of modern computer science
  - Concept of the algorithm
  - Computation with the Turing machine
  - Turing test: artificial intelligence: whether it will ever be possible to say that a machine is conscious and can think
- Worked at Bletchley Park, the UK's codebreaking centre; devised techniques for breaking german ciphers

Turing award

- Nobel Prize of computing
- The most prestigious award in Computer Science
- Since 1966
- Some of the winners were cryptographers
  - 2002 RSA inventors won the Turing award

  - Most recent winner
  - Judea Pearl: For fundamental contributions to artificial intelligence through the development of a calculus for probabilistic and causal reasoning

Take home lessons

- Although the Enigma cipher has cryptographic weaknesses, in practice the codebrakers were able to decipher message because of the combination with
  - mistakes by operators
  - procedural flaws
  - occasional captured machine or codebook