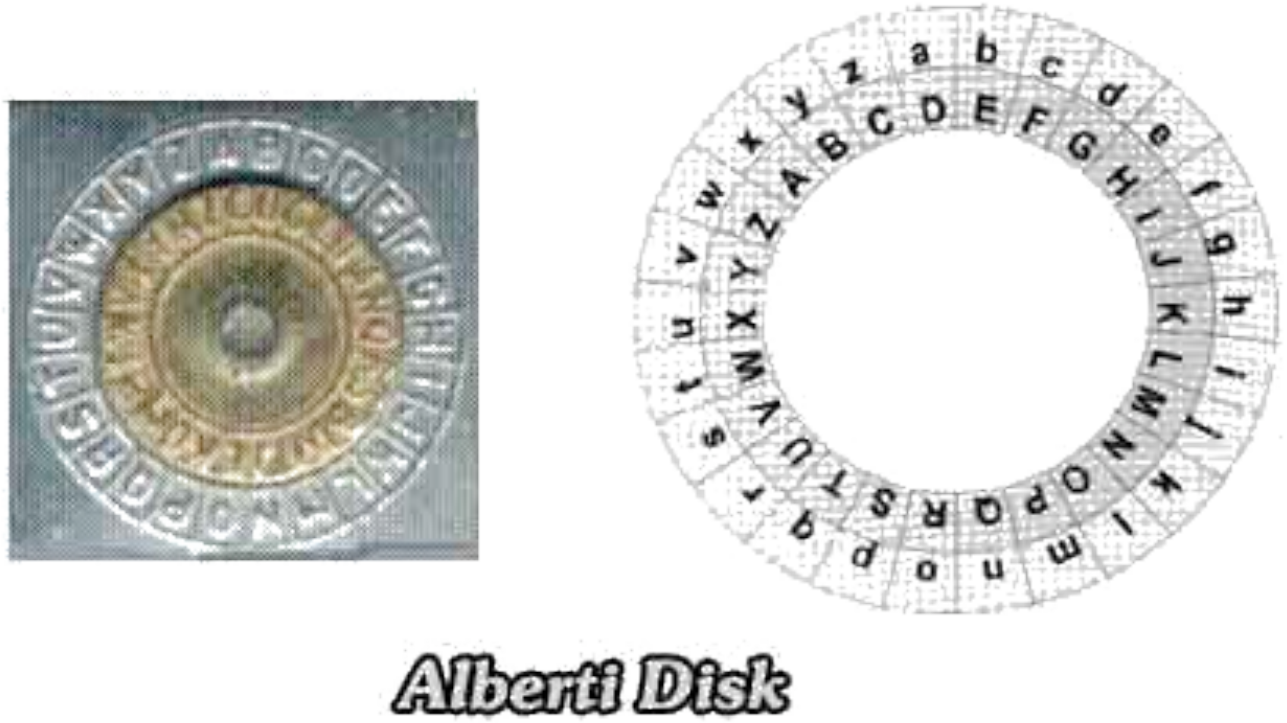
CS355: Cryptography

Lecture 5: Enigma Machine.

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

Alberti Disk

Picture courtesy of http://www.quantumlah.org/



Rotor Machines

- Basic idea: if the key in Vigenere cipher is very long, then the attacks won't work
- Implementation idea: multiple rounds of substitution
- A machine consists of multiple cylinders
  - each cylinder has 26 states, at each state it is a substitution cipher
  - each cylinder rotates to change states according to different schedule

Rotor Machines

- A m-cylinder rotor machine has
  - 26^m different substitution ciphers
    - $26^3 = 17576$
    - $26^4 = 456{,}976$
    - $26^5 = 11{,}881{,}376$

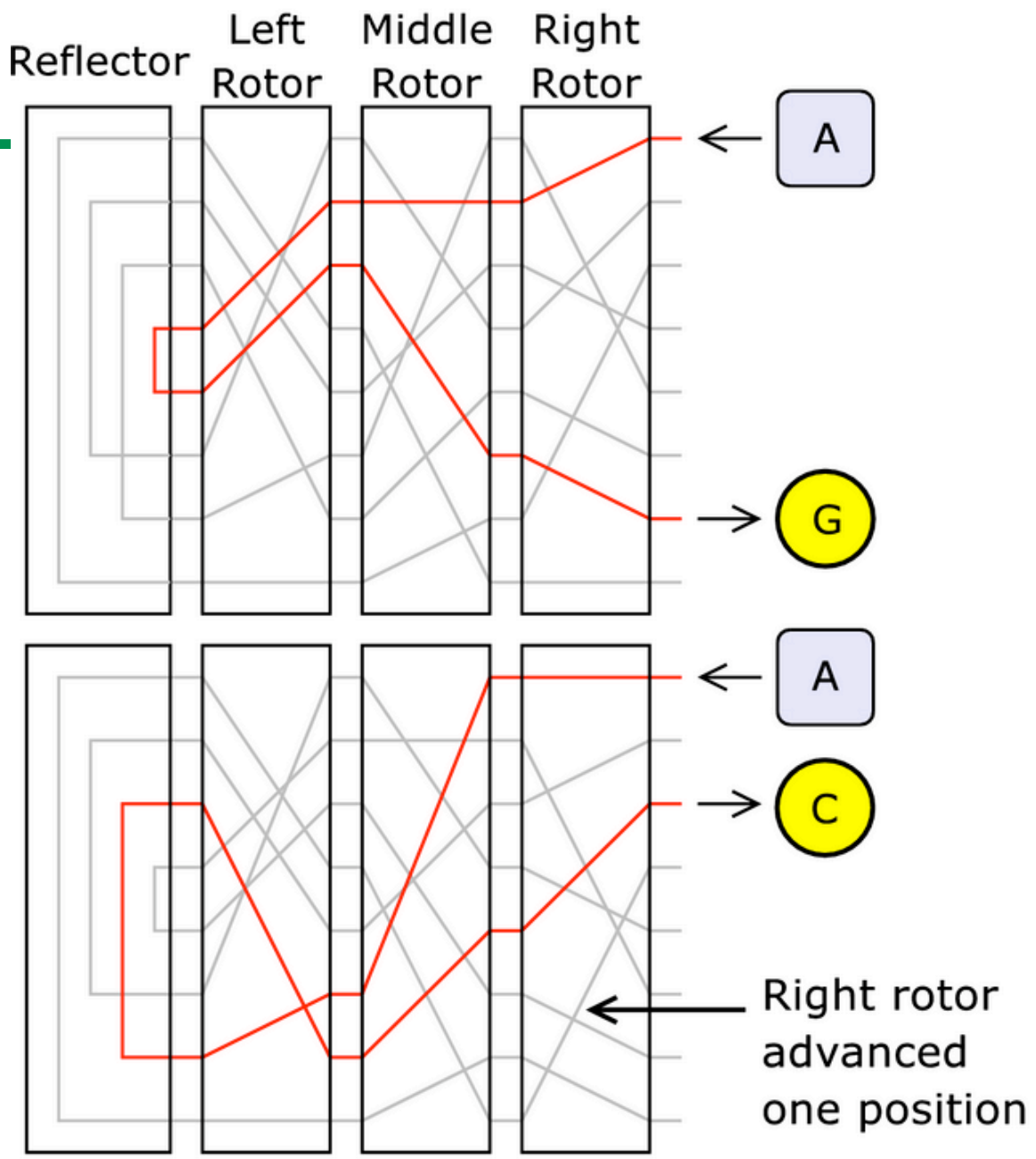
History of the Enigma Machine

- 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 repeating of the message key and knowledge of the machine design (espionage)
- Then broken by the UK intelligence during the WW II

Enigma Machine

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

- Enigma Machine: Encrypting the same letter consecutively
- A rotor rotates 1/6th after each map
- Second rotor rotates after first had a complete revolution, and so on



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 use 5 rotors and 10 pairs of letters

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
- Use of message key: a new scrambler starting position, e.g., PGH
  - first encrypt and send the message key, then set the machine to the new position and encrypt the message
  - initially the message key is encrypted twice

Encrypting with Enigma

- Machine was designed under the assumption that the adversary may have access to the machine
- **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

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?

- Catalog of “characteristics”
  - Main idea: separating the effect of the plugboard setting from the starting position of rotors
  - determine the rotor positions first
  - then 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