CS408
Cryptography & Internet Security

Lecture 4:
Rotor Machines
Enigma

Reza Curtmola
Department of Computer Science / NJIT

- How to move from pencil and paper to more automatic ways of encrypting and decrypting?
- Alberti Cipher Disk
- Jefferson Wheel
- Enigma

Alberti Cipher Disk

- Outer disk is fixed (used for plaintext)
- Inner disk can be rotated (used for ciphertext)

- Encode:
  - Split plaintext in chunks of text
  - For each chunk of text: rotate the inner disk and transform the plaintext letter into the corresponding ciphertext letter

- Decode:
  - A disk with the same alphabets must be used
  - Need to know the correct letter to match the mark to rotate the inner disk

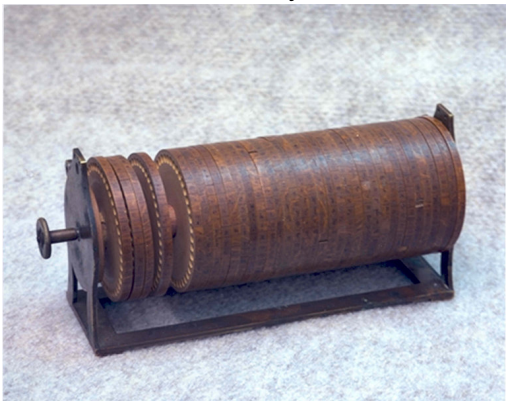
Alberti Cipher Disk - example

- Text to encode: TERRANOVA
- Pick text chunks of size 5
- Encode:
  - First chunk: align g (inner disk) under A (outer disk); encode TERRA into ipmmg
  - Second chunk: align g (inner disk) under G (outer disk); encode NOVA into pryf
  - Final encoding is: AipmmgGprvf

- Decode:
  - How do you decode?

Jefferson Wheel Cipher

- 36 disks, each disk has the 26 letters of the alphabet arranged in some random order
- The order of the disks on the axle is the cipher key
- Invented by Thomas Jefferson in 1795
- Used by the United States Army between 1923-1942

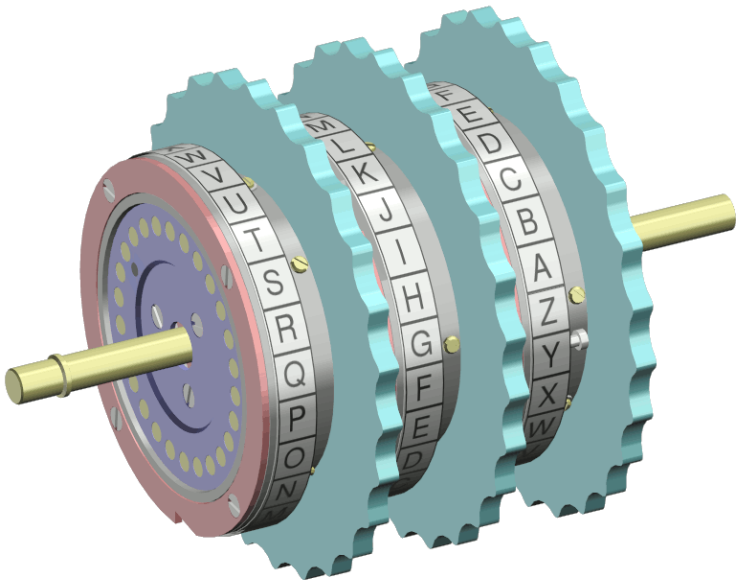


Jefferson Wheel Cipher

- Encode:
  - Rotate each disk until the desired message is spelled in one row
  - The ciphertext is any row on the disks other than the one that contains the plaintext
- Decode:
  - The disks must be arranged on the axle in the same order (which has been pre-agreed)
  - Rotate disks until the ciphertext is spelled out in one of the rows
  - Read the other rows until plaintext is found

Rotor Machines

- Basic idea: if the key in Vigenere cipher is very long, then the attacks won't work
- How to have a longer key?
- Idea: multiple rounds of substitutions
- A machine consists of multiple cylinders
  - each cylinder has 26 states, and each state it 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



Rotor Machines

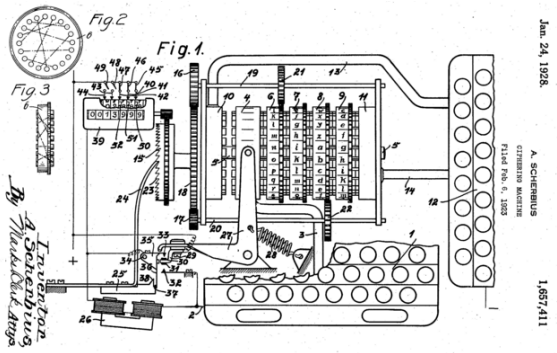
- A m-cylinder rotor machine has
  - 26^m different substitution ciphers
    - $26^3 = 17576$
    - $26^4 = 456{,}976$
    - $26^5 = 11{,}881{,}376$
- The most famous rotor machine is the Enigma machine

History of the Enigma Machine

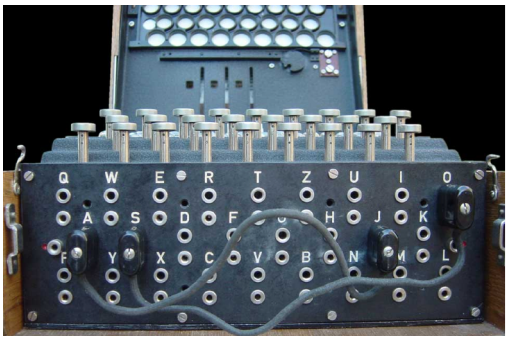
- Patented by a German engineer named Arthur Scherbius in 1918
- Widely used by the Germans from 1926 to the end of second world war
- First successfully broken by Polish in the thirties by exploiting the repeating of the message key and knowledge of the machine design (espionage)
- Then broken by the UK intelligence during the WW II
- The fact that Enigma was broken remained a secret for 30 years! Why do you think?

Enigma Machine Trivia

- Patented by Scherbius in 1918
- Came on the market in 1923, weighted 50 kg (about 110 lbs), later cut down to 12kg (about 26 lbs)
- It costs about $30,000 in today's prices

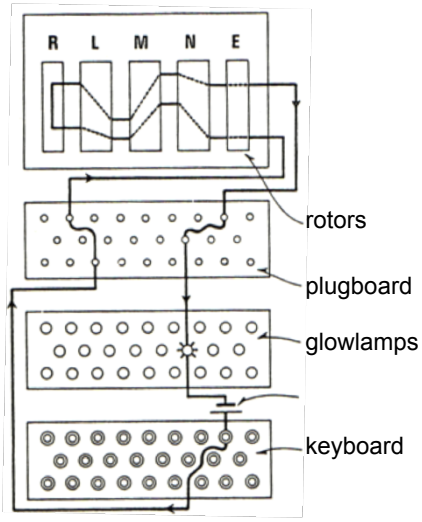


Enigma machine

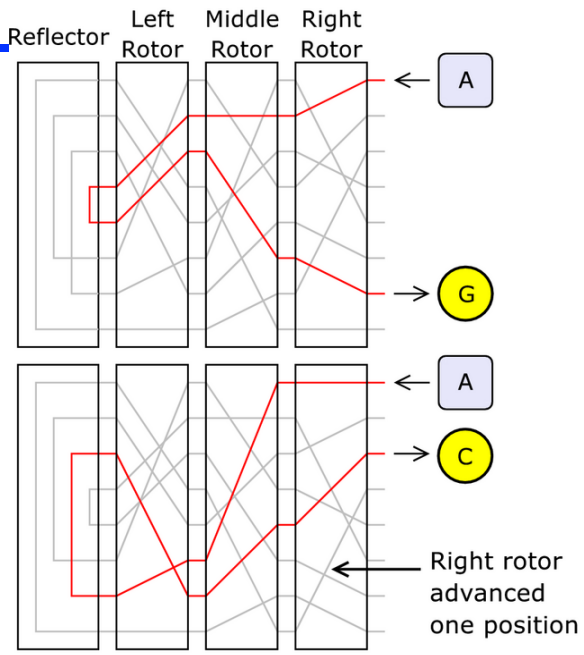


Enigma machine

- A combination of mechanical and electrical subsystems
- Keyboard
- Entry wheel (E): leaves the input unmodified
- Three rotors: L, M, N
- Each rotor:
  - on one side has 26 fixed electrical contacts;
  - on the other side there are 26 spring-loaded contacts which touch the contacts of the adjacent rotor
  - Inside each rotor, the fixed contacts are connected to the spring-loaded contacts in a random manner (these connections are different for each rotor)
- Plugboard:
  - 6 pair of letters can be connected (and thus the letters are swapped)
- A reflector (R) (has 26 contacts connected in pairs)



- This example shows how encryption works for the same letter (A) consecutively
- First rotor (R) rotates 1/26th after a key is pressed
- Second rotor (M) rotates after first rotor had a complete revolution, and so on



Enigma machine: Decryption

- Works the same way as encryption
- Sender and receiver mush have identical machines, both set to the same initial positions

Security of the Enigma machine

- What must be kept secret?
  - The initial settings of the rotors
  - The setting of the plugs on the plugboard
  - The internal wiring of the rotors
  - The internal wiring of the reflector

Questions to think about…

- 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? (shift, substitution, etc.)
- What can you say about the result of encrypting the same letter consecutively?

Enigma Machine: Size of Key Space

- Use 3 rotors:
  26^3 = 17576 substitutions
- 3 rotors can be used in any order: 6 combinations
- Plugboard: allows 6 pairs of letters to be swapped before the scramblers process started and after it ended.
  100,391,791,500 ways of interchanging 6 pairs of letters
- Total number of keys ≈ 10^{16}
- Later versions use 5 rotors and 10 pairs of letters

Encrypting with Enigma

- Machine was designed under the assumption that the adversary may get access to the machine
- **Daily key**: The settings for the rotors and plugboard changed daily according to a **codebook received by all operators**
- **Message key**: Each message was encrypted with a unique key defined by the starting position of each of the 3 rotors
  - A new message key was chosen for each message
- An encrypted message consists of:
  - the message key encrypted with the daily key (using the daily codebook); it was repeated twice
  - the message encrypted with the message key

Using Enigma Machine

- A daily key has the form
  - Plugboard setting: A/L–P/R–T/D–B/W–K/F–O/Y
  - Rotor arrangement: 2-3-1
  - Rotor starting position: Q-C-W
- Sender and receiver set up the machine the same way for each message
- Receiver decrypts message key using daily codebook; the decrypted message key gives the starting position of the rotors (e.g., PGH)

- What type of cryptography is this? Symmetric or asymmetric?
- Why bother with the rotors when the enormous key space seems to be determined by the plugboard?
- Why is the message key needed and not just use the daily key?
- 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 Daily 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
  - 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

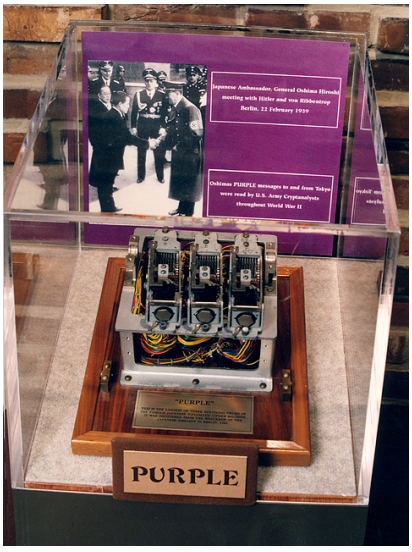
Lessons Learned From Breaking Enigma

- 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

- Although the Enigma cipher has cryptographic weaknesses, in practice it was only in combination with mistakes by operators, procedural flaws, an occasional captured machine or codebook that Allied codebreakers were able to decipher messages.

Purple (Japanese cipher machine)

- Japanese ciphering machine modeled after Enigma, used during WWII
- Broken in 1940 by US Army Signals Intelligence Service (directed by Friedman)
- Used to encode the war declaration sent to Japan's Embassy in Washington D.C. This was decoded by US codebreakers hours before the Pearl Harbor 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

Recommended Reading

- Chapter 2.12