Introduction to Cryptography CS 355

Lecture 5

The Enigma Machine

Lecture Outline

- Rotor machines
- The Enigma machine
- Breaking the Enigma machine

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

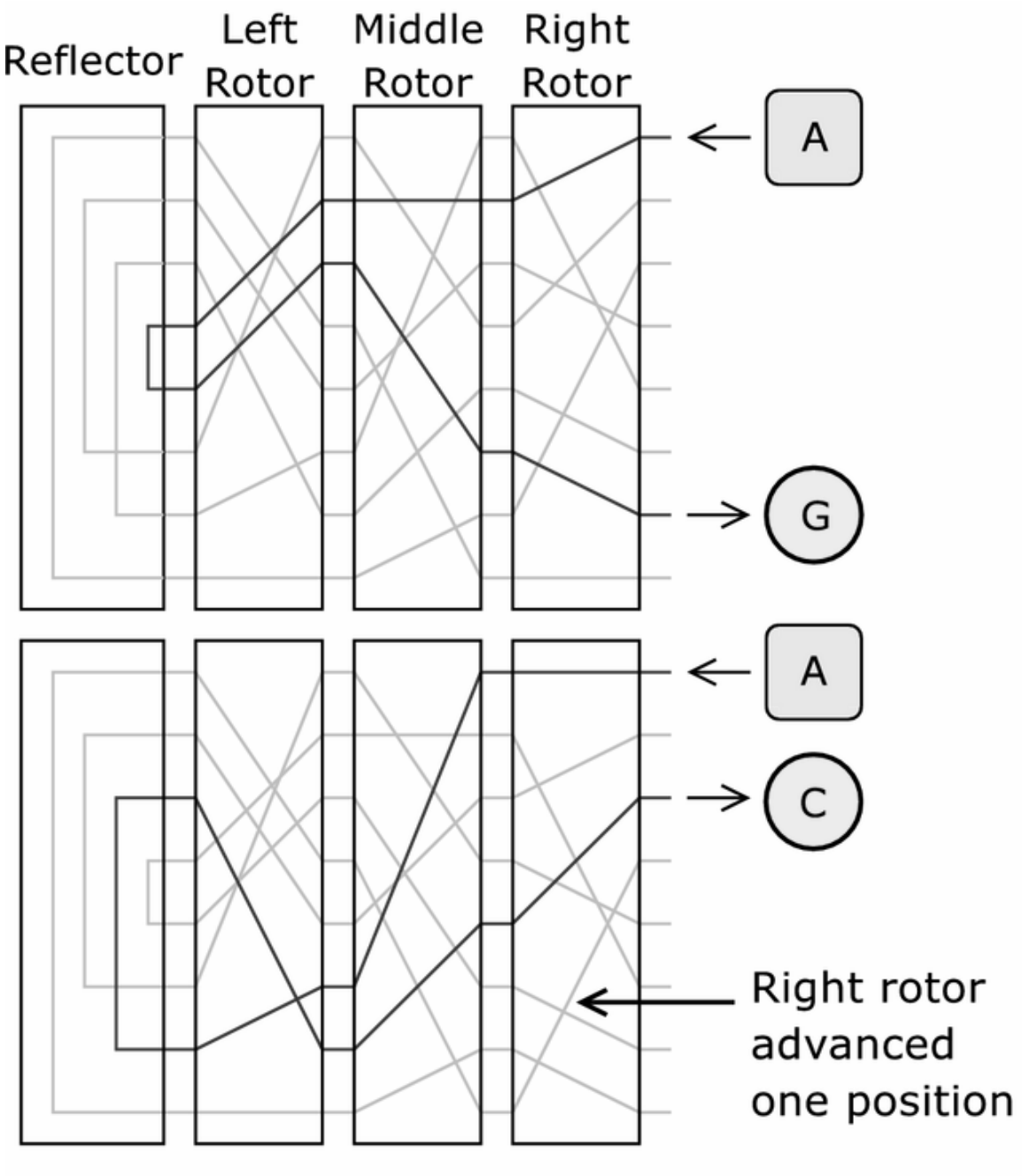
Rotor Machines

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

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



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 encryption process started and after it ended.

$$\frac{26!}{14! \bullet 6! \bullet 64} = 100,391,791,500$$

- Total number of keys $\approx 10^{16}$

Using Enigma Machine

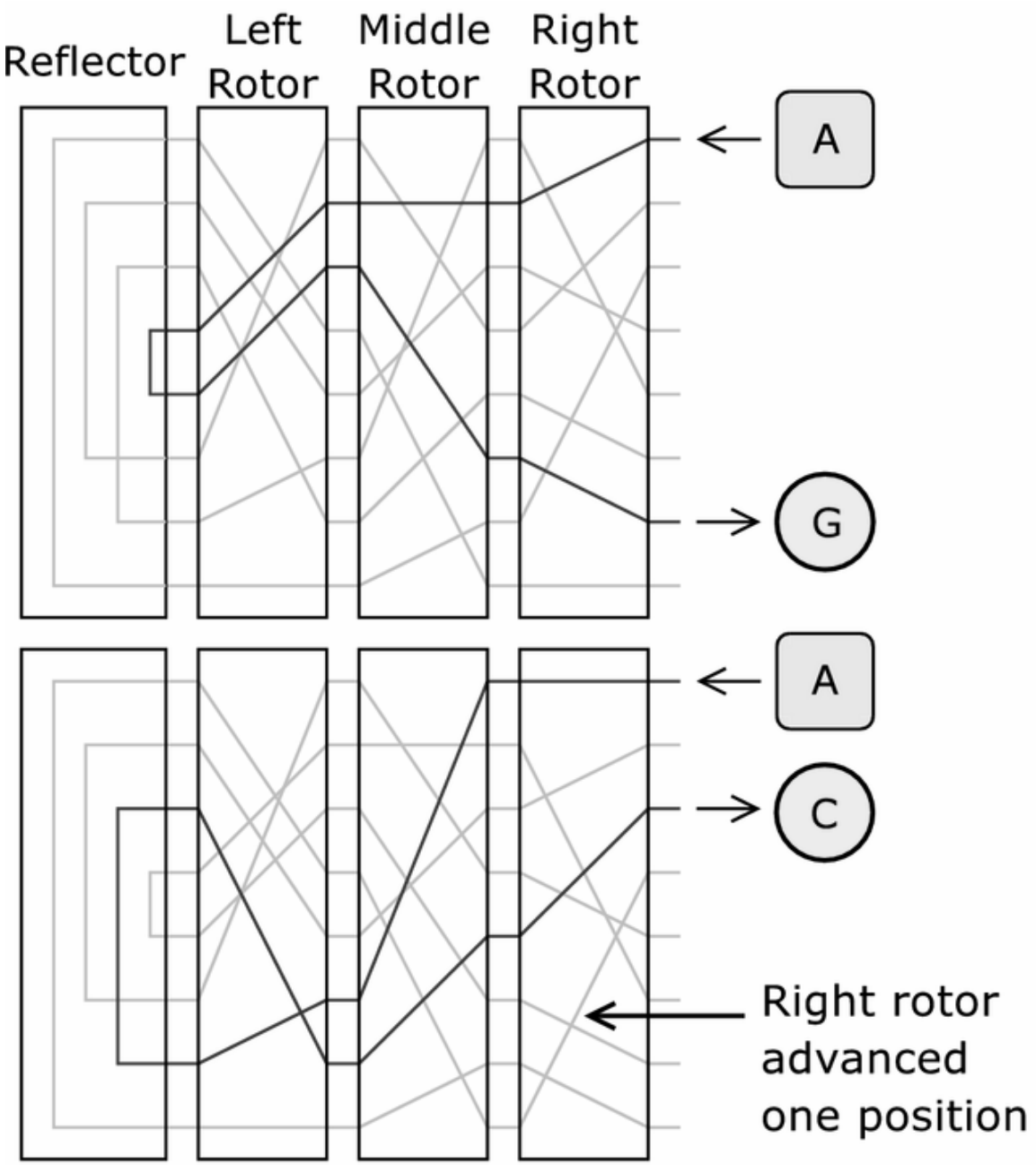
- A day key has the form
  - Plugboard setting: A/L–P/R–T/D–B/W–K/F–O/Y
  - Scrambler arrangement: 2-3-1
  - Scrambler starting position: Q-C-W
- Sender and receiver set up the machine the same way for each message
- Use of message key: a new scrambler starting position, e.g., PGH
  - first encrypt and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

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
- Then broken by the UK intelligence during the WW II

Permutations

- A **permutation** is a bijection from a finite set *X* onto itself.
- Each permutation has an inverse
- Given permutations P_1, P_2, their concatenation is also a permutation.
- The inverse of P_1P_2 is $P_2^{-1}P_1^{-1}$
- E.g., P_1 = CBDEA, P_2=DAEBC, then
  P_2P_1=?


Reflector
Left Rotor
Middle Rotor
Right Rotor
A
G
A
C
Right rotor advanced one position

Mathematical Description

- Let P denote the plugboard transformation
- Let L,M,R denote the three motors
- Let U denote the reflector,
- Then the encryption function

  $E = PRMLUL^{-1}M^{-1}R^{-1}P^{-1}$

  or, $E = PTUT^{-1}P^{-1}$
- Fact 1: $E[x] \neq x$
- Fact 2: $E[E[x]] = x$

How the Polish Break Enigma Machine

- They have a copy of the machine
  - need to find out day key to decrypt message key and then the message
- Main idea: separating the effect of the plugboard setting from the starting position of motors
  - determine the motor positions first
  - then attacking plugboard is easy
- Exploiting the repetition of message keys
  - In each ciphertext, letters in positions 1 & 4 are the same letter encrypted under the day key
  - The relationship is a permutation
  - plugboard does not affect chain lengths in the permutation

Summary

Recommended Reading for This Lecture

- The Code Book
  - Chapters 3 and 4

Coming Attractions …

- Extended Euclidean Algorithm
- The Chinese Remainder Theorem

- Recommended reading for next lecture:
  - Trappe & Washington: 3.2 & 3.4