Enigma Machine

1/21/12 1:40 PM

Enigma Set-up (get out paper enigmas)

- Typewriter with the alphabet
- Glass windows in which letters appear
- 3 rotors, labeled I, II, and II
  - unlike paper enigma machines, rotors usually have the numbers 1-26 on them instead of actual letters of the alphabet
  - order different each day
- reflector
- plugboard
  - 26 sockets
  - most are "cross-steckered" and usually about 6 or so are self-steckered
- keyboard → plugboard → right rotor → middle rotor → left rotor → reflector → left rotor → middle rotor → right rotor → glass window

Important Features

- Immune to frequency analysis
- Morse code usually used to transmit ciphertext
  - Prone to error
- Ciphertext letter never matches the plaintext letter
  - Ex: "b" can go to P, J, O, K, …. But never "B"
  - Repeats after 16, 900 (26 *25 *26) keyings
  - Messages limited to 250 letters for this reason

Cracking Enigma: Polish

- Broken by Marian Rejewski and others in 1930s
- Most information attained through German traitor working with French intelligence
- Had access to German documents and a few pages of daily enigma keys
  - Enigma keys = initial rotor settings
- First step: how the enigma machine is set up
  - Had general idea, but how are keys set up?
    - There is a way they are set up on typical German typewriter, but Rejewski correctly guessed that they were actually in alphabetical order
  - Had replicas of the machine made

- Major weakness in the machine: message key sent twice
    - Ex: “moplyb”
        - M, l come from the same letter
        - O, y come from the same letter
        - P, b come from the same letter
- Breaking it involves permutations
- Example:
    - Say we have 3 message keys from a given day
        - Dmqvbn
        - Vonpuy
        - Pucfmq
    - Each position corresponds to a different permutation of the alphabet; A, B, C, D, E, and F
    - Remember there are repeats, so “d” and “v” come from the same letter, “m” and “b” and so on
    - Strategy: look at the permutation products AD, BE, CF
    - How do you multiply permutations?
        - 1 2 3 4 5 6   x   1 2 3 4 5 6 = 1 2 3 4 5 6
        - 2 3 6 1 4 5   1 6 5 2 4 3   6 5 3 1 2 4
    - back to our example, suppose we don’t know our message key, let it be xyz
        - so xyzxyz → dmqvbn
        - know: permutation A sends x → d
        - know: permutation D sends x → v
        - also know: d → x, v → x
        - so d → x and x → v which means d → v
        - v → p and p → f so v → f and so on
    - eventually, you will get back to the beginning, but need the whole alphabet to get the entire permutation, so write as a product of disjoint cycles:
        - ABCDEFGHIJKLMNOPQRSTUVWXYZ
        - XFEARBSLHQIGCVDZWKMNJUOYTP
        - Cycles: (AXYNVUJQWOP)(BF)(CERKIHLGSMC)(PZ)
            - AXYNVUJQWOP
            - BF
            - CERKIHLGSMC

            - PZ
    - In our example, you might get the cycle products
        - AD = (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)
    - Plugboard adds a permutation S at the beginning and S^{-1} at the end
        - Cycles may be different but the number and lengths of the cycles will be the same
        - Consequence: changing the plugboard settings without changing the initial rotor position doesn't make it much more difficult to decrypt
    - Take our ciphertext and figure out the cycle lengths and find "matching" initial rotor settings in card catalog
        - Small enough so that each can be checked individually relatively quickly
        - Even quicker after started using a cyclometer (computes lengths and number of cycles)
- Problem: 1938 operator begins choosing settings for each message instead of using a daily codebook
- Rejewski's method becomes more difficult to use
- Henryk Zygalski creates perforation sheets
    - Takes advantage of "females"
        - Female = one of the repeated letters in the key is enciphered to the same letter
        - Ex: SZVSIK 1-4 female
        - Occurs in 1 of 8 messages
    - Keeps track of occurrences of females on perforation sheets
    - Set of 26 sheets for each of 6 possible sequences of rotor orders
    - Had about 1000 holes in positions on sheets where female could occur
    - How to use: superimpose sheets, move around until you find a single aperture
    - Ended up impractical, never got much use because more changes to enigma
        - 1938: 2 more rotors
        - 1939: more plugboard connections