Cracking the Enigma

Rotor machines

CS349 Cryptography
Department of Computer Science
Wellesley College

Mechanization of secrecy

- Advances in cryptanalysis prompted the need for more secure (read more complex) cryptosystems.
- However, the weakest link in any cryptosystem is generally the people who use it.
Cipher disks

- The Confederate Alberti disk may be thought of as a mechanized Caesar cipher.
- However, it can also be used in a manner that is functionally equivalent to the Vigenere cipher.

Rotor machines

- Shortly after the first world war, the German firm of Scherbius and Ritter developed an electronic version of the Alberti disk.
- Typing a "b" on the keyboard causes a current to flow through the scrambler and emerge on the other side to illuminate the "a" light lamp.
Adding an element of Vigenere

- Every time a letter is typed into the keyboard and encrypted, the scrambler rotates by one place.
- After one rotation, result of typing a "b" is functionally equivalent to first shifting "b" back one position, passing through the scrambler, then shifting the result forward one position: $c_i = p_i \cdot R \cdot p_i$.

*Here $p_i = i^{th}$ plaintext, $c_i = i^{th}$ ciphertext, $p_i = shift$ rotor by $i$ positions, and $R$ is scrambler.

Adding a second scrambler

- With only one scrambler, there are only 26 distinct starting positions.
- This is not a key space that is likely to worry even the dimmest watt bulb.
Commercial Enigma machines

- Commercial Enigma machines had three rotors and a reflector.
- The reflector is a *complication illusoire*. But it serves an important role never the less.

Wehrmacht Enigma machines

- The number of keys with three rotors is $26^3 = 17,576$.
- A dozen determined cryptographers could search the entire space in a day.
- Early Wehrmacht machines were provided with removable, interchangible rotors and a plugboard.
Enigma

- Packaged up and weighing in at about 12 kilos, thousand of Enigmas were distributed throughout the German army by the start of World War II.
- An Enigma emulator may be found at http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/enigma.html

Alan Turing meets Enigma

- The best and the brightest were brought to Bletchley Park to break the code.
The method of isomorphs

- The action of the three scramblers may be described as
  \[ S_{(i_1,i_2,i_3)} = p^{\Delta_i} R_N p^{i_1} R_M p^{i_2} R_L p^{i_3} \]

- Combining this with the action of the reflector,
  \[ c_i = p_i S_{(i_1,i_2,i_3)} U S_{(i_1,i_2,i_3)} \]
  \[ = p_i (p^{\Delta_i} R_N p^{i_1} R_M p^{i_2} R_L p^{i_3}) U (p^{\Delta_i} R_N p^{i_1} R_M p^{i_2} R_L p^{i_3}) \]
  \[ = p_i (p^{\Delta_i} R_N p^{i_1} U p^{\Delta_i} R_M U p^{\Delta_i} R_L U p^{\Delta_i} R_M U p^{\Delta_i} R_L) \]

  where
  \[ U_{(i_1,i_2,i_3)} = p^{\Delta_i} R_M p^{\Delta_i} R_L p^{\Delta_i} R_L p^{\Delta_i} R_M p^{\Delta_i} \]

Rotated alphabets

- The relationship
  \[ c_i = p_i (p^{\Delta_i} R_N p^{i_1} U p^{\Delta_i} R_M U p^{\Delta_i} R_L U p^{\Delta_i} R_M U p^{\Delta_i} R_L) \]
  implies
  \[ c_i (p^{\Delta_i} R_N p^{i_1}) = p_i (p^{\Delta_i} R_N p^{i_1}) U_{(i_1,i_2)} \]

- In other words, \( c_i (p^{\Delta_i} R_N p^{i_1}) \)
  and \( p_i (p^{\Delta_i} R_N p^{i_1}) \)
  are isomorphic sequences during period that the other rotors remain stationary.
Meet in the middle attack

- A probable word is compared with a fragment of the cryptotext:
  reconnaissance
  UPYTEJOJZEGBOT

- We test whether rotor I is the fastest moving by encoding the operation of $p_i^3 R_3 p_i^1$ on each the plaintext and ciphertext pair.

A direct hit

- The involutory property is confirmed in row $i=2$ both confirming rotor I as the fast rotor RN,
- . . . and yielding 14 pairs of entry and exit characters for the next round*:
  j g m f u h r w c n s e w
  U Z C Z B J O T A M Q E S A

*In practice, a prefabricated catalogue with $2 \times 26^2 = 1352$ entries list all $U_{(i,j,k)}^{(i,j)}$ with corresponding rotor positions was used.
Investigation in parts

- The analysis above is based on the assumption that the medium rotor RM does not move.
- If it does, then the pseudo-reflector is changed and the investigation decomposes into two parts without becoming essentially more difficult.

Alan Turing deals with the plugboard

- He began by postulating the position of a "crib". In this, he was aided by that fact that no letter ever encipher to itself.
- For example, does the following crib match the given ciphertext?

  Crib: wetternullechs
  CIPHER: I P R E N L W K M J J S X C P E J W Q
Turing loops

- Next, he constructed a list of internal loops linking plaintext and ciphertext characters.

Turing Bombes

- A consequence of the loop is to nullify the effect of the plugboard.
- Sixty Enigma machines were set up, one for each of the ways of arranging the five rotors taken three at a time.
- These sixty machines clicked around in unison until a circuit was completed and the light illuminated.
Success

- Once the correct scrambler arrangements and orientations had been established, finding the plugboard cabling was a piece of cake.
- By the end of 1942, 49 bombes were clicking around the clock.

The Kriegsmarine remained a problem

- Naval Enigmas had eight, not five scramblers and the reflector was adjustable.
- Naval operators were careful not to send stereotypical messages, depriving Bletchley of cribs and used a more secure system for exchanging keys.