CPSC 467b: Cryptography and Computer Security

Michael J. Fischer

Lecture 5b
January 29, 2013

Symmetric cryptosystem families

Stream ciphers

- Manual stream ciphers
- Rotor machines

Symmetric cryptosystem families

Symmetric cryptosystem families

Symmetric (one-key) cryptosystems fall into two broad classes, *block ciphers* and *stream ciphers*.

- A block cipher encrypts large blocks of data at a time.
- A stream cipher encrypts a character stream in an on-line fashion, encrypting and outputting each byte before reading the next.

DES and AES are block ciphers. In this lecture, we look at several approaches to construct stream ciphers, either from scratch or based on block ciphers.

Stream ciphers

Classical stream ciphers

The monoalphabetic substitution ciphers discussed in lecture 3 are naturally stream ciphers since they encrypt a character at a time.

This contrasts with the polygraphic ciphers (such as the Hill and Playfair ciphers), which require a full block of characters before any can be encrypted.

State machine ciphers

A state machine allows a different substitution to be used for a letter, depending on its position in the message.

The Vigenère cipher is a simple example, where the state s is simply the letter position modulo the key length r, and s is used to select a key k_s for the Caesar cipher from an array of r such keys.

Rotor machines are mechanical polyalphabetic cipher devices that generalize Vigenère ciphers, both in having a very large value of r and in their method of generating the substitutions from the letter positions.

Rotor machines

- Rotor machines are mechanical devices for implementing stream ciphers.
- They played an important role during the Second World War.
- The Germans believed their Enigma machine was unbreakable.
- The Allies, with great effort, succeeded in breaking it and in reading many of the top-secret military communications.
- This is said to have changed the course of the war.

Image from Wikipedia

How a rotor machine works

- Uses electrical switches to create a permutation of 26 input wires to 26 output wires.
- Each input wire is attached to a key on a keyboard.
- Each output wire is attached to a lamp.
- The keys are associated with letters just like on a computer keyboard.
- Each lamp is also labeled by a letter from the alphabet.
- Pressing a key on the keyboard causes a lamp to light, indicating the corresponding ciphertext character.

The operator types the message one character at a time and writes down the letter corresponding to the illuminated lamp.

The same process works for decryption since $E_{k_i} = D_{k_i}$.

keystream generation

The encryption permutation.

- Each rotor is individually wired to produce some random-looking fixed permutation π.
- Several rotors stacked together produce the composition of the permutations implemented by the individual rotors.
- In addition, the rotors can rotate relative to each other, implementing in effect a rotation permutation (like the Caeser cipher uses).

keystream generation (cont.)

Let $\rho_k(x) = x + k \bmod 26$. Then rotor in position k implements permutation $\rho_k \pi \rho_k^{-1}$.

Several rotors stacked together implement the composition of the permutations computed by each.

For example, three rotors implementing permutations π_1, π_2, and π_3, placed in positions r_1, r_2, and r_3, respectively, would produce the permutation

$$\begin{aligned} & \rho_{r_1} \cdot \pi_1 \cdot \rho_{-r_1} \cdot \rho_{r_2} \cdot \pi_2 \cdot \rho_{-r_2} \cdot \rho_{r_3} \cdot \pi_3 \cdot \rho_{-r_3} \\ = \quad & \rho_{r_1} \cdot \pi_1 \cdot \rho_{r_2 - r_1} \cdot \pi_2 \cdot \rho_{r_3 - r_2} \cdot \pi_3 \cdot \rho_{-r_3} \end{aligned} \tag{1}$$

Changing the permutation

After each letter is typed, some of the rotors change position, much like the mechanical odometer used in older cars.

The period before the rotor positions repeat is quite long, allowing long messages to be sent without repeating the same permutation.

Thus, a rotor machine is much like a polyalphabetic substitution cipher but with a very long period.

Unlike a pure polyalphabetic cipher, the successive permutations until the cycle repeats are not independent of each other but are related by equation (1).

This gives the first toehold into methods for breaking the cipher (which are far beyond the scope of this course).

History

Several different kinds of rotor machines were built and used, both by the Germans and by others, some of which work somewhat differently from what I described above.

However, the basic principles are the same.

The interested reader can find much detailed material on the web by searching for "enigma cipher machine" and "rotor cipher machine". Nice descriptions may be found at `http://en.wikipedia.org/wiki/Enigma_machine` and `http://www.quadibloc.com/crypto/intro.htm`.