

B. Substitution Ciphers, continued

3. Polyalphabetic: Use multiple maps from the plaintext alphabet to the ciphertext alphabet.

Non-periodic case:

Running key substitution ciphers use a known text (in a standard book, say). Encipher as for Caesar or Vigenère, except that the key is not periodic or constant. Since the key is as long as the message, this cipher may seem to be unbreakable, like the one-time pad, but it is not if the key is redundant, as in English text. Roughly speaking, this is so because a large proportion of letters in both key and plaintext will be high frequency letters (ETAOIN SHRDLU).

Rotor machines produce running key substitution ciphers with large period d . $d = 26^t$ with t rotors. The Enigma was a rotor machine ($t = 4$) used by the Germans in WW II and broken by Alan Turing (1912–1954) using group theory.

The UNIX `crypt(1)` command is a rotor machine with $t = 1$ and 256 positions.

A *one-time pad* uses a truly random sequence as long as the plaintext as its key.

The *Vernam cipher* is a one-time pad which XOR's the plaintext and key. The key must be sent in advance. Do not use a random number generator that comes with a computer; they are not cryptographically secure. Do not reuse a one-time pad: If the same key is used to encipher M_1 and M_2 , then $C_1 \oplus C_2 = M_1 \oplus M_2$, which is easy to break. (Compare with the running key ciphers above.)

4. Polygram: Make arbitrary substitution for groups of characters.

Encipher blocks of $d > 1$ letters together as a unit.

Example. Playfair cipher has $d = 2$. The key is a 5×5 matrix (no J) of 25 letters randomly placed. Used by British in WW I.

Rules to encipher (m_1, m_2) to form (c_1, c_2) :

1. If $m_1 \neq m_2$ in the same row, then c_1, c_2 are the two letters to the right of m_1, m_2 .

2. If $m_1 \neq m_2$ in the same column, then c_1, c_2 are the two letters below m_1, m_2 .

3. If m_1, m_2 are in different rows and different columns, then c_1, c_2 are the other two corners of the rectangle whose diagonal is $m_1 m_2$, with c_1 being in the same row as m_1 .

4. If $m_1 = m_2$, insert a letter (X) between them to eliminate the double letter

5. If a single character of plaintext is left at the end of the message, append an X to fill the last pair.

Example K= FUZZINESS

M: RE NA IS SA NC EX

C: MC ZC UB AB CL BT

Another example of a polygram substitution cipher is the Hill cipher.

C. Product Ciphers.

A *product cipher* is a composition of several substitution and transposition ciphers.

$$C = E_K(M) = S_t \circ T_{t-1} \circ \cdots \circ S_2 \circ T_1(M).$$

Example. DES enciphers 64-bit blocks with a 56-bit key. It has 16 “rounds” or steps.

There are $2^{56} \approx 7 \cdot 10^{16}$ DES keys. A million chips, each testing one key per microsecond, can break DES in about one day. Such a machine could be built for less than one million dollars. The key size of 56 bits is too small.

Double encipherment

$$C = DES_{K_1} DES_{K_2}^{-1} DES_{K_1}(M)$$

has been proposed. This is not so good because of the time-memory trade-off attack. DES is near the end of its useful life. It is still okay for short-term secrets like bank transactions, pay TV, press releases.