Cifrari a sostituzione polialfabetica

Permettono di scongiurare attacchi basati su frequenza dei caratteri.

Archivio cifrato di Augusto

Dato il primo libro dell'Iliade I e il testo T (in greco) da cifrare, il testo cifrato C (in numeri) è ottenuto con:

$$C_i = \text{pos}(I_i) - \text{pos}(T_i)$$

cioè a ogni carattere si sostituisce la distanza dal carattere in posizione corrispondente in I nell'alfabeto greco. La stessa lettera può corrispondere a numeri diversi e viceversa.

Difficile da forzare se la chiave è lunga, usata nella seconda guerra mondiale con chiave (pagina di un libro) cambiata ogni giorno.

Cifrario di Alberti

Leon Battista Alberti (XV secolo). Due dischi concentrici rotanti:

- quello esterno ha alcune lettere e numeri per formulare il messaggio (che deve contenere almeno un numero);
- quello interno, più ricco e disposto in modo arbitrario e diverso per ogni coppia di utenti, è usato per costruire il crittogramma.

La chiave è l'allineamento iniziale dei dischi (lettera corrispondente alla A) e la coppia di dischi (una copia identica per ogni utente che deve cifrare/decifrare). Ogni volta che decifrando una lettera si ottiene un numero, quella lettera diventa la chiave per il resto del messaggio (polialfabetico). Se i cambi di chiave sono tanti e irregolari il cifrario è molto sicuro.

Variante: indice mobile

Se decifrando si ottiene il numero n, allora il cambio di chiave avviene dopo n caratteri e la nuova chiave si ottiene decifrando la lettera a quella posizione.

Cifrario di Vigenère

XVI secolo. Meno sofisticato ma più pratico del cifrario di Alberti, visto che non richiede i dischi. Consiste nella composizione di cifrari di Cesare con shift diversi:

- la chiave è una breve sequenza di lettere, ripetuta ciclicamente;
- ogni lettera della chiave indica di quanto traslare le lettere in posizione corrispondente del testo in chiaro;
- si può costruire una tabella 26×26 per cifrare e decifrare velocemente.

Problema: conoscendo la lunghezza della chiave si può decomporre il testo in blocchi con cifratura monoalfabetica, facili da forzare.

One-Time Pad è un cifrario di Vigenère con chiave lunga quanto il testo ed usata una sola volta.