Cifrari a sostituzione monoalfabetica

Sono tutti deboli ad attacchi basati sulla frequenza delle lettere.

Cifrario di Cesare

Le lettere del messaggio in chiaro sono traslate di 3 posizioni. Non ha chiave segreta, quindi la sicurezza dipende interamente dalla segretezza del metodo (cifrario ad uso ristretto).

Si può generalizzare introducendo una chiave $k \in \{1, \dots, 25\}$:

- $C(x) = y$ t.c. $\text{pos}(y) = (\text{pos}(x) + k) \bmod 26$
- $D(y) = x$ t.c. $\text{pos}(x) = (\text{pos}(y) - k) \bmod 26$

dove 26 è la dimensione dell'alfabeto (26 non è una chiave ammissibile perché corrisponde a 0).

Proprietà:

- commutativo: si può cifrare più volte con diverse chiavi ottenendo lo stesso crittogramma indipendentemente dall'ordine di cifratura;
- una sequenza di cifrature equivale ad una sola con chiave uguale alla somma delle chiavi della sequenza – cifrare più volte non aumenta la sicurezza;
- è sufficiente trovare una singola corrispondenza tra lettera in chiaro e lettera cifrata per determinare k.

Cifrario affine

- chiave $k = (a, b)$, con $(a, 26) = 1$ (altrimenti non esiste a^{-1})
- $C(x) = y$ t.c. $\text{pos}(y) = (a\text{pos}(x) + b) \bmod 26$
- $D(y) = x$ t.c. $\text{pos}(x) = a^{-1}(\text{pos}(y) - b) \bmod 26$

Ci sono $\phi(26) \cdot 26 - 1 = 311$ chiavi possibili (scartando la chiave $(1, 0)$).

Se $k = (13, 0)$ tutte le lettere in posizione pari vanno in 0, quelle in posizione dispari in 13, quindi non è iniettiva.

Cifrario completo

La chiave è una permutazione arbitraria dell'alfabeto, quindi ce ne sono $26! - 1$ non banali e un attacco di forza bruta non è praticabile.