Crittografia

Classica

Notazioni

- P : Insieme dei messaggi "in chiaro"
- C : Insieme dei messaggi criptati
- f : Funzione di *Trasformazione Crittografica*
- K_E: Chiave di Cifratura (parametro per f)
- K_D: Chiave di Decifratura (parametro per f^{-1})

Crittografia classica

- Crittosistemi in cui, noti f e K_E, il tempo necessario a calcolare f^{-1} e K_D è approssimativamente uguale al tempo necessario a codificare un messaggio.
- La complessità computazionale necessaria per determinare K_D e decifrare un messaggio è dello stesso ordine di grandezza della complessità della cifratura.

Metodo di Cesare

- P = C = {A, B, C, …, X, Y, Z}
  = {0, 1, 2, …, 23, 24, 25}
- $K_E = k \in P,\ k \neq 0$
- $f(x) = (x + k) \bmod 26$
- $K_D = k_d \in P,\ k_d = 26-k$
- $f^{-1}(x) = (x + k_d) \bmod 26$

Metodo di Cesare

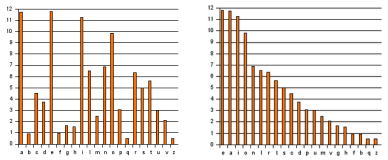
- char critta(char c, int key, string alfabeto)
- char decritta(char c, int key, string alfabeto)

Cesare - crittanalisi

- Brute force
  - n-1 possibili chiavi su alfabeto di n caratteri
- Analisi di frequenza

Lettera	Frequenza
a	11.74%
b	0.92%
c	4.50%
d	3.73%
e	11.79%
f	0.95%
g	1.64%
h	1.54%
i	11.28%
l	6.51%
m	2.51%
n	6.88%
o	9.83%
p	3.05%
q	0.51%
r	6.37%
s	4.98%
t	5.62%
u	3.01%
v	2.10%
z	0.49%

Lingua italiana frequenza caratteri



Metodo di Vigenère

- "Evoluzione" del metodo di Cesare.
- Meno suscettibile all'analisi di frequenza sulle singole lettere.
- Considerato "inattaccabile" per secoli.

Vigenère

- P = C = {A, B, C, …, X, Y, Z}
  = {0, 1, 2, …, 23, 24, 25}
- $K_E = k = [k_0, k_1, k_2, \ldots, k_{m-1}] \in P^m$, $k \neq [0, \ldots, 0]$
- $f(x_i) = (x_i + k_i) \bmod 26$

Vigenère - esempio

- Alfabeto
  - ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
- Testo in chiaro (P)
  - ITIS Leonardo da Vinci
- Chiave
  - Informatica
- Testo crittato (C)
  - Agde UsOusPDg qv hrBCp

http://www.cryptool-online.org/