Crittografia

Concetti matematici

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})

Definizione

- 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.
- In altre parole, 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}
- $K_E = k \in P, k \neq 0$
- $f(x) = (x + k) \bmod 26$
- $f^{-1}(x) = (x + (26 – k)) \bmod 26$

Esercitazione

- Scrivere la classe Java Cesare che permette di crittare un file di testo e di decrittarlo.
- Scrivere la classe CesareHacker che tenta di decrittare un file di testo crittato con il metodo di Cesare senza conoscere la chiave

Metodo di Vigenère

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

Esercitazione

- Scrivere la classe Java Vigenere che permette di crittare un file e di decrittarlo (suggerimento: ereditare dalla classe Cesare)

Domande

- Cosa succede ad applicare il Metodo di Cesare più volte, cioè a criptare un messaggio già criptato (eventualmente con una chiave differente)?
- E con il Metodo di Vigenère?

Ringraziamenti

- *Materiale tratto dalle lezioni del Prof. Alessandro Zaccagnini, Luigi Corvacchiola e Giovanna Di Donna nel "Laboratorio di crittografia" del Piano Lauree Scientifiche presso l'ITIS Leonardo da Vinci in collaborazione con la facoltà di Matematica dell'Università degli studi di Parma.*