

Tecniche tradizionali di cifratura

Lezione 3 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Studi in Informatica applicata, AA 2006-7

Indice

1. Tecniche tradizionali di cifratura
2. cifrature per sostituzione
3. crittoanalisi di cifratura monoalfabetica
4. sostituzione con blocchetto
5. cifratura di Vernam
6. cifrature per trasposizione
7. combinazioni di cifrature

cifrature per sostituzione

cifratura **monoalfabetica**, o sostituzione semplice

funzione di codifica: una **permutazione dell'alfabeto**

$$\pi = \underline{n} \rightarrow \underline{n}$$

esempio storico: **cifratura di Cesare**

$$\pi(n) = (n+3) \bmod 23$$

la cifratura di Cesare è **senza chiave** ...

si generalizza facilmente a una con chiave (alfabeto inglese):

$$\pi_k(n) = (n+k) \bmod 26$$

si dispone così di **26** chiavi ...

... tuttavia esistono **26!** permutazioni dell'alfabeto

idea: chiave = meccanismo di determinazione dell'**indice k** della permutazione π_k
fra le **26!** possibili

esempi: chiave = segmento iniziale della permutazione

criptoanalisi di cifratura monoalfabetica

complessità della sostituzione semplice:

lineare nella lunghezza del messaggio

vulnerabilità della sostituzione semplice:

sensibile alla distribuzione della **frequenza media** dei caratteri nella lingua

bastano pochi indizi per restringere la scelta fra **26!** possibili permutazioni a un numero molto inferiore

debolezza inerente:

tutte le occorrenze di ciascun carattere sono cifrate allo stesso modo

esempio: MACodExample.txt

sostituzione con blocchetto

idea: chiavi usa-e-getta da un "blocchetto" (one-time pad)

lunghezza delle chiavi concatenate = lunghezza del testo

codifica attraverso un **tableau di Vigenère**

carattere del testo in chiaro e carattere della chiave fungono da coordinate nel tableau del corrispondente carattere del testo cifrato

"cifatura perfetta" ?

anche questo metodo è sensibile alla distribuzione della frequenza media dei caratteri nella lingua! Infatti ...

le **coppie di coordinate** del tableau di Vigenère **non sono equiprobabili**

cifatura di Vernam

idea: generazione *casuale* della chiave

(lunga quanto il testo da codificare)

combinazione della chiave con il testo attraverso **XOR**

semplicità dell'algoritmo di codifica e decodifica:

$$E = D$$

si possono usare altre funzioni di (de)codifica

ad es. un tableau di Vigenère numerico

cifrature per trasposizione

le cifrature per sostituzione mirano alla **confusione** del testo

le cifrature per **trasposizione** o **permutazione** mirano alla **diffusione** del testo
attenzione: "permutazione" del **messaggio** piuttosto che dell'alfabeto (come invece accade nella sostituzione monoalfabetica)

tecnica più semplice: **trasposizione colonnare**

debolezza: è necessario disporre di **tutto il messaggio** per cominciare la codifica
(è un inconveniente per messaggi lunghi)

vulnerabilità:

facile da sospettare

indizio: frequenza dei caratteri prossima a quella tipica della lingua
criptoanalisi per **analisi dei digrammi**

combinazioni di cifrature

idea di base: **composizione** di diverse funzioni di codifica

$$E = E_2 \circ E_1$$

$$D = D_1 \circ D_2$$

la composizione **non** garantisce una crittografia più sicura

un esempio storico, la **crittografia sovietica** durante la II guerra mondiale:

uso della trasposizione colonnare per la permutazione dell'alfabeto

combinazione di diffusione e confusione non per composizione

ulteriore cifratura da blocchetto

nelle tecniche standard di crittografia (DES, AES, ...) si combinano sempre confusione e diffusione