Elementi di crittografia

Lezione 2 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 2008-9

Indice

1. Elementi di crittografia
2. protezione crittografica dell'informazione
3. algoritmi di crittografia
4. crittografia e criptoanalisi
5. criptoanalisi: fini e mezzi
6. violabilità della crittografia
7. rappresentazione numerica dell'alfabeto

protezione crittografica dell'informazione

crittografia: codifica dell'informazione per occultarne il significato

$E : P \rightarrow C$

decrittazione: il processo inverso

$D : C \rightarrow P$

sinonimi (o quasi):

crittografia, codifica, cifratura

decrittazione, decodifica, decifrazione

terminologia:

testo **in chiaro**: nella sua forma originale

testo **cifrato**: nella sua forma codificata

algoritmi di crittografia

un **algoritmo di crittografia:**

converte il testo in chiaro in testo cifrato

ha un corrispondente **algoritmo di decodifica** (inversa):

$D(E(P)) = P$

meglio se **parametrico**: si ottengono codifiche diverse per valori diversi del parametro, o **chiave** K

$C = E(K,P)$

nei sistemi di **crittografia simmetrica** le chiavi di codifica e di decodifica coincidono:

$D(K,E(K,P)) = P$

nei sistemi di **crittografia asimmetrica** le chiavi di codifica e di decodifica sono generalmente diverse (ma correlate):

$D(K_d,E(K_e,P)) = P$

crittografia e criptoanalisi

due discipline **inerentemente contrapposte**

obiettivo del **crittografo: proteggere** l'informazione dalle intrusioni
obiettivo del **criptoanalista: violare** le protezioni escogitate dal crittografo

crittografi = *"buoni"*, criptoanalisti = *"cattivi"* ?

non necessariamente!...

per almeno **due** ordini di ragioni:

contesto storico, politico, sociale
si pensi alla criptoanalisi di **Enigma** (II guerra mondiale) ...
al crittografo occorre la sapienza del criptoanalista per **collaudare l'efficacia** di algoritmi di crittografia

criptoanalisi: fini e mezzi

mira ad estrarre informazione, **anche parziale**, relativa a:

un **singolo messaggio** (violazione del messaggio)
schemi di cifratura (violazione di messaggi successivi)
deduzione di significati (senza violazione di crittografia)
deduzione della chiave (violazione di messaggi successivi)
debolezze nell'implementazione o nell'uso della crittografia
debolezze intrinseche di un algoritmo di crittografia

adopera una **grande varietà di fonti e mezzi** allo scopo:

messaggi cifrati intercettati (non decodificati)
algoritmi noti di crittografia
testo in chiaro intercettato
tecniche di analisi **matematica e statistica**
proprietà dei **linguaggi**
computer e software
"bravura", immaginazione, **fortuna...** il criptoanalista colleziona **indizi**

violabilità della crittografia

un algoritmo di crittografia è **violabile** se la criptoanalisi può rivelarlo, con tempo e dati sufficienti

in pratica occorre che tempo e dati occorrenti allo scopo stiano dentro **limiti di fattibilità** umana e tecnologica

ad **esempio:** l'**analisi esaustiva** di tutte le possibilità di decrittazione di un messaggio di 25 caratteri (maiuscoli, dell'alfabeto inglese) richiede la valutazione di $26^{25} \approx 10^{35}$ alternative ... troppe!

tuttavia ... se un **approccio ingegnoso** riuscisse a ridurre il numero di alternative da valutare a $\approx 10^{15}$, allora, con una macchina in grado di esaminarne $\approx 10^{10}$ al secondo, la violazione richiederebbe poco più di un giorno

in pratica la violabilità dipende (anche) dallo sviluppo tecnologico:

> tener conto della "**legge di Moore**" (la velocità dei processori raddoppia ogni 18 mesi), finora valida (anche se difficilmente lo sarà in eterno)

rappresentazione numerica dell'alfabeto

per convenzione, senza perdita di generalità:

> si assume che l'alfabeto del **testo in chiaro** consti delle **26 lettere maiuscole** dell'alfabeto inglese
>
> si rappresenta il **testo cifrato** con le lettere **minuscole** dello stesso alfabeto
>
> in luogo delle lettere alfabetiche si adoperano spesso corrispondenti valori numerici interi, **da 0 a 25** (ciò è conveniente perché la grande maggioranza degli algoritmi in questo campo opera trasformazioni matematiche nell'**aritmetica modulo N**, dove **N** è la dimensione dell'alfabeto), dunque:
>
> A = 0, B = 1, C = 2, ..., Z = 25