Università degli Studi di Verona

Crittografia

Riassunto dei principali argomenti

Davide Bianchi

October 7, 2018

Contents

1 Introduzione **2**

2 Cifrari di base **2**

2.1 Cifrario di Cesare 2

2.2 Permutazione casuale 3

1 Introduzione

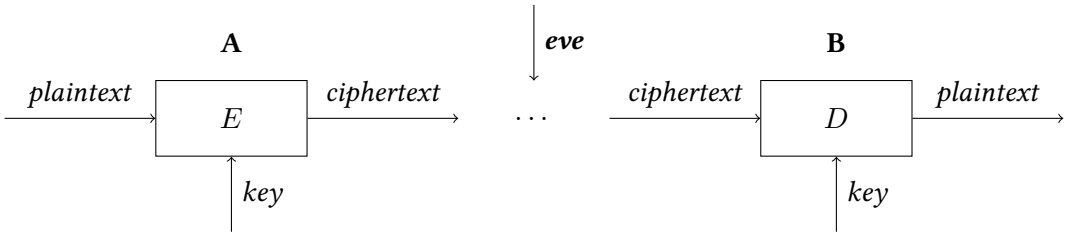
Iniziamo dando alcune definizioni fondamentali. Si useranno i termini *ciphertext* e *plaintext* per indicare rispettivamente il testo cifrato e quello in chiaro.

Definizione 1.0.1 (Crittografia) *Insieme dei metodi per rendere un messaggio non leggibile ad altri.*

Definizione 1.0.2 (Steganografia) *Insieme dei metodi per nascondere l'esistenza di un messaggio in un altro contenuto.*

Definizione 1.0.3 (Crittoanalisi) *Analisi del ciphertext per ottenere il plaintext corrispondente.*

Un generico sistema crittografico è strutturato come:



dove:

- **A** e **B** sono i due enti che si devono scambiare il messaggio cifrato;
- ***eve*** è un terzo che tenta di decrittare il messaggio;
- E e D sono i sistemi di *encrypt* e *decrypt*;
- i 3 punti (. . .) rappresentano il mezzo impiegato per la trasmissione del messaggio (qualunque esso sia).

Ovviamente, per *eve*, che tenta di decrittare il messaggio, non ha senso tentare di insistere se il costo della decrittazione è maggiore del valore dell'informazione da proteggere. In tal senso il sistema di cifratura è "sicuro".

La funzione E, inoltre, per essere sufficientemente affidabile, deve essere invertibile (in caso contrario non si potrebbe decrittare il messaggio), ma deve essere difficile fare ciò (in tal caso si dice che E è una *one-way function*). Con la chiave la funzione diventa facile anche da invertire (*one-way trapdoor*).

2 Cifrari di base

2.1 Cifrario di Cesare

Il messaggio viene cifrato sostituendo ogni lettera l del messaggio con la $l + k$ esima lettera dell'alfabeto; la chiave quindi è data dalla coppia $(l, l + k)$.

Il cifrario di Cesare è facile da attaccare in quanto basta un attacco *bruteforce*, quindi è sufficiente provare tutte le combinazioni (che sono in totale 26).

2.2 Permutazione casuale

Supponiamo di usare come cifrario una permutazione casuale dell'alfabeto, ovvero sostituendo ad ogni lettera dell'alfabeto un'altra lettera, in modo totalmente casuale. In tal caso l'attacco bruteforce richiederebbe tempo eccessivo (ci sono 26! pssibili combinazioni da provare, che sono decisamente troppe).

La tecnica usata per attaccare questo tipo di crittografia è l'*analisi delle frequenze*, ovvero l'analisi delle lettere che capitano di più in una data lingua, e associare la lettera del messaggio cifrato con una data frequenza con quella nella lingua del messaggio con una frequenza simile.