Crittografia e Combinatoria

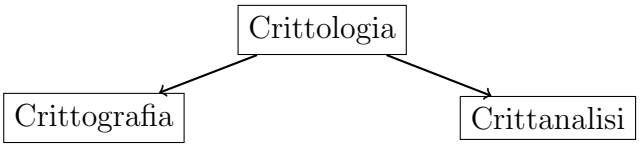
Amati Pierluigi

24 febbraio 2020

Indice

1 Introduzione

La **crittologia** è lo studio dei metodi per mantenere sicure le comunicazioni che avvengono in un canale *non sicuro*.
Essa si suddivide in **crittografia**, che studia la progettazione di tali metodi, e **crittanalisi**, che invece si occupa di infrangerli.



In generale in una comunicazione un messaggio **m** viene cifrato all'origine attraverso un algoritmo di cifratura ENC e una chiave di cifratura $\boldsymbol{k}$ e viene decifrato alla destinazione con un algoritmo di decifratura DEC (idealmente ENC^{-1}) e una chiave di decifratura $\boldsymbol{k}$. L'algoritmo di cifratura è solitamente noto a tutte le parti, ma è la chiave ad essere segreta.

$$ENC(m, k) = c$$

$$DEC(c, k) = m$$

Ipotizzando una comunicazione tra Alice e Bob, dove entrambi possiedono le chiavi di cifratura, un soggetto esterno malintenzionato, Eve (a.k.a. Evil), potrebbe:

- leggere il messaggio;
- trovare la chiave e quindi decifrare tutti i messaggi scambiati tra Alice e Bob;
- alterare un messaggio in modo tale da far sembrare che sia effettivamente spedito da una delle due parti;
- fingersi una delle due parti.

Tipologie di cifratura Esistono principalmente due tipologie di cifratura:

- la cifratura **simmetrica**, in cui la chiave di cifratura è identica alla chiave di decifratura;
- la cifratura **asimmetrica**, in cui la chiave di cifratura (generalmente pubblica) è differente dalla chiave di decifratura (privata).

2 Teoria dei numeri

2.1 Divisibilità

Definizione *Siano $a, b \in \mathbb{N}$, con $a \neq 0$, si dice che a divide b ($a|b$) se esiste $k \in \mathbb{N}$* tale che $b = ak$. In altre parole, b è un multiplo di a.

Proprietà (dimostrazioni[1])

- $a|a$
- $a|0$
- $1|b$
- se $a|b$ e $b|c$, allora $a|c$
- se $a|b$ e $a|c$, allora $a|(sb + tc)$, con $s, t \in \mathbb{N}$

[1] [Trappe p.64]

2.2 Teorema dei numeri primi

Sia $\Pi(x)$ *la quantità di numeri primi* $< x$, definita $\Pi(x) \simeq \frac{x}{\ln(x)}$,

$$\Rightarrow \lim_{x\to\infty} \frac{\Pi(x)\ln(x)}{x}.$$

2.3 Teorema fondamentale dell'aritmetica

Enunciato *Ogni numero* $n \in \mathbb{N}$ *è un prodotto di numeri primi.*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

Si dice **fattorizzazione** la ricerca di tale insieme di numeri primi.

Definizione *Si dice Massimo Comun Divisore tra a e b, il più grande numero intero che divide a e b* $[gcd(a,b)]$.

Algoritmo di Eulero

Identità di Bezout