Crittografia :polibio

Uncini federico 5A

Che cos’è la crittografia ?

Per crittografia si intende quella tecnica che permette di "cifrare" un messaggio rendendolo incomprensibile a tutti tranne che al suo destinatario. In generale i due processi principali che vengono applicati in crittografia si dividono in "cifratura" e "codifica". La cifratura lavora sulle lettere "individuali" di un alfabeto, mentre una codifica lavora ad un livello semantico più elevato, come può essere una parola o una frase.

Tipi di crittografia

- Crittografia classica : si basa su «codici» e «cifrari». Il primo caso documentato è del 1900 A.C., riguarda gli scribi egizi e si riferisce all'uso di geroglifici non standard trovati su alcune tavole d'argilla;

- Crittografia moderna : La **crittografia moderna** nasce negli anni 70' con la scoperta dei primi algoritmi asimmetrici. Le prerogative fondamentali che la crittografia moderna garantisce sono:

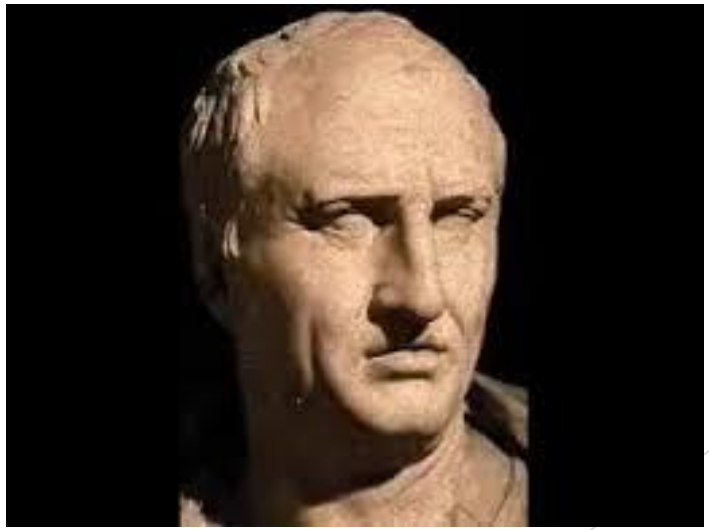
  Riservatezza :l'informazione deve essere intelligibile solo da chi ne è autorizzato.

  Integrità: deve essere possibile rilevare se l'informazione è stata alterata.

  Autenticazione: la parte autenticarsi deve dimostrare alla parte autenticante chi sostiene di essere.

Crittografia Polibio che cos’è?

Il modello di crittografia Polibio pende il nome proprio dal suo ideatore greco Polibio (~200-118AC) l'idea è quella di cifrare una lettera con una coppia di numeri compresi tra 1 e 5, in base ad una scacchiera 5x5. In tal modo il messaggio può essere trasmesso con due gruppi di cinque torce (p.es. 1,5 = una torcia accesa a destra, cinque a sinistra).



Come è composta la scacchiera di Polibio

La scacchiera originale è costituita da una griglia composta da 25 caselle ordinate in cinque righe ed altrettante colonne. Le lettere dell'alfabeto vengono inserite da sinistra a destra e dall'alto in basso. Le righe e le colonne sono numerate: tali numeri sono gli indici o "coordinate" delle lettere costituenti il messaggio in chiaro.

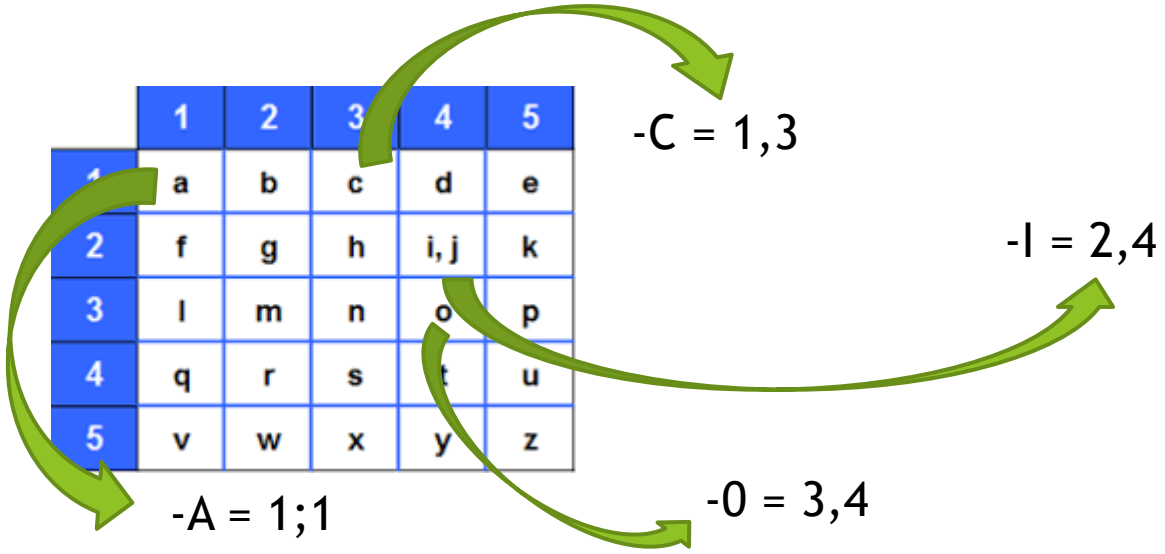
La trasposizione avviene sostituendo ad ogni lettera del messaggio un numero le cui cifre rappresentano il numero di riga e di colonna della sua posizione nella scacchiera.

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i, j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Un esempio di crittografia

Per esempio se si prende d'esempio la parola «ciao» secondo la crittografia Polibio la parola diventerà la seguente : 13241134



fonti

- Google immagini
- Enceclopedia treccani
- http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-0304/Setup_CA_linux/La%20crittografia%20moderna.htm