L'importanza della chiave nella crittografia

Crittografia e il principio di Kerckhoffs

"**Crittografia** (dal greco *kryptós*, nascosto, e *graphía*, scrittura): sistema di scrittura e trasmissione cifrata delle informazioni interpretabile solo da chi conosca il particolare artificio utilizzato".

(Enciclopedia della matematica, Garzanti Libri, 2013)

Secondo principio di Kerckhoffs:

"La sicurezza di un sistema crittografico non deve dipendere dal tenere celato l'algoritmo di cifratura, ma unicamente dalla segretezza della chiave"

"ALGORITMO"

↓

"OMTIROGLA"

Non è un algoritmo sicuro

Il cifrario di Cesare

Il **cifrario di Cesare** è un sistema a sostituzione alfabetica:

A B C D E F G H I L M N O P Q R S T U V Z

D E F G H I L M N O P Q R S T U V Z A B C

"ALGORITMO"

↓

"DOLRUNZPR"

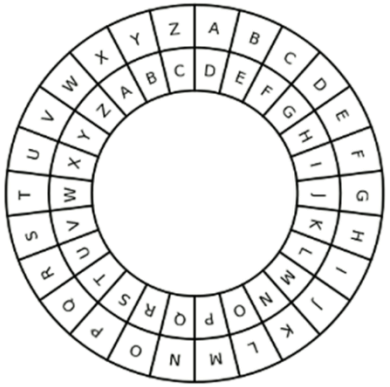
Rispetta il principio di Kerckhoffs

La chiave corrisponde al numero di lettere della traslazione. In questo caso n = 3

A	11.8 %	H	1.5 %	Q	0.5 %
B	0.9 %	I	11.3 %	R	6.4 %
C	4.5 %	L	6.5 %	S	5.0 %
D	3.7 %	M	2.5 %	T	5.6 %
E	11.8 %	N	6.9 %	U	3.0 %
F	1.0 %	O	9.8 %	V	2.1 %
G	1.7 %	P	3.0 %	Z	0.5 %

I dischi rotanti

Il **meccanismo dei dischi rotanti** è un sistema a sostituzione polialfabetica



"ALGORITMO"

↓

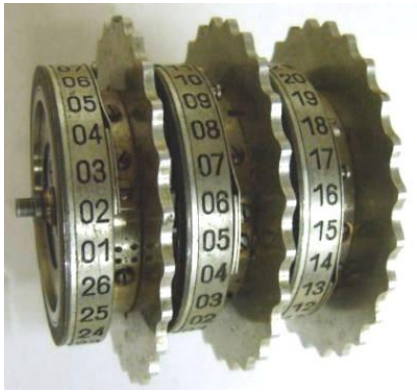
"DNHOQGQIJ"

<u>Rispetta il principio di Kerckhoffs</u>

La chiave corrisponde alla posizione iniziale dei due dischi. In questo caso la lettera A coincide con il carattere D

La macchina Enigma

La **macchina Enigma** è un sistema a sostituzione polialfabetica simile a quello dei dischi rotanti



La chiave corrisponde alla configurazione iniziale dei tre rotori.

Sono disponibili **26^3=17576** chiavi

La crittografia a chiave pubblica

- **Chiave pubblica**: nota a tutti, viene utilizzata unicamente per crittare il messaggio.
- **Chiave privata**: nota solo al ricevente, permette di decifrare i messaggi crittati con la chiave pubblica.

Il **metodo RSA** è un metodo a chiave pubblica basato su un problema matematico complesso

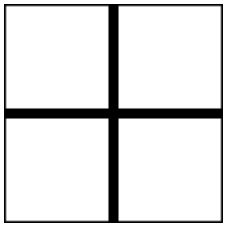
Chiave privata: $p_1 , p_2 , \dots , p_k$

Chiave pubblica: $n = \prod_{i=1}^{k} p_i$

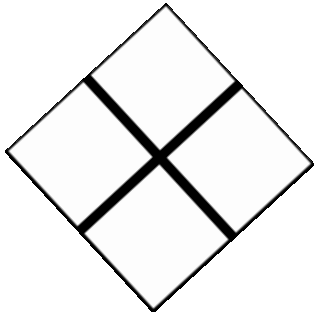
Numero di cifre	Tempo
20	24 minuti
50	4 ore
100	74 anni
200	4×10^9 anni
1000	3×10^{43} anni

Il trasferimento quantistico

Il **protocollo BB84** è un metodo crittografico che garantisce a mittente e ricevitore la possibilità di scambiarsi la chiave in modo sicuro attraverso un canale quantistico.



Risultato corretto



Risultato causale