

# Crittografia: Passato, Presente e Futuro

## Dal Cifrario di Cesare alla Crittografia Quantistica

Candidato: Domenico Di Fina



Tutor: Prof.ssa Elena Toscano

### SOMMARIO

Nel corso della storia la Crittografia si è arricchita di strumenti per trasformare un messaggio in chiaro in uno cifrato, tra cui il Cifrario di Cesare, il Cifrario di Vigenère ed Enigma, la quale fu decifrata da Alan Turing durante la Seconda Guerra Mondiale.

Oggi, uno degli algoritmi più utilizzati è RSA, che si basa sul problema della Fattorizzazione degli Interi.

Negli ultimi anni sono state presentate nuove proposte crittografiche tra cui il sistema EverCrypt e la Crittografia Quantistica.

### ILLUSTRAZIONI

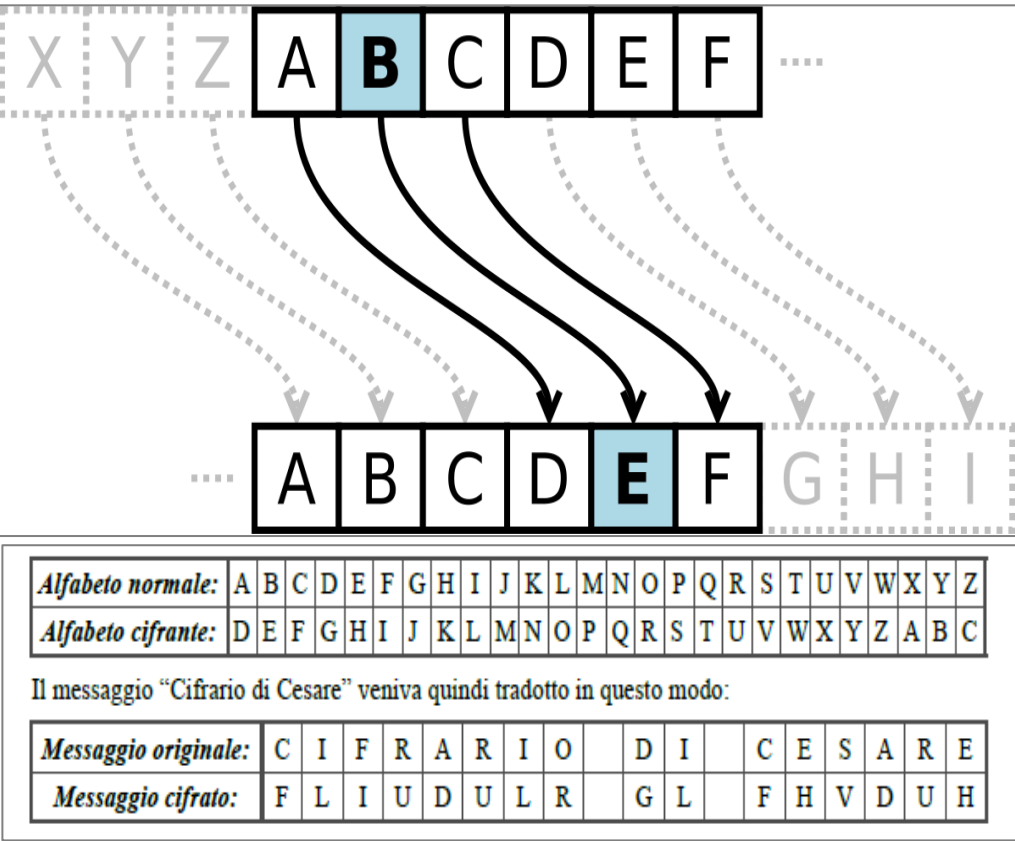


Figura 1. Cifrario di Cesare

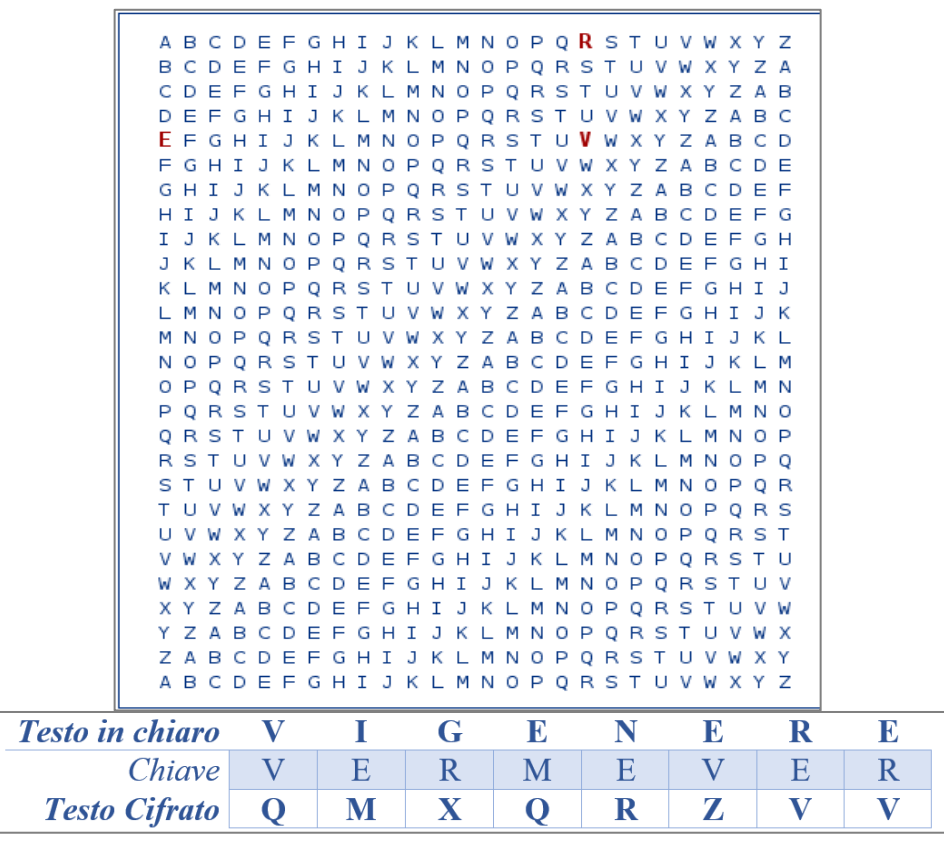


Figura 2. Cifrario di Vigenère



Figura 3. Macchina Enigma

**IL CRITOSISTEMA RSA**

Operazione di cifratura:  $C \equiv M^e \pmod{n}$ , dove C è il messaggio cifrato.

Operazione di decifratura:  $M \equiv C^d \pmod{n}$ , dove M è il messaggio in chiaro.

**SCELTA DELLE CHIAVI**

Dati due numeri primi p e q abbastanza grandi  $\rightarrow n = p \cdot q$ , dove n è detto modulo.

Si sceglie un intero casuale e grande e per cui  $M.C.D(e, (p-1) \cdot (q-1)) = 1$ .

L'intero d è calcolato a partire da p, q ed e  $\rightarrow e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$ .

Figura 4. Scelta delle Chiavi per RSA

**IL CRITOSISTEMA RSA**  
DIMOSTRAZIONE DI CORRETTEZZA

Per il teorema di Eulero  $M^{\phi(n)} \equiv 1 \pmod{n}$ .

Sapendo inoltre che  $e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$  e utilizzando le operazioni viste in precedenza abbiamo:

$$M^{e \cdot d \pmod{(p-1) \cdot (q-1)}} \equiv M^{k \cdot \phi(n) + 1} \pmod{n}.$$

Pertanto,

$$M^{k \cdot \phi(n) + 1} \pmod{n} = M \cdot M^{k \cdot \phi(n)} \pmod{n}.$$

Infine, per il teorema di Eulero:

$$M \cdot (M^{\phi(n)})^k \pmod{n} = M \cdot (1)^k \pmod{n} = M \pmod{n}.$$

Figura 5. Dimostrazione di Correttezza per RSA

**CRITTOANALISI**  
ATTACCHI POSSIBILI SU RSA

- Forza bruta:** provare tutte le chiavi possibili;
- Attacchi matematici:** basati sulla fattorizzazione intera, dove un esempio è l'algoritmo di Fermat:  
Sia n un intero dispari:  
1.  $a = \sqrt{n}$  (considerando la parte intera superiore).  
Finché  $b_1$  non è un quadrato perfetto si ripete:  
2.  $b_1 = a^2 - n$ ;  
3. se  $b_1$  non è un quadrato perfetto allora  $a = a + 1$ ;  
4.  $b = \sqrt{b_1}$ ;  
5.  $n = (a - b)(a + b)$ .
- Attacchi a tempo:** misurazioni precise sul tempo di esecuzione;
- Attacchi con testo cifrato scelto:** utilizzare la chiave pubblica per decifrare alcuni testi cifrati così da ottenere informazioni utili.

Figura 6. Crittoanalisi – Attacchi ad RSA

**CRITTOGRAFIA DEL FUTURO**  
IL PROTOCOLLO BB84

Base	0	1
+	↑	↔
×	↙	↘

- Alice invia tramite canale quantistico fotoni con una polarizzazione tra le quattro possibili (0°, 45°, 90° e 135°);
- Bob sceglie una delle due basi per la misurazione;
- Entrambi scartano le basi divergenti così da ottenere una chiave comune ad entrambi.

Figura 7. Protocollo BB84

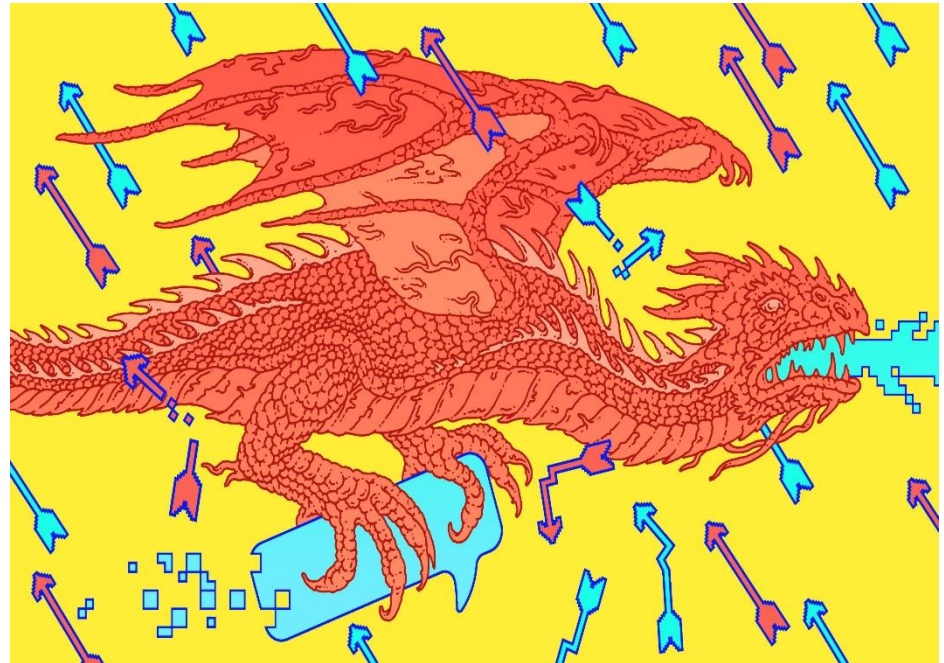


Figura 8. EverCrypt

### OBIETTIVO

L'obiettivo di questo elaborato è stato quello di fornire una panoramica generale della crittografia del passato, illustrando i principali cambiamenti crittografici avvenuti nel corso della storia, del presente, analizzando i principali algoritmi a chiave pubblica e privata ancora oggi utilizzati, e del futuro, sottolineando le nuove proposte crittografiche come la crittografia quantistica o il sistema EverCrypt.

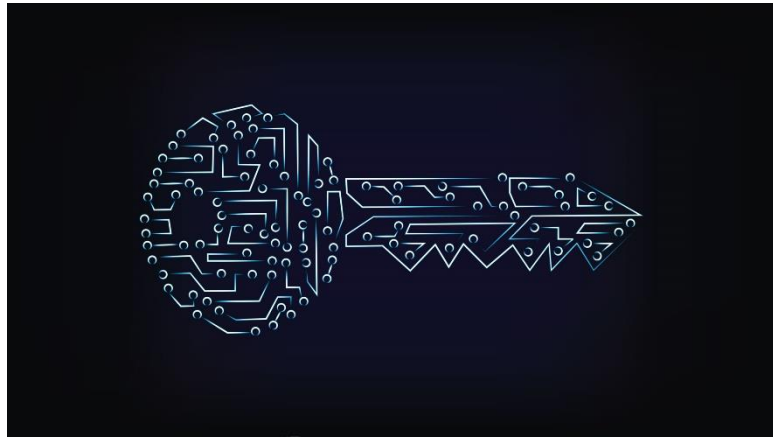
L'attenzione è stata rivolta all'algoritmo a chiave pubblica RSA che risulta ancora oggi sicuro ed utilizzato.

### CONCLUSIONI

La storia della crittografia si intreccia notevolmente con la storia dell'uomo, da sempre quest'ultimo ha cercato di nascondere i propri messaggi, difatti la comunicazione, in particolare quella segreta, ha rivestito e riveste tutt'oggi un importante ruolo per l'umanità.

Ultimamente la crittografia è diventata, in misura sempre maggiore, di dominio pubblico, è possibile infatti utilizzare software crittografici in grado di garantire la segretezza dei propri dati.

La crittografia, in particolare negli ultimi decenni, ha costituito una importante sfida intellettuale per molti ricercatori. Questa componente di sfida deriva dalla necessità continua di trovare nuovi sistemi che garantiscano sempre una maggiore sicurezza e, al contempo, dalla consapevolezza del fatto che questi, per quanto sicuri siano, potranno sempre essere messi in crisi soprattutto dall'evoluzione delle macchine, sempre più potenti nel portare attacchi sempre più evoluti.



### RIFERIMENTI

#### BIBLIOGRAFIA

R.L. Rivest, Adi Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* (1977).

Whitfield Diffie, Martin E. Hellman, *New Directions in Cryptography* (1976).

Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1987.

John F. Dooley, *A Brief History of Cryptology and Cryptographic Algorithms*, Springer, 2013.

M.W. Baldoni, C. Ciliberto, G.M. Piacentini Cattaneo, *Aritmetica, Crittografia e Codici*, Springer, 2007.

Richard A. Mollin, *RSA and Public-Key Cryptography*, Chapman & Hall/CRC, 2003.

Lynn M. Batten, *Public Key Cryptography, Applications and Attacks*, Wiley, 2013.

Dario Sangiovanni, Luca Del Basso, Enrico Gasperoni, *Crittografia Quantistica*, 2015,

<http://www.dia.uniroma3.it/~dispense/merola/critto/tesine/quantistica.pdf>