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.

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.

ILLUSTRAZIONI

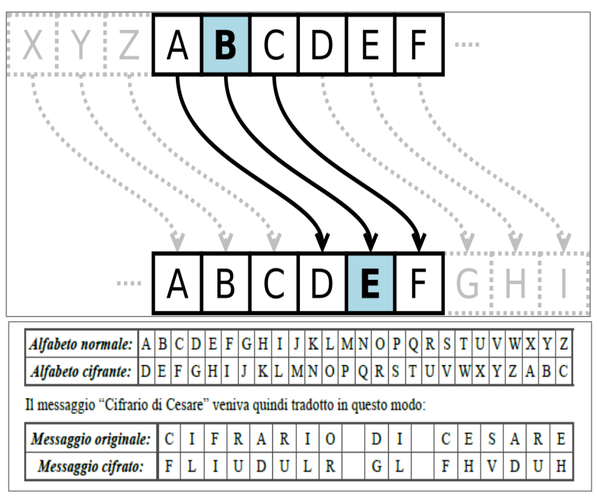


Figura 1. Cifrario di Cesare

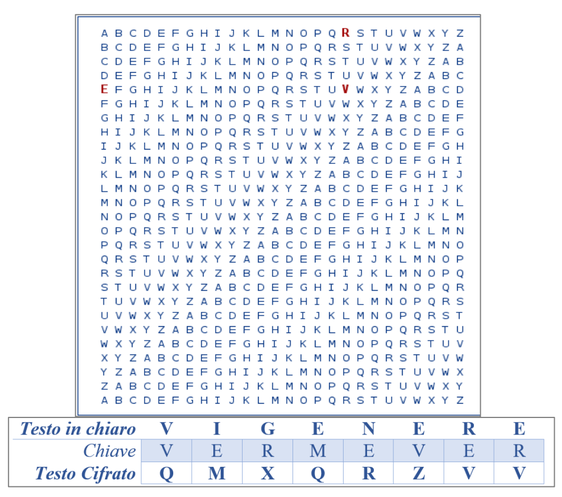


Figura 2. Cifrario di Vigenère

Figura 3. Macchina Enigma

Figura 4. Scelta delle Chiavi per RSA

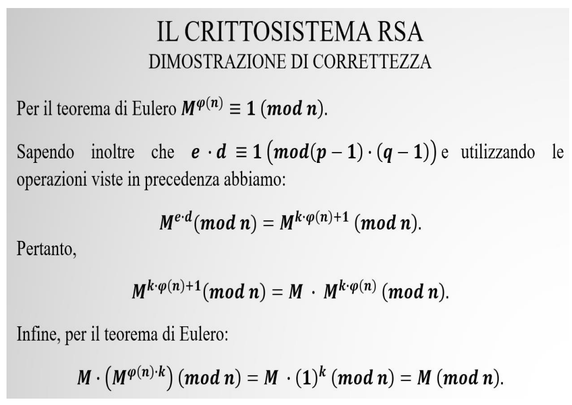


Figura 5. Dimostrazione di Correttezza per RSA

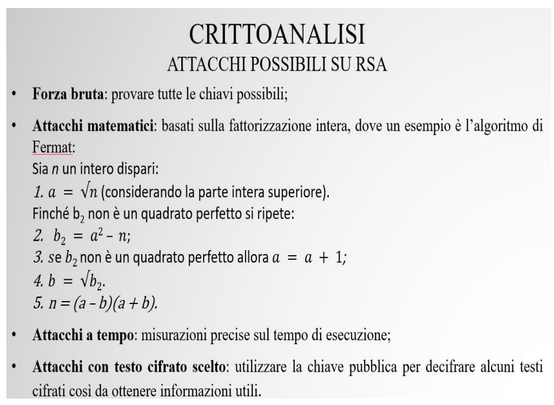


Figura 6. Crittoanalisi – Attacchi ad RSA

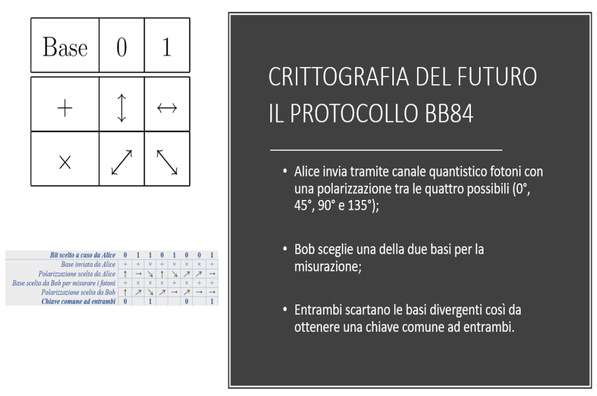


Figura 7. Protocollo BB84

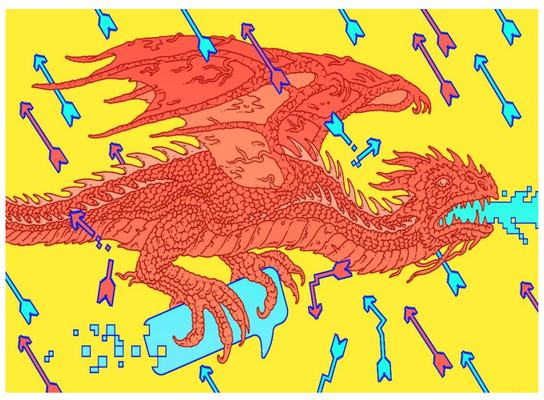


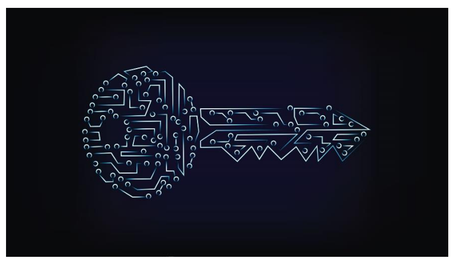
Figura 8. EverCrypt

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* (1997).

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