Learning Friday

Crittografia

Alberto Bellemo Bullo

Crittografia

(dall'unione di due parole greche: κρυπτός (*kryptós*) che significa "nascosto", e γραφία (*graphía*) che significa "scrittura")

Branca della crittologia che tratta delle "scritture nascoste"

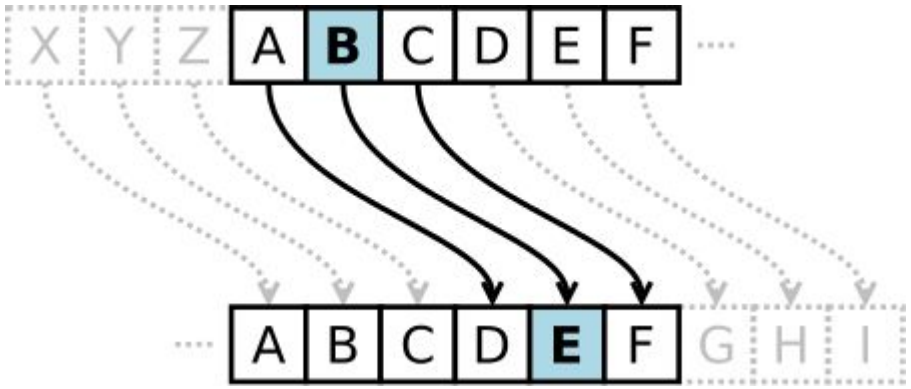
Tale messaggio si chiama **crittogramma**

Un pò di storia

Tracce di cifrari antichi quanto gli Ebrei con il loro codice di atbash

Gli Spartani utilizzavano la scitala

Gaio Giulio Cesare si attribuisce l'uso del cosiddetto cifrario di Cesare



usato anche da Bernardo Provenzano

La crittografia moderna inizia con la stesura del *De cifris* di Leon Battista Alberti

Nel 1949 Claude Shannon affronta il tema della crittologia dal punto di vista della teoria dell'informazione (**Communication Theory of Secrecy Systems**)

Cifrario di Vernam

Il cifrario di Vernam è l'unico sistema crittografico la cui sicurezza sia comprovata da una dimostrazione matematica e per questo si è guadagnato il titolo di "cifrario perfetto".

La sua forma più classica è quella in cui la chiave ha la stessa forma del testo (a ogni lettera viene associato il numero corrispondente A=0 B=1 C=2) e che sfrutta l'operazione di somma circolare (quella per cui dopo la lettera Z c'è di nuovo la lettera A, quindi A+C=0+2=2=C, B+C=1+2=3=D, Z+C=25+2=27->1=B, Z+Z=25+25=50->24=Y).

È tuttavia molto diffusa, specialmente nell'ambiente informatico, la forma che fa utilizzo dell'operazione logica XOR (disgiunzione esclusiva), che del resto non è altro che l'addizione circolare dei singoli bit.

Fu usato, intensivamente, durante la Guerra Fredda, da spie della CIA e del KGB, ma anche dalla cosiddetta Linea Rossa, il famoso collegamento telefonico diretto Washington-Mosca.

Esempio Cifrario di Vernam

Supponiamo, di dover trasmettere la parola "RANA". A ogni carattere della parola, si associa un numero, in base alla sua posizione sull'alfabeto tra 1 e 26. (a=1 ... z=26)

Utilizziamo poi, la chiave casuale K "AMID" (che ha lo stesso numero di caratteri della parola), ecco che, se utilizziamo la funzione somma, otteniamo una cosa di questo tipo:

R	A	N	A	
18	1	14	1	+
A	M	I	D	
1	13	9	4	=
S	N	W	E	

Il destinatario, dovrà utilizzare il processo inverso, andando a sottrarre a "SNWE", "AMID" ed otterrà, finalmente, "RANA".

E’ solo questione di tempo

Tranne che per il cifrario di Vernam (CIFRARIO PERFETTO), tutte le altre tecniche rendono sicuro il dato solo per un certo arco temporale e non possono garantire la durata della segretezza

ENIGMA

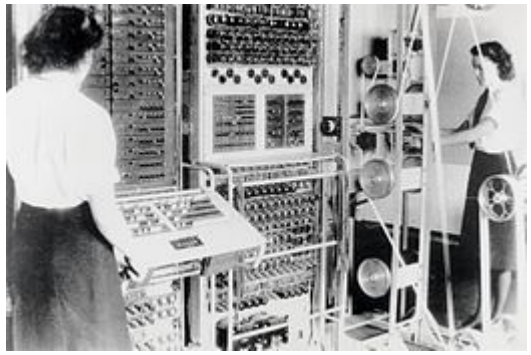
Enigma fu una macchina elettro-meccanica per cifrare e decifrare messaggi.

$$100\,391\,791\,500 \times 6 \times 17\,576 \approx 10^{16}$$

(10 milioni di miliardi di combinazioni possibili)

Il romanzo *Enigma* di Robert Harris ruota intorno al ruolo di Enigma nel contrasto all'azione dei sommergibili tedeschi durante la seconda guerra mondiale

Il **Colossus** è stato il primo computer elettronico programmabile nella storia dell'informatica. Costruito e messo in opera nel Regno Unito, durante la seconda guerra mondiale, fu in grado di forzare i codici sviluppati dalla cifratrice Lorenz SZ 40/42 usata dai nazisti per proteggere la corrispondenza fra Adolf Hitler e i suoi capi di stato maggiore, oltre che alle comunicazioni *Purple* e *Red* giapponesi, basate sulla tecnologia di Enigma. I servizi segreti britannici fecero di tutto per interpretare i codici dei nazisti, che però venivano cambiati quotidianamente.



Alan Mathison Turing (Londra, 23 giugno 1912 – Wilmslow, 7 giugno 1954) è stato un matematico, logico e crittografo britannico, considerato uno dei padri dell'informatica e uno dei più grandi matematici del XX secolo.

Tipi di crittografia

Simmetrica

AES - *Advanced Encryption Standard*

DES - *Data Encryption Standard*

La crittografia asimmetrica

RSA - Nel 1976 Whitfield Diffie e Martin E.Hellman, un matematico e un ingegnere in forza alla Stanford University, introducono l'utilizzo della chiave pubblica per la crittazione e l'autenticazione; nell'anno seguente il gruppo di ricerca del MIT formato da Ronald L. Rivest, Adi Shamir e Leonard M. Adleman realizza il primo sistema a chiave pubblica, in questo modo viene ideato l'algoritmo RSA

La crittografia quantistica

Un cifrario di Vernam che si basa sull'utilizzo della meccanica quantistica nella fase dello scambio della chiave

Applicazioni

WIFI - WEP e WPA

SSH

SSL/TLS

HTTPS

IPSEC

Nelle transazioni bancarie

Pay per view

- Irdeto
- Nagravision (mediaset)
- SECA (Tele+, Canal+)
- Viaccess
- Videoguard (Sky Italia)

Sw Per la crittografia

Un elenco esemplificativo di alcuni software che a qualche titolo utilizzano crittografia:

- BitLocker Drive Encryption
- CrypTool
- *GNUpg*, *gnupg.org*.
- **PGP**
- ProtonMail
- FreeOTFE
- Telegram
- Tresorit
- TrueCrypt
- VeraCrypt
- WhatsApp

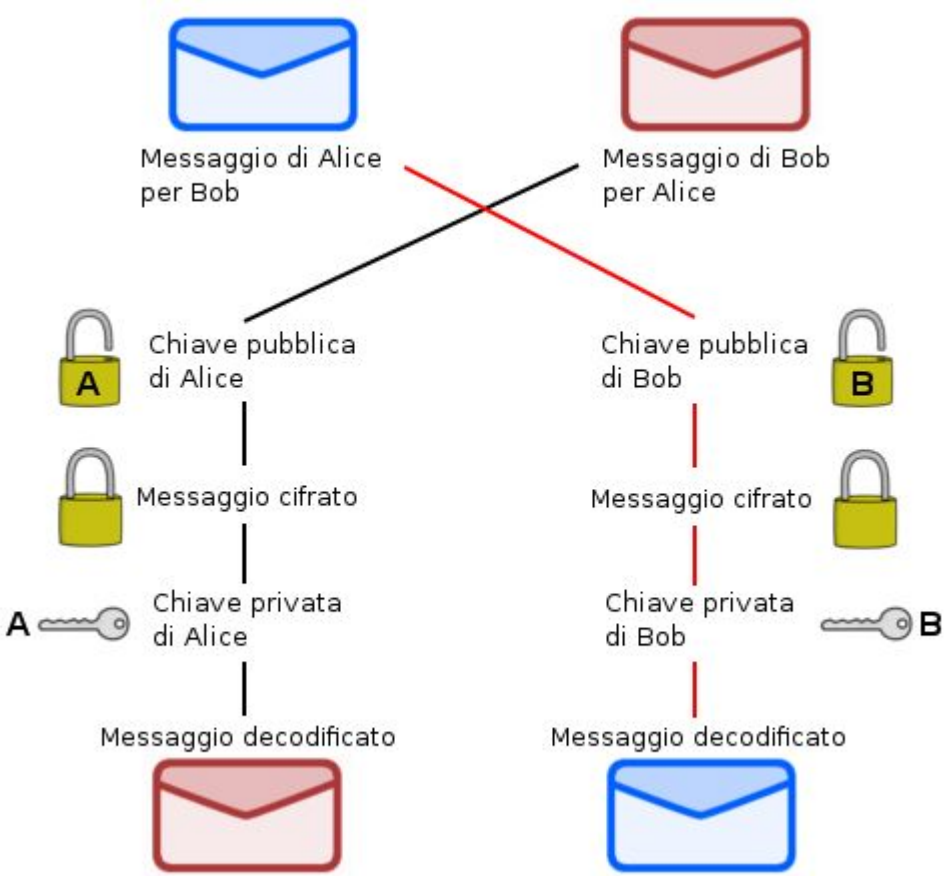
Crittografia asimmetrica

Coppia di chiavi :

- Pubblica
- Privata

La chiave pubblica deve essere distribuita

La chiave privata rimane al proprietario



Crittografia asimmetrica

A causa del peso computazionale della crittografia asimmetrica, essa di solito è usata solo per piccoli blocchi di dati, in genere il trasferimento di una chiave di cifratura simmetrica (per esempio una chiave di sessione). Questa chiave simmetrica è utilizzata per cifrare messaggi lunghi. La cifratura/decifratura simmetrica è basata su algoritmi semplici ed è molto più veloce. L'autenticazione del messaggio include hashing del messaggio per produrre un "digest" (risultato dell'output dell'algoritmo di hash), e crittografando il digest con la chiave privata per produrre una firma digitale.

1. calcolando l'hash del messaggio;
2. decifrando l'hash del messaggio;
3. confrontando la firma del messaggio.

L'uguaglianza tra i digests conferma che il messaggio non è stato modificato da quando è stato firmato, e che il firmatario, e nessun altro, intenzionalmente abbia eseguito l'operazione di firma, presumendo che la chiave privata del firmatario è rimasta segreta. La sicurezza di questo tipo di procedura dipende dall'algoritmo di hash di questa data qualità che è computazionalmente impossibile modificare o trovare un messaggio sostituito che produca lo stesso digest, ma gli studi hanno dimostrato che con gli algoritmi MD5 e SHA-1, produrre un messaggio alterato o sostituito non è impossibile. L'attuale standard di hash per la crittografia è SHA-2. Lo stesso messaggio può essere usato al posto del digest.

Public-Key Cryptography Standards

PKCS -7 Standard della sintassi per firmare un messaggio in una infrastruttura a chiave pubblica PKI

PKCS - 10 Standard per la sintassi della certificazione (Certification Authority)

Data Encryption Standard

Sviluppato nel 1970

Algoritmo a chiave simmetrica

Soli 56 bit

Nel 1999 decriptato in sole 22 ore e 15 minuti

3 DES

Fondamentalmente applica l'algoritmo DES 3 volte

Quindi chiave da 56 bit * 3 = 168 bit

Comunque attaccabile

DES Challenges

Gara per decriptare l'algoritmo DES

1998 - prima decriptato in 39 giorni

1998 - decriptato in 56 ore

1999 - decriptato in 22 ore e 15 minuti

Advanced Encryption Standard

anche conosciuto come **Rijndael**

Algoritmo a chiave simmetrica

chiavi lunghe 128, 192 e 256 bit

Decrittato con successo nel 2006

In uno dei famosi documenti di Snowden si indicava che la NSA aveva sviluppato un attacco crittografico proprio per decriptare l'AES

Algoritmo a chiave **asimmetrica**

Per ottenere una discreta sicurezza è necessario utilizzare chiavi binarie di almeno 2048 bit.

Le chiavi a 1024 bit, ancora oggi largamente utilizzate, non sono più consigliabili

Nel 2005 un gruppo di ricerca riuscì a scomporre un numero di 640 bit (193 decimali) in due numeri primi da 320 bit, impiegando per cinque mesi un cluster Opteron con 80 processori da 2,2 GHz, potenzialmente decifrando un messaggio codificato con RSA-640.

RSA è computazionalmente impegnativo

RSA - Secret-Key Challenge

Serie di contest per decriptare l'RSA

RC5-32/12/7 was completed on 19 October 1997, with distributed.net finding the winning key in 250 days and winning the US$10,000 prize. The recovered plaintext was: *The unknown message is: It's time to move to a longer key length*.

RC5-32/12/8 also carried a US$10,000 prize and was completed by distributed.net on 14 July 2002. It took the group 1,757 days to locate the key, revealing the plaintext: *The unknown message is: Some things are better left unread*.

https://www.emc.com/emc-plus/rsa-labs/historical/status-and-prizes.htm

SECURE HASH ALGORITHM

Impronta del messaggio

SHA - 1 digest di 160 bit

Violato

SHA -2

1. **SHA-224**
2. **SHA-256**
3. **SHA-384**
4. **SHA-512**

SHA1("Cantami o diva del pelide Achille l'ira funesta")
= 1f8a690b7366a2323e2d5b045120da7e93896f47

SHA1("C**o**ntami o diva del pelide Achille l'ira funesta")
= e5f08d98bf18385e2f26b904cad23c734d530ffb

Concorso per SHA -3 gradualmente verrà utilizzato

Il 23 febbraio 2017 un team di Google ha annunciato la prima tecnica pratica per generare una collisione