CRITTOGRAFIA

Introduzione

Il termine “Crittografia” deriva dalle parole greche **κρυπτός** [kryptós], "nascosto", e **γραφία** [graphía], "scrittura".

La funzione della crittografia è quella di comunicare un messaggio da una persona ad un’altra (o tra due gruppi di persone), facendo sì che nessun altro al di fuori delle due persone coinvolte riesca a comprenderne il significato.

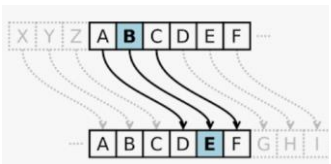
La crittografia ha origini antichissime, possiamo dire che nasce con la comunicazione stessa. Oggi la crittografia ha un valore strategico nel mondo del web. Data la sua complessità, la crittografia moderna cade quasi interamente nell’alveo della matematica e in particolare nella branca della scienza degli algoritmi.

Apparentemente potrebbe sembrare che una comunicazione sicura sia una cosa lecita per proteggersi dagli impiccioni malvagi, ma in quest’ambito la distinzione tra “buoni” e “cattivi” non è sempre stabilita. E’ ovvio che una transazione finanziaria di tipo home banking debba impedire ai truffatori di dirottare il denaro in conti diversi da quello del proprietario. Si pensi invece alle comunicazioni cifrate fra nazisti durante la seconda guerra mondiale; se gli inglesi non avessero capito gli algoritmi e interpretato correttamente tali messaggi, la guerra si sarebbe protratta ancora a lungo.

La crittografia, per esistere, ha dunque sempre bisogno di due attori: chi vuole cifrare un messaggio e chi vuole capire tale messaggio pur non essendone il destinatario. Questi due mondi si autoalimentano e il loro antagonismo permette alla crittografia di evolversi continuamente verso una complessità sempre maggiore.

Cenni storici

Il principale uso della crittografia in tempi antichi era quello militare. Tra le prime testimonianze di messaggi cifrati si ha con l’uso della **scitale** a Sparta nel V sec. a.C. La scitale è un’asta cilindrica sulla quale veniva avvolta una fettuccia con impresso il messaggio. Svolta la fettuccia dal cilindro il messaggio era indecifrabile. Il destinatario del messaggio aveva una scitale dotata di stesso raggio del mittente e così poteva ricostruire il messaggio riavvolgendo la fettuccia. In questo caso la chiave per cifrare/decifrare il messaggio è il raggio del cilindro.



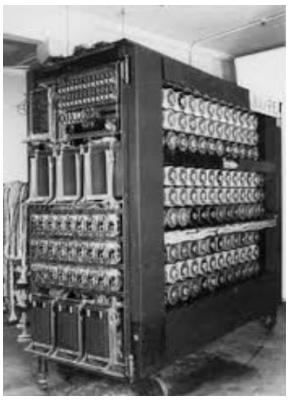
Il più noto esempio di crittografia in epoca antica è però il **cifrario di Cesare**, perché è il primo che ha caratteristiche moderne. Se ne parla nel *De Bello Gallico* e viene spiegato dallo storico Svetonio. Ogni lettera viene sostituita dalla terza successiva. Si considera un alfabeto circolare. L’algoritmo è molto semplice, ma per quei tempi era sufficiente.

I principali cifrari storici sono di due tipi:

Cifrari a sostituzione: come il cifrario di Cesare.

Cifrari a trasposizione: più complessi, ma più sicuri. In questi si suddivide il messaggio in più parti e si applica una regola di trasposizione ad ogni gruppo di caratteri.

Di particolare importanza storica è la macchina **Enigma**. Essa veniva usata dall'esercito tedesco e fu impiegata durante la seconda guerra mondiale. Era una macchina molto complessa per i suoi tempi. Durante il periodo bellico un gruppo di crittoanalisti inglesi, guidati dal matematico **Alan Turing** (1912-1954), furono reclutati per decifrare i messaggi dei militari tedeschi. Il luogo operativo era **Bletchley Park**, una località vicino Londra, e l'operazione in codice era denominata **Ultra**. Tra i crittoanalisti erano presenti matematici, giocatori di scacchi ed esperti di cruciverba. Venuti in possesso di una delle macchine enigma, il gruppo di studiosi riuscì, tramite la costruzione di calcolatori, a decifrare i messaggi dei tedeschi. Grazie a questi primi calcolatori e ai suoi studi giovanili, Turing è ricordato come il padre dell'informatica. Il film "**The imitation game**" narra tali vicende.



L'era di internet

Internet ha amplificato a dismisura l'utilizzo della crittografia. Oltre agli usi militari, in internet si fa uso della crittografia in ogni ambito, dalla firma elettronica, alla trasmissione di dati anagrafici, alle transazioni finanziarie, agli usi governativi, ecc.

Per affrontare la crittografia in internet è necessario dare alcune definizioni.

L'oggetto di studio della Crittologia è il seguente:

*un mittente (**Mitt**) vuole comunicare con un destinatario (**Dest**) un messaggio (**m**) utilizzando un canale di trasmissione insicuro, cioè tale che altri (crittoanalisti **X**) possano capire o alterare il messaggio. Il messaggio m viene codificato dal mittente con un crittogramma (**c**). Il destinatario decodifica il crittogramma c ottenendo il messaggio originale.*

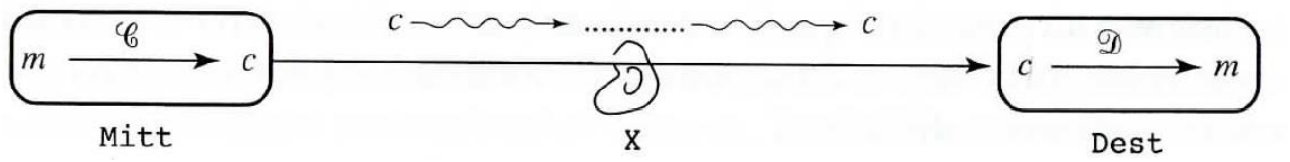
Sia **M** l'insieme di tutti i messaggi possibili, dunque m ∈ M.

Sia **C** l'insieme di tutti i crittogrammi possibili, dunque c ∈ C

Cifratura del messaggio: funzione che trasforma un messaggio m in un crittogramma c. $\mathscr{C}$: M ⟶ C

Decifratura del messaggio: funzione che trasforma un crittogramma c in un messaggio m. $\mathscr{D}$: C ⟶ M

$\mathscr{C}$ e $\mathscr{D}$ sono una la funzione inversa dell'altra, quindi $\mathscr{D}(\mathscr{C}(m))= m$



Il crittoanalista X può agire in due modi: passivo o attivo. Il comportamento passivo significa che si limite ad ascoltare come succede per esempio nello spionaggio industriale. Il comportamento attivo significa che altera o disturba la comunicazione. Il crittoanalista riesce nel suo intento se viene a conoscenza della funzione $\mathscr{D}$.

Per un discorso di praticità la crittografia informatica deve trovare un equilibrio tra velocità di cifratura e robustezza dell'algoritmo. Sebbene infatti i computer moderni siano dotati di elevatissime velocità computazionali, impiegherebbero comunque troppo tempo se la cifratura fosse troppo complicata. D'altro canto questa deve essere piuttosto robusta per impedire che venga forzata in tempi ragionevoli. Qui entrano in scena i matematici/informatici che di volta in volta devono inventare algoritmi sempre più complessi, ma più leggeri possibile.

In internet, allo scopo di garantire comunicazioni crittate tra tantissime persone, non si tengono segrete la $\mathscr{C}$ e $\mathscr{D}$, ma la **chiave** (**k**) che, inserita nel processo di cifratura e decifratura, impedisce comunque a X di conoscere il messaggio. Si parlerà allora di $\mathscr{C}$(m,k) e $\mathscr{D}$(c,k). La chiave di cifratura

è molto più leggera rispetto a tutta la funzione di Cifratura e quindi più pratica da generare e trasmettere.

Facciamo un esempio. Supponiamo che una chiave sia composta da 20 cifre e che un potente calcolatore impiegasse un milionesimo di secondo per calcolare $\mathscr{D}$(c,k) e verificarne la significatività, occorrerebbe circa un milione di anni per provare tutte le chiavi possibili.

La crittografia a chiave si distingue in due tipi:

1. sistemi a chiave segreta o simmetrici
2. sistemi a chiave pubblica o asimmetrici

Nel primo tipo esiste una sola chiave che serve sia al mittente che al destinatario. Il vantaggio è che è un sistema veloce, ma ha lo svantaggio di dover comunicare la chiave tra i due agenti.

Nel secondo tipo esistono due chiavi, una **pubblica** e una **privata**. Il messaggio viene cifrato da una chiave pubblica, conosciuta da tutti, ma solo il destinatario ha la chiave privata per decifrare il messaggio.

Questo sistema fu introdotto da Whitfield Diffie, Martin Hellman e indipendentemente da Ralph Merkle nel 1976.

Il più noto sistema di crittografia asimmetrica è l'algoritmo **RSA**, dal nome degli inventori Ronald **Rivest**, Adi **Shamir** e Leonard **Adleman**, formalizzato nel 1977. L'algoritmo RSA si basa su due concetti fondamentali della matematica: l'**aritmetica modulare** e i **numeri primi**. La prima fu inventata da Gauss che la tratta nella sua opera principale ***Disquisitiones Arithmeticae*** del 1801. Le *Disquisitiones Arithmeticae* costituiscono l'opera che dà il via alla teoria dei numeri. L'aritmetica modulare viene chiamata anche aritmetica dell'orologio. Infatti 9+4=1 sembrerebbe falsa, ma se si considerano i numeri come ore, il conto torna! I numeri primi entrano nella crittografia perché si è scoperto che trovare il risultato della moltiplicazione tra due numeri primi è semplice, per esempio 29 x 37 = 1073. Molto meno semplice è il viceversa, cioè scomporre un numero nel prodotto di due primi. Si provi ad esempio a scomporre 202417.

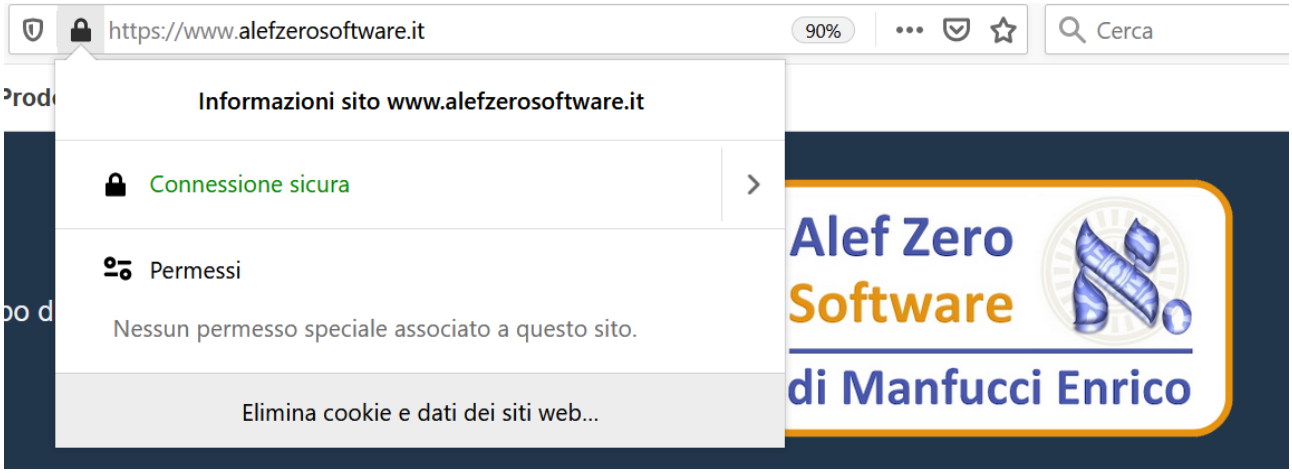
Il metodo per la generazione delle chiavi è il seguente (da wikipedia in sitografia):

1. si scelgono a caso due numeri primi, p e q abbastanza grandi da garantire la sicurezza dell'algoritmo (ad esempio, il più grande numero RSA, RSA-2048, utilizza due numeri primi lunghi più di 300 cifre)
2. si calcola il loro prodotto $n = pq$, chiamato *modulo* (dato che tutta l'aritmetica seguente è modulo n), e il prodotto $\varphi(n) = (p-1)(q-1)$, dove $\varphi(n)$ è la funzione toziente
3. si considera che la fattorizzazione di ***n*** è segreta e solo chi sceglie i due numeri primi, ***p*** e ***q***, la conosce
4. si sceglie poi un numero e (chiamato *esponente pubblico*), coprimo con $\varphi(n)$ e più piccolo di $\varphi(n)$
5. si calcola il numero d (chiamato *esponente privato*) tale che il suo prodotto con e sia congruo a 1 modulo $\varphi(n)$ ovvero che $ed \equiv 1 \pmod{\varphi(n)}$

La chiave pubblica è (n, e), mentre la chiave privata è (n, d).[5]

Per garantire transazioni sicure su internet si usa anche il sistema **SSL** (Secure Sockets Layer) e la nuova versione **TLS** (Transport Layer Security). Il sistema SSL/TLS viene usato per esempio sul protocollo di comunicazione dei browser **http**, diventando **https** (caratterizzato da un'icona con il lucchetto)

Facendo click sul lucchetto vengono visualizzati i dati della connessione:



Dettagli tecnici

Connessione crittata (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, chiavi a 128 bit, TLS 1.2)

La pagina visualizzata è stata crittata prima della trasmissione via Internet.

La crittazione rende difficile osservare le informazioni scambiate tra computer a persone non autorizzate. È quindi improbabile che qualcuno sia riuscito a leggere il contenuto di questa pagina durante il transito attraverso la rete.

Informazioni chiave pubblica

Algoritmo	RSA
Dimensione chiave	2048
Esponente	65537
Modulo	DD:CE:75:21:4F:DB:00:60:63:D1:2F:4D:6A:73:A5:77:6F:70:E5:84:D2:02:4B:F1:33:8...

BIBLIOGRAFIA – SITOGRAFIA

- Paolo Ferragina e Fabrizio Luccio - Crittografia – Bollati Boringhieri
- http://matematica.unibocconi.it/articoli/crittografia-e-numeri-primi
- https://it.wikipedia.org/wiki/RSA_(crittografia)