Crittografia classica e quantistica

Alessandro Minisini

Liceo Scientifico Niccolò Copernico

1 La crittografia: definizione e cenni storici

La crittografia è l'arte di creare dei messaggi nascosti, ovvero messaggi che nono impossibili da leggere per una persona non autorizzata a conoscerne il contenuto.
Inizialmente la crittografia aveva poco a che fare con quella che utilizziamo al giorno d'oggi, infatti non si basava su algoritmi basati su dimostrazioni matematiche, ma su semplici escamotage per nascondere il messaggio addosso al corriere.
I primi esempi li possiamo trovare nella Grecia antica: Plutarco ci parla della cosiddetta scitale spartana. Quest'ultima consisteva nell'arrotolare una cintura di cuoio attorno ad un bastone di diametro fissato e, a questo punto, trascrivere il messaggio partendo da un'estremità del bastone all'altra, parallelamente all'asse. Infine si svolggeva il cuoio e si trasmetteva al destinatario. Per poter leggere il messaggio era necessario utilizzare un bastone con lo stesso diametro, altrimenti riavvolgendo il messaggio le lettere non sarebbero state allineate. Un'altra tecnica e quella steganografica. Un esempio celebre è quello utilizzato da Mileto: si rasava la testa di un uomo e vi si scriveva sopra il messaggio e, quando i capelli erano ricresciuti, si mandava l'uomo a consegnare il messaggio. Ovviamente queste tecniche, soprattutto la seconda, erano concentrate sul nascondere il messaggio, piuttosto che renderlo illeggibile agli occhi di un esterno.
Il primo cifrario considerato tale è il cosiddetto "Cifrario di Cesare", utilizzato in ambito militare per comunicare con i vari comandanti sparsi per il mediterraneo. Inizialmente Cesare, come scrive lui stesso nel "De bello gallico", decise di cambiare le lettere dell'alfabeto latino con quelle greche:

ibi ex captivis cognoscit, quae apud Ciceronem gerantur quantoque in periculo res sit. Tum cuidam ex equitibus Gallis magnis preamiis persuadet, uti Ciceronem epistulam deferat. Hanc Graecis conscriptam litteris mittit, ne intecepta epistula nostra ab hostibus consilia cognoscantur. (De Bello Gallico V, 48.2-4)

Ai tempi di Cesare, questo sistema poteva essere considerato sicuro, poiché lo studio del greco era riservato solo alla classe dirigente romana che poteva permettersi un precettore privato e costosi viaggi di studio in Grecia.
Questo non è l'unico caso accertato di uso di cifrari a trsposizione da parte di Cesare; si sa, infatti, che Cesare ricorreva spessissimo a cifrari per trasposizione, anche per comunicare coi parenti. Sappiamo, in proposito che la cifratura era talmente tanto spesso utilizzata da Cesare, che Valerio Probo dedicò ai suoi cifrari un intero trattato, che purtroppo è andato perduto. Ma ci sono altre testimonianze, come quelle di Svetonio. Si legge infatti nelle "Vite dei Cesari":

Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.
(Vita di Cesare, 56)

Come ci dice Svetonio, il cifrario di Cesare era molto semplice da utilizzare: ogni lettera del testo in chiaro viene sostituita con una lettera che si trova ad un numero fissato di posizioni successive. Questi tipi di cifrario si dicono cifrari a sostituzione o scorrimento.
Il funzionamento di questo cifrario può essere descritto tramite l'aritmetica modulare: la funzione che descrive lo scambio della lettera in posizione x è la seguente

$$f(x) \equiv x + y \mod m$$

dove m è il numero di lettere dell'alfabeto.
Da questa si può ricavare facilmente la funzione inversa, che garantisce la

validità della cifratura:

$$\begin{aligned} f(x) &\equiv x + y \mod m \\ f(x) - x &\equiv y \mod m \\ x &\equiv f(x) - y \mod m \end{aligned}$$

Dunque

$$f^{-1}(x) \equiv x - y \mod m$$

Questi tipi di cifratura sono ormai considerati obsoleti, pociché la potenza di calcolo di un computer permette di provare ogni singola combinazione di lettere in un tempo irrisorio.
In realtà, questo tipo di cifratura è stato superato già nel Medioevo.
Un matematico arabo chiamato al-Kindi (IX secolo d.C.) elaborò un metodo di decrittazione basato sull'analisi delle frequenze: le lettere più frequenti nel messaggio devono corrispondere con le lettere più usate dalla lingua del messaggio originale. Questo fatto permette di ridurre drasticamente il numero di tentativi necessari, permettendo di decrittare il messaggio anche a mano.

2 Crittografia a chiave pubblica

I sistemi dicrittografia odierni sono detti a chiave pubblica: ogni persona che vuole parlare in mdoo cirfrato possiede due chiavi, una pubblica e una privata.
Definiamo E l'algoritmo di criptazione, D l'algoritmo di decriptazione e M il messaggio in chiaro da trasmettere. Ci sono quattro algoritmi essenziali per un sistema a chiave pubblica:

(a) Decifrare un messaggio cifrato ritorna il messaggio originale

$$D(E(M)) = M$$

(b) Anche il procedimento opposto deve ritornare il messaggio M

$$E(D(M)) = M$$

(c) Sia E che D devono essere sufficientemente facili da calcolare

(d) La chiave pubblica non deve compromettere la segretezza della chiave privata

2.1 Algoritmo RSA

In questo specifico sistema utilizza degli algoritmi E e D che si basano sull'aritmetica modulare. Per poterlo utilizzare dobbiamo rappresentare dobbiamo trasformare il messaggio M in forma numerica (ad esempio convertendo le lettere tramite tabella UNICODE). Supponiamo che M sia un numero intero tra 0 e $n-1$. Se il messaggio è troppo lungo possiamo dividerlo in più parti e criptarle separatamente. Siano e, d, n degli interi positivi e definiamo la coppia (e, n) come chiave pubblica e (d, n) la chiave privata. Ora per criptare il messaggio sarà sufficiente elevare M alla e modulo n, ottenendo il messaggio cifrato C. Per decritpare il messaggio bata elevare C alla d modulo n, ottenendo di nuovo M.Formalmente, otteniamo le seguenti definizione per E e D:

$$\begin{aligned} C \equiv E(M) \equiv M^e \mod n \\ M \equiv D(C) \equiv C^d \mod n \end{aligned} \tag{1}$$

Ora ci concentriamo sul meodo da seguire per creare le due chiavi (privata e pubblica). Prima di tutto scegliamo due numeri primi p, q sufficientemente

grandi e li moltiplichiamo per ottenere $n = pq$. Anche se n fa parte della chiave pubblica, la segretezza di p e q è garantita dal fatto che ricavarli da n è un'operazione computazionalmente complessa, impraticabile con i metodi odierni.
Ora rimangono da generare e è d. Scegliamo un d sufficientemente grande in modo che sia coprimo con $\varphi(n)$.

Definizione (Funzione φ di Eulero)**.** *La funzione φ di Eulero, detta anche toziente, è una funzione definita, per ogni intero n, come il numero di interi compresi tra 1 ed n che sono coprimi con n.*
Una delle proprietà fondamentali della funzione è la seguente:

$$\varphi(ab) = \varphi(a) \cdot \varphi(b) \tag{2}$$

Notare inoltre che per ogni primo p, $\varphi(p) = p - 1$.

Per concludere, troviamo e utilizzando i valori d, p e q, in modo che e sia l'inverso moltiplicativo di d modulo $\varphi(n)$. Ciò significa soddisfare la seguente congruenza

$$e \cdot d \equiv 1 \mod \varphi(n)$$

ovvero

$$e \cdot d = k \cdot \varphi(n) + 1$$

per un $k \in \mathbb{Z}$. Dalla (2), otteniamo facilmente $\varphi(n)$

$$\begin{aligned} \varphi(n) &= \varphi(p) \cdot \varphi(q) \\ &= (p-1)(q-1) \\ &= n - (p+q) + 1 \end{aligned}$$

Per l'aritmetica modulare, l'inverso moltiplicativo di a modulo m esiste se e solo se a ed m sono coprimi. Siccome d e $\varphi(n)$ sono coprimi per ipotesi, allora esiste sicuramente un e tale che sia l'inverso moltiplicaitivo di d e che $1 \leq e \leq \varphi(n)$.
A questo punto, dobbiamo verificare che l'algoritmo descritto con le chiavi appena generate soddisfi le condizioni imposte inzialmente.
Innanzitutto notiamo che le condizioni (a) e (b) implicano la stessa condizione, infatti:

$$D(E(M)) \equiv (E(M))^d \equiv (M^e)^d \mod n = M^{e \cdot d} \mod n \tag{3}$$

$$E(D(M)) \equiv (D(M))^e \equiv (M^d)^e \mod n = M^{e \cdot d} \mod n$$

Siccome $e \cdot d = k \cdot \varphi(n) + 1$, possiamo sostituire l'espressione nelle equazioni precedenti, ottenendo:

$$M^{e \cdot d} \equiv M^{k \cdot \varphi(n)+1} \mod n$$

. Affinché l'algoritmo funzioni, vogliamo che questa espressione valga esattamente M. Per provarlo, ricordiamo un'altra propietà della funzione di Eulero: per ogni intero M coprimo con n, vale che

$$M^{\varphi(n)} \equiv 1 \mod n$$

Siccome abbiamo definito $0 \leq M \leq n$, sappiamo che M *non* è coprimo con n se e solo se $p \mid M$ o $q \mid M$. Di questi due casi ce ne occupiamo in seguito. Per tutti gli altri casi possibili, vale che:

$$M^{e \cdot d} \equiv M^{k \cdot \varphi(n)+1} \equiv \left(M^{\varphi(n)}\right)^k \cdot M \equiv 1^k \cdot M \mod n = M$$

Come volevasi dimostrare.
Ora analizziamo il caso particolare in cui $p \mid M$ o $q \mid M$. Siccome $M < n$, le due espressioni non possono essere contemporaneamente vere. Senza perdita di generalità, supponiamo che valga $p \mid M$. Questa assunzione ci permette di dire che

$$MCD(M, p) = p$$

ovvero

$$M = pt \text{ con } t \in \mathbb{Z}$$

e che

$$MCD(M, q) = 1$$

poiché q è primo. Per il piccolo teorema di Fermat, sappiamo che:

$$M^{q-1} \equiv 1 \mod q \tag{4}$$

Ora, eleviamo i due membri della (4) alla $k(p-1)$, ottenendo la seguente congruenza (equivalente alla prima):

$$M^{k(q-1)(p-1)} \equiv 1 \mod q$$

$$M^{k(q-1)(p-1)} = 1 + hq \tag{5}$$

per $h \in \mathbb{Z}$.
Ora moltpilichiamo i due membri della (5) per M, ottenendo:

$$M^{1+k(q-1)(p-1)} = M + Mqh$$

Ora sostituiamo alcune parti dell'equazione con alcuni risultati ottenuti sopra, nello specifico sappiamo che $(q-1)(p-1) = \varphi(n)$ e che $M = pt$. Otteniamo che:

$$\begin{aligned} M^{1+k\cdot\varphi(n)} &= M + \overbrace{pq}^{n} th \\ M^{1+k\cdot\varphi(n)} &= M + nth \\ M^{1+k\cdot\varphi(n)} &\equiv M \mod n \end{aligned}$$

Sotituiamo $e \cdot d = 1 + k \cdot \varphi(n)$:

$$M^{e\cdot d} \equiv M \mod n$$

Che è proprio ciò che volevamo verificare.
La dimostrazone quindi garantisce la validità del sistema di criptazione RSA per ogni M.