Crittografia classica e quantistica

Alessandro Minisini

Liceo Scientifico Niccolò Copernico

Indice

1 Introduzione 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.

2 Crittografia a chiave privata: Cifrario di Cesare

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.

3 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

3.1 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.

3.2 Sicurezza del sistema RSA

4 La crittografia quantistica

4.1 Protocollo BB84

Il protocollo che verrà descritto in seguito è il cosiddetto BB84, sviluppato da Charles H. Bennet e Gilles Brassard nel 1984. È stato il primo metodo di crittografia quantistica mai inventato ed è utilizzabile come metodo per comunicare in modo privato una chiave segreta tra due utenti per poi utilizzare un protocollo del tipo OTP, descritto in precedenza.

4.2 Principi fisici che garantiscono il funzionamento del BB84

Per sfruttare questo sistema si utilizza la luce. Per la meccanica quantistica la luce è composta da quantità discrete di energia, chiamate fotoni. Ogni fotone possiede anche un carattere ondulatorio che gli conferisce un proprio angolo di polarizzazione, definito come l'angolo tra il piano in cui essi oscillano e il piano di propagazione degli stessi fotoni.
Normalmente una sorgente di luce produce fotoni a polarizzazione arbitraria. Per far assumere una particolare polarizzazione ad un fotone si utilizza un filtro polarizzatore, che permette solo ai fotoni con una determinata polarizzazione di proseguire il loro cammino. Ogni polarizzatore ha un angolo ben preciso di polarizzazione che chiameremo θ. Ruotando opportunamente il filtro polarizzatore in modo che permetta il passaggio solo di fotoni con polarizzazione θ, allora tutti i fotoni con polarizzazione diversa da θ vengono fermati, oppure oltrepassano il filtro con una polarizzazione θ. Le leggi della meccanica quantistica ci dicono che un fotone inizialmente polarizzato con un angolo ϕ oltrepassa il filtro con la seguente probabilità:

$$p_\theta(\phi) = \cos^2(\phi - \theta)$$

La probabilità che venga respinto invece è naturalmente:

$$1 - p_\theta(\phi) = \sin^2(\phi - \theta)$$

Per semplicità, supponiamo di utilizzare raggi luminosi che contengono un singolo fotone polarizzato. Per i nostri scopi, utilizzeremo solo quattro angoli di polarizzazione: 0°,45°,45°,135°.

I fotoni verranno trasmessi da un capo all'altro della comunicazione tramite fibra ottica, mentre per misurare la polarizzazione del fotone si utilizza un cristallo di calcite. Quando il fotone attraversa il cristallo infatti, possono accadere due cose:

- il fotone lo attraversa in linea retta ed emerge polarizzato perpendicolarmente rispetto all'asse ottico del cristallo
- il fotone viene traslato ed emerge polarizzato parallelamente rispetto all'asse ottico.

Se il fotone è inizialmente polarizzato ortogonalmente rispetto all'asse ottico allora il suo stato non subirà modifiche. Se invece non è così, il fotone seguirà uno dei due cammini con eguale probabilità, subendo un'opportuna ripolarizzazione. Un comportamento del tutto casuale si ha quando la polarizzazione è a metà fra le due direzioni, quindi forma un angolo di 45° o 135° col piano ottico del cristallo: in tal modo ogni informazione sullo stato iniziale viene completamente persa. Per questo motivo, nel protocollo BB84 vengono utilizzati gli angoli precedentemente indicati: se per le misure ortogonali non è necessario apportare modifiche al cristallo, per le misure diagonali è sufficiente ruotare il cristallo originale di 45°.

4.3 Procedimento operativo

Ipotizziamo che Alice e Bob vogliano comunicare in maniera cifrata e che utilizzino il protocollo BB84 per trasferire la chiave di criptazione. Ognuno dei bit (unità dell'informazione) che compongono la chiave è rappresentato da un fotone polarizzato come nella tabella seguente:

R	D	Bit
↔	↗	1
↕	↘	0

Supponiamo poi che ogni impulso contenga un solo fotone. Il protocollo è il seguente:

1. Alice sceglie una sequenza casuale di bit ed una sequenza casuale di basi di polarizzazione (rettilinea o diagonale) e manda a Bob una sequenza di fotoni, ognuno rappresentante un bit della stringa, nella base scelta.

2. Bob sceglie casualmente per ogni fotone mandatogli da Alice (e indipendentemente dalle scelte fatte da Alice) se misurare la polarizzazione rettilinea o diagonale e interpreta ogni risultato come 0 o 1, a seconda dell'esito della corrispondente misura. Bob ottiene quindi dati significativi solo dal 50% dei fotoni che ha misurato (quelli per i quali ha indovinato la corretta base di polarizzazione) supponendo che non vi siano state alterazioni dovute ad origliamento. Notare che ogni misura fatta da Bob altera lo stato del fotone, rendendo impossibile ricostruire il suo stato iniziale.

3. Bob annuncia pubblicamente le basi con cui ha analizzato i fotoni.

4. Alice comunica pubblicamente a Bob se per ciascun fotone che egli ha ricevuto ha eseguito il tipo giusto di misurazione. Si scartano tutte le posizioni dei bit per le quali Bob ha eseguito un tipo di misurazione sbagliato o per le quali non è stato rilevato alcun fotone (Ciò può capitare per svariate ragioni, dovute sia ad un eventuale origliatore che all'errore degli strumenti di misura).

5. Alice e Bob, per verificare se le loro risultanti stringhe di bit sono identiche, confrontano pubblicamente un sottoinsieme casuale dei bit correttamente ricevuti da Bob, cioè con la base esatta. Se tutti i fotoni (o quasi) concordano, Alice e Bob possono concludere che la trasmissione quantistica è stata libera da significativi origliamenti, per cui i rimanenti bit segreti possono costituire la chiave. Se invece vi è stato un notevole origliamento, la trasmissione è scartata e si riprova con un nuovo gruppo di fotoni.

In seguito è riportato un esempio di trasmissione della chiave quantistica da parte dei due interlocutori.

1a.	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
1b.	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
1c.	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
2a.	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
2b.	1		1		1	0	0	0		1	1	1		1	0
3.	R		D		R	D	D	R		R	D	D		D	R
4a.			OK		OK			OK				OK		OK	OK
4b.			1		1			0				1		0	1
5a.					1									0	
5b.					OK									OK	
5c.			1					0				1			1

Trasmissione quantistica	
1a.	Bit scelti da Alice
1b.	Basi scelte da Alice
1c.	Fotoni polarizzati spediti sul canale quantistico
2a.	Basi scelte da Bob per misurare i fotoni
2b.	Bit ricevuti da Bob
Discussione pubblica	
3.	Bob dichiara le basi che ha utilizzato
4a.	Alice dice a Bob quali basi erano corrette
4b.	Bit validi per la chiave di criptazione
5a.	Bob rivela alcuni bit della chiave ottenuta
5b.	Alice conferma i bit inviati, verificando la validità della chiave
Risultato	
5c.	Bit rimanenti utilizzati nella chiave

4.4 La meccanica quantistica ci fornisce il certificato di sicurezza

Principio di indeterminazione di Eisenberg + Non-cloning theoerm.