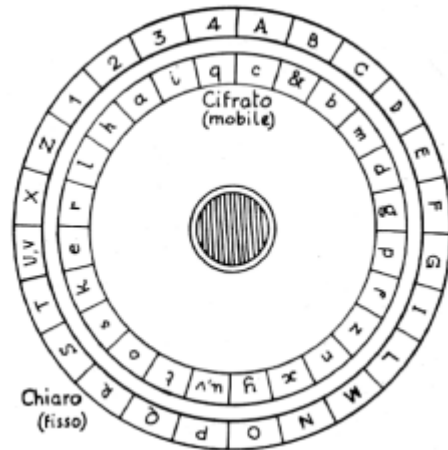

I numeri primi e la crittografia

Maddalena Bovetti

Liceo Scientifico Tecnologico

"Deambrosis" di Rapallo

E-mail: maribo15@libero.it



ABSTRACT: Breve storia della crittografia narrata attraverso gli eventi e le vicende storiche ma con attenzione alla matematica e ai suoi contenuti.

È un testo didattico che può essere utilizzato con facilità in classe o letto da uno studente da solo a casa.

PAROLE CHIAVE: Crittografia, didattica della matematica.

“Il mio nome è Bond, James Bond”, chi non ricorda questa battuta leggendaria pronunciata dal celebre agente segreto nato dalla fervida fantasia di Ian Fleming?

Protagonista di numerosi romanzi e relativi film, il nostro eroe è sempre impegnato a combattere pericolosi assassini e a smascherare terribili macchinazioni contro l'umanità, utilizzando dispositivi tecnologici di grande effetto, codici segreti, cifrari, macchine decrittatici e tutto ciò che fa parte del “corredo” di una spia che si rispetti.

Ma cosa c'entra l'agente 007 con la matematica? Be', è soltanto un modo un po' spensierato per addentrarci in un mondo altrettanto affascinante e intrigante, ma non per questo meno impegnativo, quello dei testi cifrati, delle intercettazioni, dei messaggi segreti: in altre parole, la crittografia, a sua volta legata, appunto, alla matematica.

L'informatica, e, in particolare, Internet, hanno fatto sì che il problema della segretezza e della riservatezza delle comunicazioni diventasse sempre più importante e sempre più improrogabile l'urgenza di trovare tecniche inviolabili e impenetrabili.

Pensiamo, per esempio, ai mezzi informatici di pagamento che usiamo comunemente ogni giorno: bancomat, carte di credito, il famoso Telepass che ci evita tante “code” ai caselli autostradali, per non parlare della posta elettronica, del commercio elettronico e così via: tutte queste informazioni devono essere comunicate attraverso dispositivi di partenza (computer, sportelli..) a quelli remoti mediante “sistemi di criptazione dell'informazione” e sono guai seri se qualche male intenzionato riesce a decifrarli prima del legittimo destinatario.

Prima di entrare nel merito della questione, permettetemi di aprire una parentesi per chiarire il significato di alcune parole che useremo spesso nella nostro racconto.

Cominciamo con quello che sarà il filo conduttore di questo capitolo, la crittografia, parola che deriva dal greco *kryptós*, che significa nascosto e da *gráphein* che significa scrivere; quindi, è l'insieme di “ quei sistemi in grado di rendere incomprensibile un messaggio a chiunque ne venga in possesso, ad eccezione del legittimo destinatario; la crittanalisi, invece, è l'arte di “rompere” tali sistemi; mentre la crittologia le comprende entrambe.

Chiamiamo, poi, algoritmo l'insieme delle operazioni che consentono di trasformare un testo in chiaro (quello che possiamo leggere tutti) nel corrispondente testo cifrato e viceversa; la chiave, invece, è la particolare parola, o frase, “che consente, tramite l'applicazione dell'algoritmo di cifratura, di trasformare un testo in chiaro in un testo cifrato e viceversa”

La necessità di scambiarsi informazioni segrete, soprattutto di tipo militare, non riguarda solo i tempi moderni e risale addirittura agli antichi spartani, cui appartiene uno dei primi tipi di cifrario, la cosiddetta scitála lacedemonica.

Partiremo, perciò, dalla città di Sparta, più di 2500 anni fa , analizzeremo alcuni codici dell'antichità come esempio, e, poi, prenderemo in considerazione i metodi di cifratura dei giorni nostri, dove, ancora una volta, la matematica sarà protagonista.

A questo punto possiamo iniziare la nostra breve storia della crittografia, cominciando dal primo esempio di messaggio cifrato di cui ci parla Plutarco, nella sua opera Vite Parallele: lo storico greco scrive che gli efori, cioè i magistrati che avevano il compito di controllare l'opera dei re ed erano responsabili della politica estera, trasmettevano ai generali messaggi segreti con un metodo molto ingegnoso. Mittente e destinatario facevano uso di due bastoni di legno cilindrici perfettamente uguali, cioè aventi lo stesso diametro e la stessa lunghezza; tale pezzo di legno era noto come scitála .(Fig.n1). Il mittente avvolgeva a spirale un sottile nastro di pergamena, (o di cuoio) lungo e stretto come una cinghia, intorno al suo bastone cilindrico e scriveva il messaggio in righe

longitudinali. Quando la pergamena veniva srotolata il testo del messaggio appariva privo di senso e riacquistava significato solo se riavvolta intorno alla scitola gemella che era posseduta solo dal legittimo destinatario.

Questo perché le lettere del testo cifrato erano le stesse del testo in chiaro, ma erano in una diversa posizione (la regola è detta appunto trasposizione)

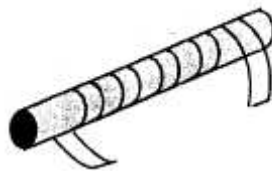


Figura 1

Un altro esempio di cifrario del passato di cui si ha testimonianza scritta, è quello di Enea il Tattico: alcuni studiosi ritengono che Enea fosse un generale del Peloponneso, vissuto nel IV secolo A.C.

Narra Polibio, storico greco autore de *Le storie*, che Enea il Tattico, descrisse uno strumento, forse inventato dai Cartaginesi, adatto alle comunicazioni a grande distanza.

Il congegno era fondato sull'uso di due recipienti cilindrici in rame, di uguali dimensioni, aventi alla base un foro di ugual diametro, chiuso da uno spinotto. Ogni cilindro, riempito di acqua, portava a galla un tappo di legno che scorreva verticalmente lungo l'asse del recipiente con il defluire dell'acqua. Su questo tappo era fissata l'asta verticale su cui, a diverse altezze, erano incise o dipinte, figure che rappresentavano degli eventi. Colui che trasmetteva, segnalava con fiaccola al suo corrispondente il momento in cui, contemporaneamente, si dovevano estrarre gli spinotti. L'acqua defluiva da entrambi i recipienti, in uguale quantità, ed il galleggiante si abbassava, portando l'asta ed il messaggio prescelto, a coincidere con il bordo del cilindro. Altro segnale con la fiaccola, e gli spinotti, bloccando il defluire dell'acqua, fermavano la comunicazione ed i suoi contenuti. Con questo sistema ingegnoso, il messaggio arrivava rapidamente al destinatario.

Ricordiamo, ancora, il famoso cifrario di Giulio Cesare, che faceva largo uso di crittografia, tanto che Valerio Probo gli dedicò un intero trattato, che purtroppo è andato perduto. Tuttavia Svetonio, nella *Vita dei Cesari*, racconta di uno dei metodi usati dal grande condottiero.

Il sistema consiste in una semplice traslazione di tutte le lettere dell'alfabeto di un numero prestabilito di posizioni, che costituisce la chiave. Per esempio, se la chiave scelta fosse 3, ogni singola lettera dell'alfabeto non cifrato verrebbe trasposta nella terza che la segue, e le ultime lettere verrebbero sostituite dalle prime. Provate a decifrare il seguente messaggio con la chiave sopra indicata: "BHQN, BNGN, BNFN".

Vi ricorda qualcosa?

Anche nel Vecchio Testamento troviamo tre principali scritture segrete : l' Atbash, l' Albam e l' Atbah. Il primo codice cifrato, l' Atbash, è stato ideato dal popolo ebraico. Esso consisteva nel capovolgere l'alfabeto, di conseguenza la prima lettera diventava l'ultima e l'ultima la prima e così per tutte le altre lettere dell'alfabeto. Usando il nostro alfabeto, l' Atbash è espresso dalla seguente tabella di cifratura:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

L'Albam richiede che l'alfabeto venga diviso in due parti e che ogni lettera venga sostituita con la corrispondente dell'altra metà, quindi alla lettera A corrisponde la L, alla B la M e così via.

Infine, l'Atbah, richiede che la sostituzione soddisfi una relazione di tipo numerico: le prime nove lettere dell'alfabeto vengono sostituite in modo tale che la somma della lettera da sostituire e della lettera sostituita risulti uguale a dieci. Per le restanti lettere dell'alfabeto deve valere una regola simile con somma pari a 28, per le ultime 8 lettere dell'alfabeto la regola è la stessa, con somma pari a 45.

YFLMZ OVGGFIZ ! E' un messaggio in Atbash, divertitevi a decifrarlo.

E questi sono solo alcuni esempi, ma è chiaro che la necessità di evitare che un messaggio finisse in mani sbagliate ha fatto sì che nel corso dei secoli venissero elaborati metodi crittografici sempre più sofisticati e difficili da scoprire.

Vale la pena ancora di ricordare Enigma, una macchina molto simile ad una macchina da scrivere, risalente alla seconda Guerra Mondiale e utilizzata dalle Forze armate tedesche.

La macchina fu inventata nel 1918 da Arthur Scherbius e subì varie modifiche per migliorarne le capacità, diminuirne il costo e, soprattutto, la possibilità di decifrazione; I crittografi tedeschi erano così convinti della sicurezza del loro sistema che peccarono di ingenuità, la più grave quella di usare troppo a lungo la stessa "chiave" di cifratura.

I crittografi britannici e il gruppo di lavoro del grande matematico inglese Alan Turing, con la collaborazione del matematico polacco Marin Rejewsky e l'aiuto di calcolatori elettromeccanici detti "bombes", permisero all'Intelligence inglese di decifrare molti importanti messaggi in codice dell'esercito del Reich.

Questo fatto fu talmente importante che lo storico inglese Sir Harry Hinsley sostiene che "...se la Government Code and Cypher School non fosse riuscita a decifrare i crittogrammi di Enigma, la guerra sarebbe finita nel 1948, invece che nel 1945".

Per curiosità del lettore ricordiamo che allo studio di Enigma prese parte anche Ian Fleming, allora ufficiale di corvetta della Marina, che per entrare in possesso della chiave per risolvere il problema propose di assaltare una nave tedesca. Il piano fu approvato, ma non venne mai messo in atto per i rischi che l'operazione avrebbe comportato. Ian Fleming lavorò per l'Intelligence Service sino alla fine della guerra, per poi dedicarsi all'attività di scrittore.

Tutti i metodi crittografici utilizzati fino a non molti anni fa avevano una caratteristica comune, non particolarmente pratica; infatti per tutti i messaggi trasmessi in codice, mittente e destinatario dovevano, in qualche modo, incontrarsi per comunicarsi il metodo di codifica, dalle semplici scitale alla più sofisticata Enigma, nel primo caso si dovevano conoscere le dimensioni del cilindro, nel secondo dal comando centrale di Berlino si doveva comunicare ai decifраторi la chiave per il "settaggio" iniziale delle ruote che costituivano la macchina per permettere la decodifica della comunicazione.

Questo tipo di crittografia si chiama simmetrica, cioè viene utilizzata un'unica chiave sia per codificare, sia per decodificare i messaggi. Le informazioni (la chiave e l'algoritmo) necessarie per chi deve inviare il messaggio sono quindi le stesse di quelle necessarie a chi deve leggerlo.

Per concordare una chiave il mittente e il destinatario devono mettersi d'accordo: o incontrarsi, o in qualsiasi altro modo che non fosse lo stesso canale dell'invio del messaggio, che non sarebbe stato, ovviamente, sicuro, visto che ci si doveva servire della cifratura...

Tutto ciò, ovviamente, aumentava la probabilità che la segretezza del messaggio andasse perduta e la poca praticità.

Il problema è stato risolto in tempi relativamente recenti, intorno agli anni Settanta, con l'invenzione della crittografia a chiave pubblica. Con algoritmi di questo tipo esistono due chiavi: una pubblica da distribuire a tutti quelli con cui si vuole comunicare, e una privata da tenere segreta.

Prima di continuare, come già preannunciato, ricordiamo che ancora una volta la matematica ha un ruolo importante anche nella crittografia e, quindi, dovrò indossare di nuovo gli abiti da “prof” e fare un po’ di lezioni teoriche.

Bene, possiamo cominciare con questa operazione: $9+4=1$. Qualcuno penserà: ma siamo impazziti? Niente affatto! Rispondiamo, perché, se ci pensiamo un momento, se il primo numero rappresenta le ore 9 del mattino, dopo 4 ore, sono le tredici, cioè sul nostro orologio la lancetta è sul numero uno!

Ma allora, sempre pensando all’orologio, basta sommare i due numeri, sottrarre 12 ed il gioco è fatto! Quindi:

$$8+6=2$$

$$10+6=4 \text{ e così via}$$

Quello che molto semplicisticamente abbiamo chiamato “gioco”, in effetti, rappresenta una parte importante della matematica, detta appunto, aritmetica dell’orologio, poiché su tale principio si basa il calcolo delle ore a cicli di 12 o 24, o più precisamente, aritmetica modulare che ha molte applicazioni, fra cui la crittografia.

E’ chiaro al posto di 12 posso scegliere un numero qualunque, per esempio :

$$3+5=3 \pmod{5} \quad (3+5=8 \rightarrow 8-5=3) \text{ se abbiamo scelto il numero } 5$$

$$8+4=5 \pmod{7} \text{ se abbiamo scelto il numero } 7$$

La scrittura, formalmente corretta, prevede anche l’aggiunta di mod. n e, quindi, le operazioni precedenti sono:

$$8+6=2 \pmod{12} \text{ e così via.}$$

Penso che ormai i nostri lettori avranno capito il meccanismo applicato, che è, in fondo, quello interessa nel nostro caso, tralasciando la parte teorica, non sempre di facile comprensione.

Un altro concetto che ci servirà per spiegare il problema delle chiavi in crittografia è quello di numero primo.

Ricordiamo che un numero naturale (cioè intero e maggiore di zero), diverso da uno, è primo se è divisibile solo per uno e per se stesso, cioè se ha solo due divisori, pertanto il numero uno viene escluso (per precisione, questa non è la sola ragione, ve ne sono altre). Quindi, 2 è primo (è l’unico pari ad esserlo), 3, 7, 11, ecc, sono primi, 9, 1234 non sono primi.

I numeri primi hanno un’interessante storia, perché la loro successione rappresenta fin dall’antica Grecia, uno dei misteri più affascinanti della scienza: generazioni di matematici hanno lavorato per risolvere vari quesiti relativi a quelli che Marcus du Sautoy definisce “il ritmo cardiaco, irregolare, della matematica”

Se conosciamo tutti i numeri primi fino a un certo numero, possiamo prevedere quale sarà il prossimo? C’è una formula capace di generare numeri primi?

Du Sautoy, docente di matematica all’Università di Oxford è uno dei maggiori specialisti mondiali di teoria dei numeri ed è l’autore di un interessante ed avvincente libro dal titolo “L’enigma dei numeri primi- L’ipotesi di Riemann, l’ultimo grande mistero della matematica” dove affronta proprio i problemi prima posti e la storia di questi particolari numeri, spiegando tutte le varie ipotesi e i teoremi che su di essi sono stati elaborati.

Du Sautoy afferma che i numeri primi sono, per il matematico, ciò che gli atomi rappresentano per il chimico, ma mentre in chimica è stato possibile costruire un elenco di tutti gli atomi che esistono in natura, cioè quella che viene chiamata la Tavola Periodica e che elenca 109 elementi chimici con cui sono costruite tutte le molecole, non è stato possibile fare altrettanto in matematica. Infatti mentre i gli atomi sono 109, i numeri primi sono infiniti e, questo, lo aveva già dimostrato Euclide.

Il sistema più semplice per ricercare i numeri primi minori di un certo numero N è stato ideato da **Eratostene di Cirene**, matematico e filosofo greco vissuto nel II secolo a.c., bibliotecario della Biblioteca di Alessandria ed oggi ricordato soprattutto per aver misurato per primo, con grande precisione, le dimensioni della Terra.

Il suo metodo, noto con il nome di Crivello di Eratostene, si fondava su un principio piuttosto semplice, che oggi viene tradotto anche in linguaggi di programmazione: si scrivono tutti i numeri minori di N a partire da 2 (questo elenco lo chiamiamo setaccio); poi si cancellano (setacciano) tutti i multipli del primo numero del setaccio (escluso il numero stesso), cioè due. Si prosegue con 3, 5, così fino ad arrivare in fondo. I numeri che restano sono i numeri primi minori od uguali a n . È come se si utilizzassero dei setacci a maglie via via più larghe: il primo lascia passare solo i multipli di 2, il secondo solo i multipli di 3, e così via. Ci si ferma al primo numero che supera la radice quadrata di n .

Nel corso dei secoli molti matematici e fisici hanno elaborato teorie che dimostrassero l'esistenza o meno di un ordine nella sequenza, apparentemente caotica, di questi particolari numeri o la possibilità di trovare una formula o una regola che permettesse di stabilire qual è, per esempio, l'ennesimo numero primo; qualsiasi storia sui numeri primi non può non ricordare il contributo di Bernhard Riemann, matematico e fisico tedesco nato a Breselenz il 17 settembre 1826 e morto a Sealsca il 20 giugno 1866.

Egli elaborò un'ipotesi, nota, appunto come ipotesi di Riemann, che Hilbert, uno dei più grandi matematici dell'epoca, inserì, all'ottavo posto tra i famosi ventitré problemi (tra questi anche il teorema di Fermat), che presentò, nell'agosto del 1900, al Congresso internazionale dei matematici, alla Sorbona di Parigi.

L'ipotesi non fu né dimostrata, né confutata per tutto il ventesimo secolo ed è ora considerata tra i sette più difficili problemi del nuovo millennio: nel 2000 il Clay Mathematics Institute ha offerto un premio di un milione di dollari a chi riuscirà a provarli, ma stranamente non ha offerto nessun premio a chi ne dimostrasse la falsità.

Attualmente, tramite l'uso di computer, si è calcolato che, per i primi miliardo e mezzo di numeri primi (scusate la ripetizione, ma non si può fare altrimenti) l'ipotesi è vera: per la matematica, però, ciò non è sufficiente. Infatti basterebbe un solo contro esempio perchè l'ipotesi sarebbe assolutamente falsa.

Purtroppo non è possibile presentare in termini semplici l'ipotesi di Riemann, d'altra parte semplificarla troppo ci farebbe correre il rischio di banalizzare o di svilire il lavoro di un grande studioso; perciò apriremo una parentesi con una breve spiegazione della formula per gli appassionati e avvisiamo chi non ha troppa simpatia per formule o equazioni di "saltarla", perché ciò non pregiudica la comprensione di quello che seguirà.

Cominciamo a introdurre la cosiddetta funzione Zeta di Riemann $\zeta(s)$ che è definita per ogni numero complesso ¹ $s \neq 1$ dalla serie:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (1)$$

Per $s = 2$ la (1) diventa $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots$

La funzione zeta si annulla se s assume un qualunque valore intero negativo pari; per esempio $-2, -4$ che sono detti zeri banali

L'*Ipotesi di Riemann* afferma che tutti gli altri numeri complessi s per cui $\zeta(s) = 0$ hanno parte reale uguale a $1/2$, cioè tutti gli zeri non banali della funzione zeta hanno parte reale $1/2$, ovvero stanno sulla retta di equazione $x = 1/2$, detta retta critica.

Per ragioni che è impossibile spiegare in poche parole, la distribuzione degli zeri di $\zeta(s)$ è a sua volta strettamente legata alla distribuzione dei numeri primi.

Quello che possiamo sicuramente affermare è che Riemann lasciò ai matematici un problema molto importante: dimostrare che l'ordine che regolava il mondo dei numeri primi da lui ipotizzato, esisteva effettivamente.

La dimostrazione dell'ipotesi di Riemann avrebbe importanti conseguenze: per esempio, molti teoremi matematici che iniziano dicendo "Supponendo che l'ipotesi di Riemann sia esatta...", sarebbero automaticamente veri, un'altra conseguenza è che si aprirebbero nuove strade per la comprensione della struttura dei numeri primi, non ultima, forse, la possibilità di trovare un criterio per scomporre un numero in fattori primi molto più rapido di quelli attuali e, come afferma Du Sautoy ciò "metterà in ginocchio l'intero commercio elettronico nello spazio di una notte".

Ma, allora, in che modo tutto ciò è legato alla sicurezza informatica e, in generale, alla protezione di comunicazioni, di messaggi, di codici e così via? Prima di rispondere a questa domanda ricordiamo ancora un altro importante teorema che ci sarà utile, quello che viene indicato come il "teorema fondamentale dell'aritmetica": Ogni numero naturale diverso da 1 o è un numero primo o si può esprimere come prodotto di numeri primi. Tale rappresentazione è unica se si prescinde dall'ordine in cui compaiono i fattori.". Per esempio $15 = 3 \times 5$, $12 = 3 \times 2 \times 2$, e così via.

Prima della lunga parentesi teorica, avevamo parlato della crittografia simmetrica e dei suoi limiti; limiti che sono superati dalla crittografia asimmetrica, vediamo di cosa si tratta.

Esistono due chiavi, una segreta ed una pubblica: chiunque può adottare la chiave pubblica per criptare un messaggio, ma solo il proprietario della chiave segreta sarà in grado di leggerne il contenuto. Cioè, mentre nella crittografia simmetrica la chiave è unica, in quella asimmetrica le chiavi sono due. Mi spiego meglio: per criptare un messaggio si usa un algoritmo controllato da una chiave di codifica detta pubblica, ma per decodificarlo si usa un algoritmo connesso al primo che però è controllato da una chiave detta privata.

Volendo ulteriormente chiarire il concetto può essere utile una frase di Simon Sing, autore di "Codici & segreti" ed altri numerosi testi di divulgazione scientifica, tra cui "L'ultimo teorema di Fermat":. "*La crittografia*

¹ Un numero complesso è un numero del tipo $a+ib$, dove a è la parte reale, i l'unità immaginaria e b il coefficiente dell'immaginario; ogni numero reale è un particolare numero complesso con parte immaginaria uguale a zero.

asimmetrica potrebbe essere illustrata nel modo seguente: chiunque può chiudere un lucchetto facendo scattare l'anello metallico, ma solo chi ha la chiave può aprirlo. La chiusura è alla portata di tutti (come la cifratura) ma l'apertura è privata (come la decifrazione) e possibile solo per il possessore della chiave.”

Le chiavi pubbliche vengono distribuite in rete, mentre quelle private sono note soltanto al destinatario.

Un classico esempio è il commercio elettronico: il responsabile di un'attività commerciale, che vende i suoi prodotti su Internet, fornisce ai suoi clienti la chiave pubblica con cui possono crittografare (con opportuni software) il numero della propria carta di credito. A questo punto, il messaggio criptato può essere decodificato solo da chi gestisce il commercio, in quanto solo lui e, nessun altro, possiede la chiave privata. Quindi, se anche una terza persona venisse indebitamente in possesso dei numeri, ormai criptati, non potrebbe farne uso, perché non conosce la chiave per decifrarli.

Uno degli algoritmi asimmetrici più conosciuti è l'algoritmo RSA, acronimo formato dalla prima lettera dei cognomi di coloro che lo inventarono nell'aprile del 1977: Ronald L. Rivest, Adi Shamir e Leonard M. Adleman.

Le due chiavi possono essere ricavate l'una dall'altra, ma la garanzia fornita da RSA è che l'operazione di derivare la chiave segreta da quella pubblica è troppo complessa per venire eseguita in pratica, anche su un calcolatore molto potente; infatti RSA sfrutta il fatto che è facile calcolare il prodotto di due numeri primi anche molto grandi, ma dato un numero è molto più difficile scomporlo, cioè trovare i numeri primi il cui prodotto è proprio il numero dato.

Per capire meglio facciamo un esempio pratico che dovrebbe chiarire l'idea su cui si basa l'RSA:

1. si scelgono a caso due numeri primi, p e q , l'uno indipendentemente dall'altro, abbastanza grandi da garantire la sicurezza dell'algoritmo
2. si calcola il loro prodotto $n = n \times p$, chiamato *modulo* (ricordate l'aritmetica dell'orologio)
3. si sceglie poi un numero e (chiamato *esponente pubblico*), più piccolo e primo (cioè il cui unico divisore comune è 1) con $(p-1)(q-1)$
4. si calcola il numero d (chiamato *esponente privato*) tale che $e \bullet d = 1 \text{ mod } (p-1)(q-1)$

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

Il punto di forza dell'algoritmo sta nel fatto che con numeri molto grandi il calcolo di d è molto lungo e difficoltoso. Proviamo a illustrare i passaggi sostituendo a p e q due numeri (non particolarmente grandi per non complicare troppo il calcolo), ma teniamo conto che nella realtà sono usati numeri dell'ordine di 10^{100} .

1. Prendiamo due numeri primi $p=11$ e $q=7$
2. Sia $n = 77$ sia il loro prodotto,
3. Scegliamo $e=13$ che è minore di n e primo con $(p-1)(q-1)$.

Eseguiamo il calcolo: $(p-1)(q-1)=(11-1)(7-1)=10 \cdot 6=60$; 13 e 60 sono primi fra loro.

4. Calcolare d (intero) in modo che: $d \cdot e = 1 \text{ MODULO } (p-1)(q-1)$ significa trovare un numero tale che

$$d \cdot e = 1 \text{ mod } 60. \rightarrow d=37$$

Infatti $37 \cdot 13 = 1 \text{ mod } 60$ in quanto $481/60 = 8$ resto 1

Nel nostro caso la chiave pubblica è $(77, 13)$, mentre la chiave privata è $(77, 37)$.

Il calcolo di d è complesso in quanto per trovare il prodotto $(p-1)(q-1)$ devo scomporre n , calcolo difficile tenendo conto delle dimensioni di n, p e q .

Lo scambio di chiavi rimane comunque un problema grave, nonostante l'uso della crittografia asimmetrica. Infatti, anche se non viene trasmessa la chiave privata, è comunque necessario inviare alcuni dati (i numeri n ed e) che qualcuno, diverso dal legittimo destinatario, potrebbe intercettare ed utilizzare per ricostruire l'intera chiave..

Uno dei sistemi più sicuri è il cosiddetto codice Vernam da nome di colui che lo inventò nel 1916, la cui indecifrabilità è assicurata da una dimostrazione matematica. La caratteristica di tale codice è l'uso di una chiave illimitata, o comunque lunga almeno quanto il testo da cifrare, totalmente casuale e utilizzabile solo una volta per avere la sicurezza assoluta.

Questo sistema non è particolarmente comodo a causa degli svantaggi dovuti all'espansione della chiave, ciononostante sembra che sia stato usato negli anni della guerra fredda dai servizi segreti dell'Est e per il telefono rosso tra Washington e Mosca. Un cifrario di Vernam era anche quello trovato addosso al Che Guevara, dopo la sua uccisione nel 1967.

A questo punto, dobbiamo pensare come il grande scrittore Edgar Allan Poe che “È veramente da mettere in dubbio che l'intelligenza umana possa creare un cifrario che poi l'ingegno umano non riesca a decifrare con l'applicazione necessaria »?.

Certamente non sono d'accordo con lo scrittore, Bennet, Brassard ed Ekert , pionieri della crittografia quantistica, che rende possibile cifrare messaggi in maniera tale che nessun malintenzionato possa decifrarli.

Purtroppo l'argomento non è di facilissima comprensione in quanto coinvolge concetti di fisica quantistica abbastanza complessi, quindi cercheremo di ridurre la parte più strettamente teorica, ma cercheremo lo stesso di far capire al lettore come questi nuovi sistemi permettano a due interlocutori di scambiarsi informazioni senza correre il pericolo di essere intercettati.

Cominciamo definendo la meccanica quantistica o fisica quantistica quell'insieme di teorie fisiche, formulate nel biennio 1925-1927 ad opera di W. Heisenberg, e Dirac che descrivono il comportamento del mondo microscopico, cioè di particelle la cui grandezza è dell'ordine di quelle dell'atomo o anche inferiori, comportamento non spiegabile con le leggi della fisica classica .

In anni più recenti tali teorie hanno trovato importanti applicazioni per creare dispositivi utili all'uomo, in particolare sistemi per il trattamento dell'informazione: infatti i fenomeni

quantistici permettono di creare degli apparati in grado di trovare la soluzione di problemi irrisolvibili con le tecnologie che si basano sulla fisica classica, come quelli attuali.

La meccanica quantistica applicata ai computer ha determinato una vera rivoluzione in quanto i calcolatori tradizionali, per quanto potenti, hanno, comunque, delle limitazioni computazionali che non permettono di risolvere certi problemi in tempi molto brevi. Mentre un calcolatore quantistico ha elevatissime capacità di calcolo, teoricamente infinite, che permetterebbero di effettuare la fattorizzazione di un numero anche molto grande in tempi brevissimi e quindi la sicurezza di codici come l' RSA sarebbe violata con la massima facilità.

Alla luce di questo fatto, è chiaro non basta più aumentare la lunghezza delle chiavi o la complessità degli algoritmi per rendere sicuro un documento da trasmettere, ma bisogna ricorrere a qualcosa di completamente nuovo.

Abbiamo visto che per utilizzare il codice Vernam, che fa parte di quel sistema detto “blocco usa-e-getta”(“one time pad”), in cui la chiave è lunga quanto il messaggio; occorre innanzi tutto produrre chiavi segrete realmente casuali e rinnovarle praticamente ogni volta.

Quindi, anche la sicurezza di questo metodo dipende, a sua volta, dalla sicurezza relativa alla distribuzione e alla conservazione delle chiavi tra mittente e destinatario

L'idea nuova è la crittografia quantistica, che non è un nuovo sistema crittografico, e che consente di risolvere tale problema, in quanto è possibile distribuire coppie di chiavi identiche in modo assolutamente sicuro tra due interlocutori, in quanto la distribuzione della chiave quantistica avviene contemporaneamente alla sua generazione, pertanto due utenti possono generare e condividere le chiavi per i loro messaggi segreti senza alcuna necessità di incontrarsi preventivamente o usare canali, che potrebbero non essere sicuri, per scambiarsele.

L'idea, in verità, non è poi così recente. Essa risale alla fine degli anni '60, quando uno studente di dottorato della Columbia University, Stephen Wiesner, ebbe per primo l'intuizione della crittografia quantistica e scrisse un articolo su ciò che aveva intuito. Ma l'idea era talmente avanzata per quei tempi che fu quasi rifiutata.

Wiesner ne parlò ad un suo amico, Charles Bennett, che, invece, si rese conto dell'importanza dell'intuizione del giovane, ma non era in grado di tradurla in pratica. Per dieci anni, circa, Bennett continuò, però, a lavorare su questo problema, e quando divenne ricercatore presso i laboratori Watson dell'IBM illustrò le teorie di Wiesner a Gilles Brassard, un informatico dell'università di Montreal ed insieme riuscirono a risolvere il problema.

Nacque così il cosiddetto protocollo ormai noto come BB84 che consente lo scambio di una chiave in maniera sicura tra due utenti che non dispongono di alcuna informazione segreta in comune.

Gli utenti che ricorrono a chiavi crittografiche quantistiche, infatti, sono in grado di accorgersi direttamente se vi siano stati tentativi d'intercettare la chiave durante la sua generazione, e quindi possono decidere se utilizzarla o meno. Inoltre, anche nel caso in cui l'informazione sia stata codificata, il contenuto dell'intercettazione non potrà più, per principio, essere trasmesso.

Per spiegare in modo abbastanza comprensibile il problema riportiamo un esempio del professor Rodolfo Zunino docente del Corso di Laurea Specialistica in Ingegneria Eletttronica dell'Università di Genova:

“La crittografia quantistica sfrutta questo principio per costruire un canale di comunicazione a prova di intercettazione. Poniamo che Alice voglia trasmettere a Bob un bit (0/1); allora prende una particella elementare (un fotone, ad esempio) e la “impacchetta” quantisticamente in modo che solo Bob, misurandolo, possa rilevare se vale 0 oppure 1; quindi glielo spedisce. Un malintenzionato che intercetta il fotone lungo il suo viaggio si trova di fronte ad una grama scelta: se effettua una misura per leggere il bit trasmesso, disturberà il fotone e non potrà più reimpacchettarlo come lo aveva confezionato Alice e quindi Bob si accorgerà dell'intrusione. Se invece l'intercettatore lascia passare indisturbato il fotone, non potrà avere alcuna informazione da esso.

È uno schema semplice ma molto efficace perché si basa su una legge di natura, e quindi la rottura della crittografia quantistica presuppone una confutazione od una revisione delle teorie quantistiche.”

Anziché scendere ulteriormente nei particolari teorici e tecnici di questo tipo di trasmissione segreta di informazioni, che, ripeto, forse potrebbe risultare un po' difficoltoso, vorrei soffermarmi su di un altro concetto, quello della cosiddetta firma digitale: la firma digitale, o firma elettronica qualificata, è basata sulla tecnologia della crittografia a chiavi asimmetriche ed è un sistema di autenticazione di documenti digitali da non confondersi assolutamente con la firma autografa digitalizzata, cioè la rappresentazione digitale di un'immagine corrispondente alla firma autografa.

La firma digitale è, in genere, contenuta, dentro una smart card (simile ad un bancomat), cioè una card che contiene un microprocessore; la firma digitale attesta la volontà del titolare della chiave privata di sottoscrivere il documento informatico e quindi di assumere la responsabilità del suo contenuto.

Grazie alla cosiddetta legge Bassanini un documento informatico dotato di firma digitale ha lo stesso valore legale di un tradizionale documento cartaceo con sottoscrizione autografa. Vediamo in dettaglio in cosa consiste.

Il processo di firma digitale si basa sulla crittografia asimmetrica: ogni titolare dispone di una coppia di chiavi, una privata - segreta e custodita sulla Smart Card e protetta da un codice di accesso (PIN) - l'altra pubblica - custodita e pubblicata dall'Ente Certificatore, autorizzato dal Dipartimento per l'innovazione e le Tecnologie. - che viene usata per la verifica della firma. Le due chiavi sono collegate in maniera univoca, ciononostante dalla chiave pubblica è impossibile risalire a quella privata.

Parliamo, ora, di un progetto partito nel 2004 e chiamato SECOQC, acronimo che sta per "Sviluppo di una rete globale per comunicazioni sicure basate sulla cifratura quantistica" che vede coinvolti importanti istituti di ricerca di 12 paesi europei, tra cui l'Italia, per un totale di 41 partners, come il CNR, il Dipartimento di Fisica dell'Università di Pavia e il Politecnico di Milano (equipe guidata dal prof. Cova), centri di ricerca universitari, aziende specializzate e laboratori.

Lo scopo del progetto è quello di sconfiggere lo spionaggio informatico economico e industriale, effettuato in gran parte attraverso la rete di sorveglianza mondiale Echelon. Questo sistema fu progettato e viene tuttora amministrato dalla NSA americana (National Security Agency) ed ha lo scopo di intercettare normali e-mail, fax, telex e telefonate che viaggiano nella rete di telecomunicazione mondiale. Più precisamente esso è un nome in codice che si riferisce ad una rete informatica, segreta fino al 1997, capace di controllare l'intero globo e di intercettare, selezionare e registrare ogni forma di comunicazione elettronica. E' composta da satelliti artificiali, super computer e un certo numero di stazioni a terra in grado di ricevere informazioni dai satelliti artificiali presenti in orbita. Gli obiettivi di Echelon non sono solo militari, ma anche civili, come ad esempio governi, ambasciate, cittadini comuni di qualsiasi paese"².

Cominciate a sentirvi dei veri 007? Bene, perché il giallo si infittisce, come si usava dire una volta, e noi rivolgiamo la nostra attenzione ad un altro sistema molto affascinante per nascondere un segreto: mi riferisco a quella tecnica che viene indicata con il nome di steganografia. La parola *steganografia* deriva dall'unione dei due vocaboli greci **στεγνο** (rendo occulto, nascondo) e **γραφη** (la scrittura) e, come la crittografia, vuole rendere nascosta un'informazione, ma a differenza di quest'ultima, non "trasforma" il contenuto del messaggio, ma nasconde il messaggio stesso dentro un altro contesto, apparentemente insignificante.

Anche in questo caso l'idea non è certo recente; Erodoto racconta un curioso episodio che potrebbe rappresentare uno dei primi esempi di steganografia: un nobile persiano fece tagliare a zero i capelli di uno schiavo fidato, fece tatuare un messaggio sul suo cranio e, una volta che i capelli furono ricresciuti, inviò lo schiavo dal destinatario del messaggio, con la sola istruzione di tagliarseli nuovamente.

Non proprio in tempo reale, ma originale....

² Fazio Angela e Guidi Luca dal sito <http://www.cli.di.unipi.it/~guidi/echelon/tesi.html#che>

Un altro esempio è costituito dagli inchiostri invisibili, che, usati su carta normale non lasciano alcuna traccia, ma se il foglio viene sottoposto ad una fonte di calore diventano visibili; un metodo simile fu utilizzato, per esempio, durante la seconda guerra mondiale, usando l'inchiostro di cobalto reso visibile con particolari reagenti chimici.

Un altro espediente, usato sempre dai tedeschi, fu quello dei cosiddetti "micropunti fotografici": si tratta di fotografie della dimensione di un punto dattiloscritto che, una volta sviluppate e ingrandite, diventano pagine stampate di buona qualità e possono contenere molte informazioni.

Padre della steganografia è considerato l'abate Giovanni Tritemio (1462-1516) autore di due trattati sull'argomento, "Steganographia" e "Clavis Steganographiae", nei quali l'abate spiega come comunicare un messaggio segreto, nascondendolo in un testo, a prima vista, normale e quasi privo d'interesse.

Questi pochi esempi dovrebbero aver chiarito ulteriormente la differenza tra la crittografia e la steganografia, che hanno scopo comune, ma metodologie diverse.

Ricordate i famosi "pizzini"? Nicola Amato, autore di un interessante libro dal titolo "La Steganografia da Erodoto A Bin Laden" afferma: "Il pizzino, per antonomasia, è un canale di comunicazione nascosto e, molto spesso, celato all'interno di dinamiche comunicazionali palesi. Ed è proprio l'essenza del concetto della steganografia, ossia il consentire a due persone di comunicare tra loro senza che una terza persona si avveda del fatto che una qualsiasi comunicazione stia avvenendo..."

E' facilmente comprensibile che l'enorme sviluppo delle nuove tecnologie ha fornito agli esperti in steganografia tecniche e mezzi sempre più sofisticati e difficili da scoprire. Le immagini sono la copertura più utilizzata, ma non solo, anche file PDF, file HTML (pagine Web) e file MP3. Questa tecnica può servire, per esempio, per nascondere all'interno di un file informazioni sul copyright e proteggere l'autore da usi non autorizzati da parte di terzi; si racconta che il pittore Thomas Kinkade firmi le sue opere più significative usando inchiostri mescolati al DNA del proprio sangue, proteggendo, così, i suoi estimatori e proprietari di suoi quadri da possibili imitazioni.

Purtroppo, però, la tecnica è usata, anche, in attività criminali, quali terrorismo e pedofilia.

Come esempio, vediamo come si può nascondere dei dati in un'immagine. Si utilizzano due file: quello contenente una foto di copertura nasconderà le informazioni, e uno con il messaggio che si vuole nascondere. Questo messaggio potrà essere del testo in chiaro o un testo cifrato, o, addirittura, un'altra immagine, o comunque qualsiasi altra informazione codificata in bit che sostituiscono i "bit meno significativi" delle immagini digitalizzate. Il risultato finale, a occhio nudo, appare identico a ad uno non alterato, e, anche se ciò non fosse e la qualità dell'immagine presentasse qualche imperfezione non sarebbe facile scoprirne la causa: si attribuirebbe l'errore ad una tecnica di digitalizzazione non perfettamente applicata o ad un difetto di visualizzazione.

Abbiamo accennato all'uso criminale della steganografia ed un esempio è fornito dal caso di cui parlò Usa Today il 6 febbraio 2001 che indicò Napster (il sito Internet che permette di "scaricare" file musicali MP3 gratuitamente) come un mezzo usato dai terroristi di tutto il mondo per lo scambio di messaggi in maniera anonima.

Quando a New York fu avviato il processo per le stragi alle ambasciate Usa avvenute nell'agosto del 1998, (224 morti e altre 4mila feriti), ad opera di Osama Bin Laden, emerse che la sua organizzazione usava la rete Internet per scopi criminali. Sempre secondo il quotidiano americano, infatti, la rete terroristica di Bin

Laden usava anche siti a luci rosse e chat-room sportive della Rete per comunicare le istruzioni per attività terroristiche e scambiarsi mappe e fotografie di obiettivi strategici con la tecnica prima illustrata.

Il nostro viaggio nel mondo della crittografia è finito, ma è chiaro che sono ancora molti gli aspetti che potrebbero essere affrontati; noi preferiamo lasciare al lettore la scelta di continuare o meno ad approfondire l'argomento: noi abbiamo gettato l'esca e ora tocca a voi decidere se abboccare.