Codici segreti: l'antica arte della crittografia diventa una scienza moderna*

Renato Betti

Dipartimento di Matematica, Politecnico di Milano

1. Introduzione

Verso la fine degli anni Sessanta del Novecento, sotto l'influenza dei rapidi sviluppi dei sistemi di calcolo automatico, le vecchie macchine cifranti elettromeccaniche usate per scopi di crittografia – vale a dire per trasmettere messaggi al riparo da possibili, indesiderate, intercettazioni – vennero progressivamente sostituite da dispositivi elettronici che, oltretutto, garantivano maggiore velocità, maggiore sicurezza e risparmio economico. Allo stesso tempo, il grande pubblico venne a conoscenza di alcuni successi crittografici di notevole rilievo che, fino ad allora, erano noti ai soli specialisti di questioni militari, diplomatiche o commerciali. L'immaginazione fu colpita soprattutto da vicende belliche relative alla Seconda Guerra Mondiale, nella quale si intrecciano spionaggio, cultura meccanica e capacità di addentrarsi nelle strutture logiche e combinatorie più intricate, come nel caso della macchina Enigma, da parte delle forze alleate in Europa, della decrittazione del codice giapponese Purple durante la guerra nel Pacifico, o quella, resa nota in tempi più recenti, della sistematica lettura della tedesca Geheimschreiber da parte del controspionaggio svedese. Fu in questo contesto problematico e tecnologico che, nel 1976, due scienziati americani, Whitfield Diffie e Martin Hellman diedero vita al nuovo settore della *crittografia a chiave pubblica*, il quale, solo due anni più tardi ricevette una concreta implementazione nel sistema detto RSA dal nome dei suoi ideatori: Ronald Rivest, Adi Shamir e Leonard Adleman[1].

L'uso di metodi crittografici è vecchio di migliaia di anni e lo sviluppo concettuale e pratico di numerose procedure è da sempre corso in parallelo con l'applicazione di strutture formali. Ora, sotto le nuove esigenze di riservatezza che caratterizzano le necessità operative moderne, questi metodi stavano manifestandosi sempre più connessi e dipendenti dall'autentica ricerca scientifica, in particolare matematica. È l'esigenza di nuove, più sicure e generali, modalità di trasmissione dei dati. Se, fino ad un certo punto dello sviluppo, le esigenze di riservatezza sono rimaste confinate a problemi di carattere diplomatico o militare – e quindi all'occultamento di informazioni trasmesse lungo linee poco sicure – oggi è pressante la necessità di proteggere la grande quantità

* Lezione tenuta il 20 ottobre 2009 presso l'Auditorium del Consiglio regionale della Toscana, nell'ambito dell'edizione 2009 di *Pianeta Galileo*.

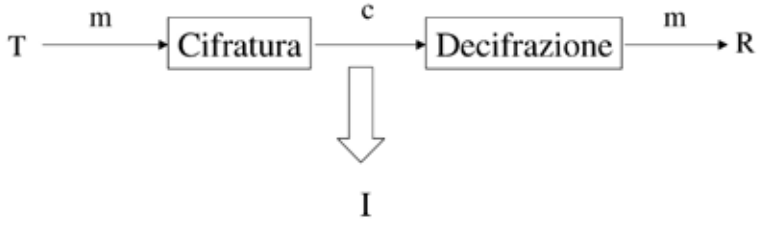
di dati che vengono elaborati dai grossi sistemi di calcolo. Con la crescita del commercio on-line, della posta elettronica, delle transazioni bancarie a distanza etc. un accesso illegittimo alle informazioni costituisce un pericolo enorme per la società.

Con uno slogan che chiarisce il sottotitolo di questo intervento: la *chiave pubblica* sta provvedendo a trasformare la crittografia da un'antica 'arte' in una scienza moderna, in grado di affrontare adeguatamente questi problemi. Ciò avviene grazie all'incontro della pratica millenaria della crittografia, dotata soprattutto di regole empiriche, con una scienza formale rigorosa – la *teoria dei numeri* – che, nella concezione di Gauss è la "regina della matematica" (che a sua volta, sempre nella sua concezione, è la "regina della scienza").

Qui intendiamo fornire qualche elemento per accostarsi all'incontro appena accennato. In particolare, con l'intenzione di dare un'idea della nozione di *chiave pubblica* e di *canale asimmetrico* lungo il quale è possibile trasmettere con buona sicurezza le informazioni riservate, chiarire il meccanismo di base del sistema stesso e mettere in luce altre notevoli applicazioni (quali la firma digitale o il sorteggio a distanza). A questo scopo, occorrerà ricordare gli aspetti matematici essenziali della *aritmetica modulare*, sulla cui base avviene l'implementazione del sistema RSA. Naturalmente sarà necessario anche introdurre alcuni elementi di carattere storico-concettuale, allo scopo di ambientare propriamente il discorso nel suo sviluppo reale.

2. Il principio di Kerckhoffs

Lo schema essenziale del problema crittografico è il seguente:



Un *trasmettitore* T intende mandare al *ricevitore* R il messaggio riservato "m", al riparo dalla lettura di un "intercettatore" I. A questo scopo lo *cifra* secondo qualche regola nota solo a lui ed al suo interlocutore, in modo che questi sia in grado di *decifrare* il messaggio cifrato "c" e ricostruire l'originale "m". L'attesa è che l'intercettatore I, pur a conoscenza del messaggio cifrato "c", non sia in grado di decifrarlo o, cosa che sarebbe peggiore, non sia in grado di *decrittare*, o *infrangere*, il sistema, vale a dire mettersi in condizione di leggere tutti i messaggi che vengono scambiati con quella procedura.

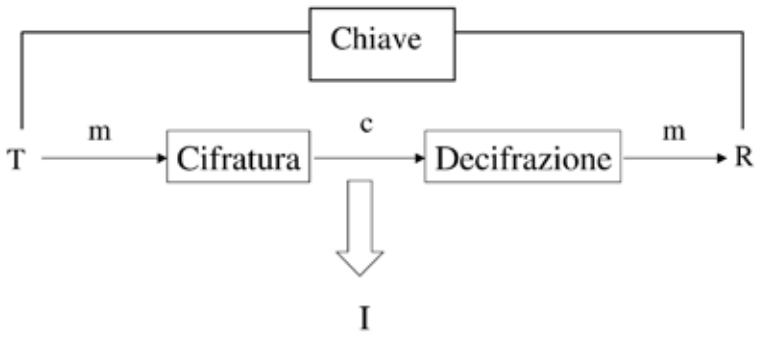
Il problema crittografico si può anche vedere come una forma di 'competizione' che si stabilisce fra la cifratura e la decrittazione[2], vale a dire fra la capacità di ideare sistemi sempre più sicuri ed efficienti e la disposizione a renderli leggibili a partire da qualche conoscenza a essi relativa (ad esempio avendo a disposizione alcuni esemplari cifrati e la loro espressione in chiaro).

Il nome del filologo olandese Auguste de Kerckhoffs (1835-1903) è legato a uno dei principi che viene riconosciuto da tutti. Nel suo lavoro *La cryptographie militaire*,[3] che pure è relativamente recente rispetto al millenario sviluppo della crittografia, fra le altre richieste da fare ad un buon sistema, viene sottolineata l'importanza della *chiave crittografica*:

> È necessario che non occorra il segreto e che [il sistema] possa senza danno cadere in mano nemica…. La chiave deve essere comunicata e conservata senza ricorrere a note scritte, ed essere cambiato o modificata a discrezione dei corrispondenti.

In sostanza, la sicurezza di un sistema crittografico dipende *solo* dalla segretezza di una informazione essenziale, la *chiave* – necessariamente condivisa dai corrispondenti – che deve evitare quanto possibile di essere incorporata in un supporto materiale per non cadere in mano nemica, giacché c'è da aspettarsi con grande probabilità che il sistema stesso possa essere noto a chi intercetta: quello che ne rende impossibile l'uso è allora la non conoscenza della chiave. Qui si concentra tutta la sicurezza del cifrario.

Allo scopo di scambiarsi la chiave e quando occorre modificarla, è necessario un *canale sicuro* che sia al riparo dalle intercettazioni: magari un canale temporaneo, o che forse si può stabilire in condizioni speciali, utile per brevi comunicazioni e comunque non disponibile per lunghi messaggi cifrati. Lo schema precedente si arricchisce con la presenza di questo nuovo canale e, soprattutto, l'idea di chiave è riconosciuta come l'elemento fondamentale del sistema crittografico. Vale la pena di mettere in evidenza il ruolo della chiave dal punto di vista di alcuni dei sistemi che sono stati sviluppati nel tempo.



Un'ulteriore osservazione, prima di entrare nel merito delle scritture cifrate, riguarda il fatto che, quando la matematica interviene a collaborare con qualche altra disciplina, inevitabilmente opera delle unificazioni grazie ai propri strumenti formali. In questo caso continuiamo a riferirci al problema della sicurezza di un messaggio cifrato, ma algoritmi basati su analoghi principi hanno il loro funzionamento anche in un'altra serie di problemi: firma digitale (riconoscimento del mittente), autenticità del testo, sorteggi a distanza, problemi a conoscenza zero (come convincere qualcuno che si possiede un segreto senza rivelarlo?) e altri, sui quali verrà accennato al termine.

3. Le prime scritture nascoste

La necessità di possedere metodi efficienti per comunicare in modo riservato è stata avvertita da sempre, soprattutto per motivi militari o diplomatici, o anche sentimentali. Già Erodoto, in relazione alle guerre fra Grecia e Persia nel V secolo a.C., racconta episodi importanti nei quali opportuni ordini militari vengono accuratamente celati in modo da non farli scoprire all'avversario. Il modo più istintivo è per l'appunto quello di nascondere il messaggio: in questo caso si parla propriamente di *steganografia*. Mentre quando non si nasconde il messaggio, bensì il suo contenuto – e risulta evidente a tutti che il vero messaggio non è il testo trasmesso – allora si ha a che fare con la *crittografia*, termine usato per la prima volta, a quanto sembra, nel 1641 da John Wilkins, uno dei fondatori della Royal Society, ma pratica antica quanto l'uomo.

Nel senso della crittografia, uno dei primi esempi documentati di messaggio cifrato viene fatto risalire a Giulio Cesare, che era solito ricorrervi nella guerra contro i Galli. Secondo la *Vita Caesarorum* di Svetonio (II secolo d.C.) il sistema cifrante consisteva nel "traslare circolarmente" l'alfabeto, sostituendo di conseguenza tutte le lettere del messaggio in chiaro. Ad esempio, con una traslazione di 2 unità dall'alfabeto in chiaro (riga superiore) si ottiene quello cifrato (riga inferiore):

A B C D E F G H I L M N O P Q R S T U V Z

C D E F G H I L M N O P Q R S T U V Z A B

Metodi di questo genere sono noti oggigiorno come *cifrari di Cesare*. È chiaro che si hanno a disposizione solo 20 cifrari distinti di questo tipo, e la chiave cifrante, il segreto speciale, è il numero n (compreso fra 1 e 20) che specifica di quanto è necessario traslare l'alfabeto in chiaro per ottenere quello cifrato. Un numero molto esiguo di cifrari che si presta ad essere eluso con pochi tentativi. Una variazione che aumenta enormemente il numero di cifrari distinti consisterebbe nell'assumere una qualunque permutazione delle 21 lettere dell'alfabeto in chiaro invece di eseguire una semplice traslazione. I cifrari distinti diventano in questo caso 21! – un numero altissimo, dell'ordine di grandezza di 10^{18} – mettendosi al riparo da possibili decrittazioni dovute a qualche tentativo ben mirato. In questo caso la chiave cifrante è costituita proprio da tutta la permutazione. E si capisce allora che il metodo contravviene a una delle regole auree che saranno in seguito riconosciute da Kerckoffs: troppo difficile conservare a mente l'intera permutazione di 21 lettere e pericoloso registrarla su un supporto materiale allo scopo di ricordarla.

Come spesso avviene, si raggiunge un compromesso. Precisamente l'idea è quella di *generare* una permutazione con un meccanismo semplice, efficiente e facile da memorizzare: a questo punto la vera chiave è diventata il metodo generatore. Ad esempio, si può usare una parola chiave che non abbia lettere ripetute, come "domani", oppure eliminare le ripetizioni da un termine scelto (ad esempio "ierlaltro" diventa "ierlato") e utilizzare la parola per indicizzare le permutazioni partendo da una posizione convenuta: la parola chiave viene usata a partire da quella posizione e, nel seguito, si procede

alfabeticamente, saltando ovviamente le lettere già usate. Ad esempio, la permutazione che si ottiene con la parola chiave "ierlaltro" a partire dalla posizione 4 è quella che segue:

A B C D E F G H I L M N O P Q R S T U V Z
U V Z I E R L A T O B C D F G H M N P Q S

La memorizzazione della chiave (ierlaltro, 4) è agevole per tutti e un cifrario di questo genere sembra al riparo da attacchi basati su tentativi ripetuti. Ma …

Il crittoanalista, cioè colui che tenta di infrangere il cifrario, posto di fronte ad un testo cifrato abbastanza lungo, è a conoscenza del fatto che il testo in chiaro è scritto in italiano (o in inglese, o in russo …) e che riguarda affari (o problemi diplomatici, militari, commerciali, sentimentali …) e, soprattutto, conosce il *dizionario delle frequenze* con cui si ripetono le lettere nei discorsi del dato argomento. In altri termini, approfitta delle informazioni che, in ogni lingua e per ogni tipo di discorso, i linguisti e gli statistici hanno rilevato prendendo in esame campioni lunghi e articolati. Ad esempio, sa che in un dato contesto italiano le frequenze sono le seguenti[4]:

Lettera	%	Lettera	%	Lettera	%
a	11,8	h	1,5	q	0,5
b	0,9	i	11,3	r	6,4
c	4,5	l	6,5	s	5
d	3,7	m	2,5	t	5,6
e	11,8	n	6,9	u	3
f	1	o	9,8	v	2,1
g	1,7	p	3	z	0,5

Studiando le frequenze con cui compaiono le varie lettere nel testo trasmesso – che deve essere abbastanza lungo e significativo – si possono fare delle ipotesi attendibili riguardo al loro significato in chiaro. Altre informazioni si ottengono ad esempio dalla frequenza delle lettere ripetute, da particolari associazioni o dalla loro mancanza … Con un certo numero di tentativi ben mirati è possibile infrangere ogni cifrario di quelli mostrati in precedenza[5].

4. I cifrari polialfabetici

Analizzando i sistemi cifranti presi finora in considerazione, emerge il difetto che li rende immediatamente attaccabili: uno studio accurato delle frequenze. Il problema è che questi cifrari sono *monoalfabetici*, nel senso che una lettera viene cifrata *sempre* con la stesso simbolo, mantenendo quindi nel testo cifrato le stesse frequenze del testo in chiaro. Come rendere uniformi le frequenze nel testo cifrato?

L'idea è quella di ricorrere ad un cifrario *polialfabetico,* vale a dire di associare ad ogni lettera in chiaro un simbolo cifrato in maniera *dipendente dal contesto* nel quale avviene la cifratura. Ad esempio, visto che in italiano la frequenza della lettera "a" è quasi del 12%, si potrebbero usare 12 simboli diversi $X_1, X_2, \ldots, X_{12}$: il primo viene usato

la prima volta che compare la lettera "a" nel testo in chiaro, il secondo la seconda volta e così via, circolarmente. Analogamente per tutte le altre lettere, tenendo conto delle corrispondenti frequenze. È chiaro, che in questo modo, tutti i simboli cifranti – che devono essere in numero di 100 – ricorrono con la stessa frequenza.

Ma si capisce subito che anche questa idea è impraticabile. In contrasto con il principio di Kerckhoffs, bisognerebbe tenere a mente una tabella che ad ogni lettera dell'alfabeto italiano associa un certo numero di simboli. O registrarla da qualche parte. Niente da fare. Occorre cercare un altro compromesso allo scopo di generare, ancora una volta, in maniera semplice, l'alfabeto cifrante in dipendenza dal contesto nel quale ci si trova ad operare. Ed è qui che si sposta l'idea di chiave.

All'albore del Rinascimento, metodi polialfabetici, del genere di quelli che saranno descritti, sono sorti praticamente in ogni paese europeo. E ogni paese, spesso ogni regione o provincia, rivendica la priorità dell'idea. Questo fatto segnala forse che l'esigenza era sentita da molti e che le idee erano mature per essere realizzate. Uno dei primi esempi è legato al nome di Leon Battista Alberti, nella seconda metà del Quattrocento[6].

L'idea dell'Alberti è quella di usare due dischi concentrici, in grado di ruotare l'uno rispetto all'altro, e contenenti l'alfabeto in chiaro (il disco esterno) e quello in cifra (il disco interno). Dopo la cifratura di una lettera, ottenuta facendo corrispondere le lettere dei due dischi che sono una sopra l'altra, il disco esterno viene ruotato di una *tacca*, e la corrispondenza fra le lettere cambia – di fatto cambia tutto l'alfabeto cifrante, che si ripete dopo un periodo lungo quanto sono le lettere che compaiono nei dischi. È chiaro che il congegno può cadere in mano nemica senza danno: la chiave crittografica in questo caso è data dall'assetto iniziale dei due dischi.

Vale la pena di osservare che su un simile principio funzionava anche la macchina cifrante Enigma usata dall'esercito tedesco durante la seconda guerra mondiale, e decrittata fin dal 1942 dalla *intelligence* inglese, con il contributo decisivo del matematico Alan Turing[7]: fra i vari congegni, un certo numero di dischi rotanti provvedeva alla cifratura mediante collegamenti elettrici. Dopo ogni lettera il primo disco ruotava con uno scatto e proponeva un nuovo collegamento, dopo tutto un giro lo scatto competeva al secondo disco rotante, e poi al terzo e così via, in sequenza, come adesso avviene con i moderni contachilometri meccanici.[8]

La priorità dell'Alberti compete senz'altro all'ideazione di un congegno meccanico per cifrare. Di fatto, il cifrario che, dal Rinascimento, rimase in uso per molti secoli e che in qualche modo costituì il paradigma di ogni metodo di cifratura polialfabetica è legato al nome del diplomatico francese Blaise de Vigenère (1523-1596). L'idea, contenuta nel suo *Traité des chiffres ou secrètes manières d'escrire* del 1586, è quella di utilizzare per ogni lettera un diverso alfabeto cifrante, il quale viene *indicizzato* da una parola chiave. Non è più necessario che la parola chiave sia priva di lettere ripetute. Nell'esempio seguente riprendiamo la chiave "ierlaltro", senza modifiche. Tutti i possibili 20 cifrari (*à la Cesare*) vengono riportati sotto l'alfabeto in chiaro come nello schema che segue:

A B C D E F G H I L M N O P Q R S T U V Z
B C D E F G H I L M N O P Q R S T U V Z A
C D E F G H I L M N O P Q R S T U V Z A B
D E F G H I L M N O P Q R S T U V Z A B C
E F G H I L M N O P Q R S T U V Z A B C D
F G H I L M N O P Q R S T U V Z A B C D E
G H I L M N O P Q R S T U V Z A B C D E F
H I L M N O P Q R S T U V Z A B C D E F G
I L M N O P Q R S T U V Z A B C D E F G H
L M N O P Q R S T U V Z A B C D E F G H I
M N O P Q R S T U V Z A B C D E F G H I L
N O P Q R S T U V Z A B C D E F G H I L M
O P Q R S T U V Z A B C D E F G H I L M N
P Q R S T U V Z A B C D E F G H I L M N O
Q R S T U V Z A B C D E F G H I L M N O P
R S T U V Z A B C D E F G H I L M N O P Q
S T U V Z A B C D E F G H I L M N O P Q R
T U V Z A B C D E F G H I L M N O P Q R S
U V Z A B C D E F G H I L M N O P Q R S T
V Z A B C D E F G H I L M N O P Q R S T U
Z A B C D E F G H I L M N O P Q R S T U V

Il testo da cifrare sia "NEL MEZZO DEL CAMMIN DI NOSTRA VITA….". Per mantenerlo segreto lo cifriamo con la chiave "*IERLALTRO*". Sovrapponiamo la chiave tanto quanto basta:

N E L M E Z Z O D E L C A M M I N D I N O S T R A V I T A
I E R L A L T R O I E R L A L T R O I E R L A L T R O I E

La cifratura della prima lettera ("N") avviene con l'alfabeto che comincia con "*I*", la

quale si trova immediatamente sotto la "N" in chiaro – dunque, all'incrocio della riga "I" con la colonna "N" si ottiene "V" – similmente la "E" viene cifrata a partire con l'alfabeto che comincia con "*E*", la "L" dalla "*R*" e così via, ottenendo:

V I D V E I S G R O P.....

Si continui per esercizio e si osservi che le prime tre lettere "E" sono cifrate ordinatamente con "*I*", "*E*" e "*O*", viceversa, due "*V*" del messaggio cifrato corrispondono rispettivamente ad "N" ed "M": ecco in funzione un cifrario polialfabetico!

Sembra di essere al riparo degli attacchi statistici. Ma in realtà questi iniziarono fin dall'inizio, in maniera poco sistematica, ma efficiente, ad opera soprattutto dello scienziato e filosofo Giovan Battista della Porta, che viene considerato uno dei principali crittografi del Rinascimento.[9] Dagli attacchi sporadici, spesso legati anche a conoscenze degli autori e dei possibili messaggi, delle abitudini personali e delle mode, si passa progressivamente a trovare un metodo. Il primo attacco sistematico naturalmente viene portato alla *lunghezza della chiave*, trovata la quale tutto si ripete e si può considerare di lavorare con *spezzoni* monoalfabetici.

Il merito di aver escogitato un metodo generale per attaccare con successo i cifrari polialfabetici spetta ad un ufficiale dell'esercito prussiano, Friedrich W. Kasiski, il quale trovò una regola per determinare la lunghezza della chiave e la pubblicò in un lavoro del 1863: *Die Geheimschriften und die Dechiffrirkunst*. Intorno all'inizio del Novecento era ormai generalmente accettata la vulnerabilità dei sistemi polialfabetici ed i sistemi *à la Vigènere* persero progressivamente interesse. La cosa divenne maggiormente evidente nel 1925 in seguito alla scoperta del cosiddetto *indice di coincidenza* – una tecnica di conteggio delle coincidenze di termini nel testo in chiaro ed in quello cifrato – messo a punto dallo statistico militare americano William F. Friedman (1891-1969).

Ormai, intorno all'inizio del Novecento, i cifrari polialfabetici erano superati. Ma nel frattempo siamo arrivati al periodo dell'elaborazione automatica: avanzano le macchine cifranti e con esse avanzano nuove idee.

5. I cifrari perfetti

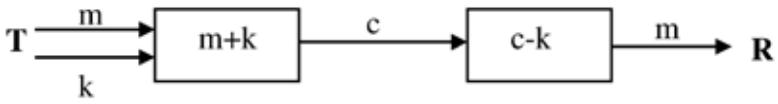
Nel contesto dei sistemi meccanici di calcolo, fin dall'inizio del Novecento, sorge l'idea che si possa costruire un *cifrario perfetto*, vale a dire un cifrario che non può essere infranto. La prima realizzazione risale al 1917 e porta il nome dell'ingegnere americano delle comunicazioni Gilbert Vernam, il quale si rende conto che a questo scopo è necessario che la chiave cifrante abbia tanta informazione quanto i possibili messaggi da cifrare. Un'apparente contraddizione che tuttavia, come è successo altre volte nel corso del tempo, serve solo a spostare il livello al quale si deve tener conto della chiave.

Il messaggio, ormai, a questo punto dello sviluppo tecnologico, è una successione di *bit*, una stringa numerica binaria, e la chiave è un'altrettanto lunga sequenza di *bit* generata in modo casuale e custodita in un libro delle chiavi – detto *one-time pad*, per intendere che deve essere usato una sola volta giacché l'uso ripetuto delle chiavi mette a rischio tutto il complesso. Il sistema non è decrittabile con metodi statistici, poiché

ogni carattere in chiaro può essere rappresentato con la stessa probabilità da un qualunque carattere cifrato, e non esistono più modelli perché la scelta della chiave avviene in modo casuale.

Oltre a qualche aspetto particolare, spesso legato al messaggio corrente ed alla scelta dell'operatore, come ad esempio il punto nel quale interviene la chiave, il vero segreto è ormai racchiuso nel metodo di generazione della chiave.

Lo schema è il seguente:



Qui, k rappresenta la chiave e le operazioni di somma e sottrazione sulle cifre binarie del messaggio e della chiave sono proprio, almeno nella prima applicazione, le operazioni di somma e sottrazione *binarie*, le quali si eseguono nello stesso modo, con il vantaggio che il meccanismo per cifrare coincide con quello per decifrare:

±	**0**	**1**
0	0	1
1	1	0

Il sistema è sicuro. Ma la gestione dei libri delle chiavi, spesso ingombranti, che devono essere noti sia al trasmettitore che al ricevitore, i metodi della loro generazione e della loro diffusione, le particolarità legate alle scelte dell'operatore, la non ripetibilità delle chiavi … tutto ciò rappresenta altrettanti punti critici che invitano a cercare nuove modalità per la sicurezza dei sistemi.

L'ostacolo della gestione dei libri delle chiavi si aggira spesso aumentando a dismisura la complessità dell'algoritmo cifrante, pur di riportare la chiave a una dimensione molto alta ma più facilmente gestibile. Così, nella seconda metà del Novecento, si ricorre in maniera massiccia a macchine da calcolo veloce sempre più potenti: ad esempio, lo *standard* normativo per la crittografia commerciale che l'amministrazione degli Stati Uniti fissa a partire dal 1977 allo scopo di evitare il proliferare incontrollato di sistemi cifranti incompatibili l'uno con l'altro – il Des, *Data Encryption Standard* – riposa su una chiave di 48 *bit* più 8 *bit* di controllo, gestibile solo da un grosso elaboratore.

La crittografia è diventata il dominio della 'forza bruta' – da calcolo naturalmente. E, com'era inevitabile, il Des viene decrittato nel 1998.

6. L'idea della chiave pubblica

I problemi precedenti vengono accresciuti di molto dagli usi moderni: basta pensare alla necessità che un *centro* debba rimanere in collegamento riservato con migliaia di utenti, come può accadere ad esempio nel caso di una banca e dei suoi clienti, intenzionati ad operare da casa o da uno sportello automatico. Il problema di distribuire a cia-

scuno una chiave particolare – da riconoscere nel momento opportuno – pone enormi problemi gestionali. Ora, l'idea è di mettere a disposizione di ogni utente una chiave personale, segreta, che lo identifica e che, solo a lui, permette di decifrare i messaggi che gli sono indirizzati. Gli enormi problemi di gestione e distribuzione delle chiavi del sistema *one-time pad* sono virtualmente scomparsi.

A questo scopo, occorre fare ricorso a nuovi principi, e tanto vale usare in maniera sistematica macchine da calcolo sofisticate e potenti. Questa è l'idea della *chiave pubblica*, in quanto opposta alla *chiave condivisa*, segreta, da sempre utilizzata nei cifrari. La chiave pubblica sarà nota a tutti, perché è utile per cifrare i messaggi… ma non per decifrarli. Sarà a conoscenza anche del famigerato intercettatore. La sicurezza di questi sistemi non dipende dalla complessità dell'algoritmo cifrante e non si misura dall'incertezza statistica, ma dalla scoperta e dall'uso di funzioni 'a trabocchetto'[10], che sono funzioni invertibili – giacché devono servire sia per cifrare che per decifrare – facili da calcolare in una direzione ma estremamente difficili da calcolare in senso inverso[11]... a meno che non sia nota qualche informazione supplementare. La cifratura del messaggio avviene con una di queste funzioni, la decifratura con la funzione inversa (che è nota solo a chi riceve il messaggio).

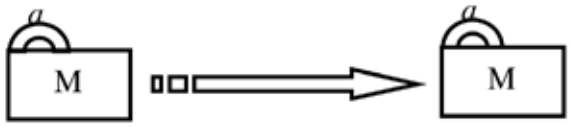
In questi casi si dice anche che il canale lungo il quale avviene la trasmissione è *asimmetrico*, per intendere che il messaggio può muoversi in una sola direzione, contrariamente alla simmetria implicita fra trasmettitore e ricevitore che si ha nel caso della chiave condivisa, posseduta da entrambi e usata sia per cifrare che per decifrare.

La sicurezza del sistema è ormai racchiusa in questa informazione supplementare, che sarà conservata in maniera segreta da chi intende ricevere messaggi riservati, in quanto permette a lui solo di costruire in maniera facile la chiave che inverte la funzione cifrante. In particolare, neppure il trasmettitore, che usa la funzione cifrante a trabocchetto indicatagli dal ricevitore, sarebbe in grado di decifrare il messaggio che ha mandato (ma peraltro non ne ha bisogno).

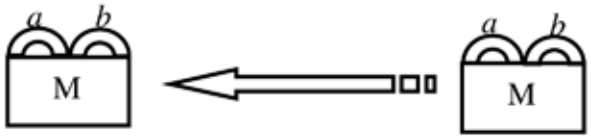
Fra le funzioni a trabocchetto che sono state escogitate, quella più nota – e utilizzata nel sistema RSA – si basa sulla difficoltà pratica nella scomposizione di un intero in fattori primi: se il numero dato ha molte cifre decimali, anche le tecniche più raffinate e i calcolatori più veloci risultano inefficaci. Una stima attendibile, che mette il tempo di fattorizzazione in dipendenza dal numero di cifre, è la seguente (anche se risalente a molti anni fa, risulta ancora molto indicativa):

n° cifre	**tempo**
20	24 min.
50	4 ore
100	74 anni
200	$4 \cdot 10^9$ anni
1000	$3 \cdot 10^{43}$ anni

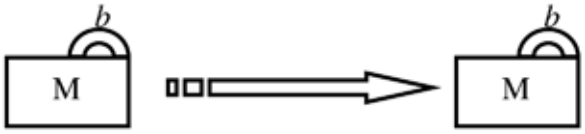
Un paradigma di come sia possibile che ciascuno sia in possesso della propria chiave, individuale, e tuttavia il sistema possa funzionare – nel senso di permettere una trasmissione sicura – si ottiene con il seguente schema:



Il messaggio M viene 'chiuso' in un recipiente mediante una chiave *a* e spedito al ricevitore R: durante il trasferimento è al sicuro, ma R non può entrarne in possesso perché non conosce la chiave. Allora, a sua volta, R applica una propria chiave *b* al recipiente e lo rispedisce al trasmettitore T:



A questo punto, neanche T è in grado di aprire il contenitore (ma non gli interessa, conosce già il contenuto). Però può togliere la propria chiave, rispedirlo e, questa volta, mettere in condizione R di aprire il contenitore:



Sono occorsi tre passaggi, però in ogni caso il messaggio è transitato ogni volta al sicuro dalle intercettazioni.

7. Aritmetica modulare

Il crittosistema RSA implementa le idee della chiave pubblica mediante alcuni teoremi elementari di teoria dei numeri. Ecco gli elementi fondamentali, i quali costituiscono la base della cosiddetta *aritmetica modulare*, la quale riguarda essenzialmente le operazioni aritmetiche, rese modulari rispetto ad un intero assoluto *n*.

Nella sua grande opera *Disquisitiones arithmeticae* del 1801, Carl Friedrich Gauss formalizza la nozione di *congruenza modulo n*:

Definizione. Due interi (relativi) *a* e *b* si dicono congruenti modulo *n* (intero assoluto) se la loro differenza è un multiplo intero di *n*.

Si scrive così: $a \equiv b \pmod{n} \Leftrightarrow a - b = kn$ con $k \in Z$.

È facile vedere che due interi sono congruenti modulo *n* esattamente quando hanno lo stesso resto rispetto alla divisione per *n*. Inoltre, la relazione di congruenza modulo *n* è una relazione di equivalenza (vale a dire soddisfa le proprietà: riflessiva, simmetrica

e transitiva) dunque permette di suddividere l'insieme Z degli interi relativi in classi di equivalenza, rappresentate, ciascuna dal resto rispetto alla divisione per n. Con Z_n indichiamo l'insieme delle *classi di resti* modulo n:

$$Z_n = \{0,1,2,\ldots, n\text{-}1\}$$

È chiaro che ogni intero relativo appartiene ad una ed una sola classe di resti.

L'aritmetica modulare è l'aritmetica dell'insieme numerico Z_n, possibile grazie al fatto che la relazione di congruenza è stabile rispetto alle operazioni di somma e prodotto. In altri termini, la relazione di congruenza condivide con l'uguaglianza le relazioni fondamentali:

$$\begin{cases} a \equiv b \\ c \equiv d \end{cases} \Rightarrow \quad a + c \equiv b + d, \quad ac \equiv bd \pmod{n}$$

L'idea sottostante questa aritmetica è che, in molte considerazioni, quello che interessa non sono i numeri in sé, ma i loro resti della divisione per n. In Z_n si eseguono le operazioni aritmetiche modulo n (per la somma e il prodotto non ci sono difficoltà, per la divisione bisogna prestare qualche attenzione) e si dimostrano risultati teorici analoghi a quelli usuali. Il più immediato è il seguente:

Teorema. In Z_n l'equazione di primo grado $ax = 1$ ha un'unica soluzione se e solo se

$$\text{MCD}(a,n) = 1.$$

Così, per gli interi modulo n, ammettono inverso solo quelli che sono primi con n (vale a dire che non hanno divisori primi non banali in comune con n).

Meno immediato, ma di facile dimostrazione è il seguente risultato (noto come *piccolo teorema di Fermat*):[12]

Teorema. Se p è un numero primo che non divide a, allora $a^{p-1} \equiv 1 \pmod{p}$.

In realtà, per implementare il metodo RSA, occorre una generalizzazione del piccolo teorema di Fermat, ottenuta un secolo dopo da Eulero e che utilizza una funzione particolare: la funzione *totiente* o funzione Φ di Eulero (1707-1783):

Definizione. $\Phi(n)$ è il numero di interi minori di n e primi con n.

I primi valori della Φ sono facili da calcolare:

$$\Phi(1) = 1,\ \Phi(2) = 1,\ \Phi(3) = 2,\ \Phi(4) = 2,\ \Phi(5) = 4,\ \Phi(6) = 2,\ \Phi(7) = 6,\ \ldots\ldots$$

ma in generale il calcolo di $\Phi(n)$ ha la stessa complessità di calcolo della scomposizione di n in fattori primi. Infatti, è immediato calcolare $\Phi(p)$ quando p è un numero primo ($\Phi(p) = p\text{-}1$) ed è facile il calcolo di $\Phi(n)$ quando si conosce la scomposizione di n in fattori primi. Questo risulta dalla seguente proprietà di Φ di essere una *funzione moltiplicativa*.

Teorema. Se MCD$(m, n) = 1$, allora $\Phi(m\cdot n) = \Phi(m)\cdot\Phi(n)$.

Ecco ora la generalizzazione necessaria del piccolo teorema di Fermat:

Teorema (di Eulero-Fermat). Se MCD $(a, \Phi(n)) = 1$ allora $a^{\Phi(n)} \equiv 1 \pmod{n}$.

Abbiamo ormai tutti gli elementi per introdurre il metodo RSA.

8. Il cifrario a chiave pubblica RSA

La chiave pubblica viene scelta da chi vuole ricevere messaggi riservati, diciamolo ancora R, e divulgata a tutti: è per l'appunto pubblica. A questo scopo, R sceglie e fa conoscere due numeri (e, n) in modo tale che e e $\Phi(n)$ siano primi fra di loro: MCD(e, $\Phi(n)$) = 1. Questa è l'unica informazione che comunica: (e, n). Avrà avuto cura, per questioni di sicurezza, di scegliere n molto grande e in modo tale che per lui sia facile il calcolo di $\Phi(n)$: ad esempio scegliendo $n = p \cdot q$ prodotto di due numeri primi con molte cifre. In questo caso $\Phi(n) = (p-1)\cdot(q-1)$.

Poi, R calcola la propria chiave privata: quella che gli permetterà di decifrare i messaggi e che deve tenere rigorosamente segreta. Per ottenere questa chiave deve risolvere un'equazione in $Z_{\Phi(n)}$. Precisamente: $ex \equiv 1 \pmod{\Phi(n)}$. Si osservi che, per il primo teorema enunciato nel paragrafo precedente e per la maniera con cui R ha scelto la sua chiave pubblica (e, n), si ha che questa congruenza ha un'unica soluzione in $Z_{\Phi(n)}$. Diciamo d questa soluzione: è la chiave privata di R la quale, per definizione, soddisfa la relazione $e \cdot d = k \cdot \Phi(n) + 1$ in relazione a qualche intero k.

Ora, il messaggio in chiaro m (un numero intero che supponiamo $< n$) che il trasmettitore T intende inviare in maniera cifrata a R verrà trasformato nel messaggio cifrato $c \equiv m^e \pmod{n}$. Si osservi che T usa esattamente l'informazione che ha ricevuto dalla chiave pubblica di R. E si consideri che, anche se n è un numero molto grande, questa operazione di cifratura non è per lui onerosa pur di avere a disposizione buoni strumenti di calcolo. Adesso il problema è il seguente: come può R ricostruire il messaggio in chiaro utilizzando la chiave privata d? Basta che calcoli un'altra potenza: infatti un semplice conto, effettuato in Z_n, convince che $m \equiv c^d \pmod{n}$. Ecco il conto:

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\Phi(n)+1} \equiv (m^{\Phi(n)})^k m \equiv m \pmod{n}$$

Perché $m^{\Phi(n)} \equiv 1$ per il teorema di Eulero-Fermat e quindi, per la stabilità della relazione di congruenza rispetto al prodotto, vale anche $(m^{\Phi(n)})^k \equiv 1 \pmod{n}$.

In questo modo R ricostruisce il messaggio in chiaro. E si capisce che è l'unico che può farlo, a meno che qualcun altro sia stato così abile da trovare la chiave privata d partendo dalla chiave pubblica (e, n): ma sappiamo che per fare questo avrebbe dovuto scomporre n in fattori primi: e questa operazione è inaccessibile.

9. Firma digitale, autenticità del mittente, sorteggio

Il procedimento che porta alla firma digitale ribalta in un certo senso quello precedente. Chi vuole 'firmare' il proprio messaggio, sia ad esempio R, userà a questo scopo la propria chiave segreta d, ben sapendo che il destinatario, questa volta T, è a conoscenza della sua chiave pubblica (e, n). Non è detto che il messaggio m (che supponiamo ancora un numero $< n$), sia da mantenere segreto. Allora, R in realtà spedisce una coppia di informazioni mod n, precisamente (m, m^d): il messaggio, in chiaro, e la componente m^d, grazie alla quale T può sincerarsi che il mittente non può che essere R.

Infatti, con lo stesso calcolo appena fatto nel caso della sicurezza della trasmissione,

T ricava $m \equiv (m^d)^e \pmod{n}$. Si osservi che, rispetto alla pratica corrente di uso della firma, quella digitale è *contestuale*: la firma dipende anche dal documento che viene firmato.

Una variante di questo procedimento permette di operare in sicurezza a chi abbia una grande quantità di interlocutori che deve saper riconoscere. Sia B, ad esempio, un ente i cui interlocutori sono i *clienti* C_1, C_2,…., C_k (che possiamo pensare siano dei numeri che tengono il posto dei nomi). Allora, B sceglie come prima un intero n in maniera opportuna: ad esempio come prodotto $n = p \cdot q$ di due numeri primi molto grandi. Quindi genera una chiave pubblica e_i per ogni C_i (con la sola condizione che sia un numero primo con n: MCD(n, e_i) = 1. Risolvendo come si è visto in precedenza una congruenza di primo grado, genera inoltre la chiave privata d_i – che invia a C_i e della quale è bene che si disinteressi subito, per non lasciare traccia che possa collegare d_i all'interlocutore C_i.

A questo punto il messaggio di C_i può essere mandato in chiaro e firmato $C_i^{d_i} \pmod{n}$ affinché sia riconosciuto il mittente da parte di B.

Altro problema. Come è possibile effettuare un sorteggio a distanza? Questo significa che ciascuno dei due contendenti A e B deve avere le stesse probabilità di successo (50%) ed essere sicuro che non ci siano imbrogli da parte dell'altro.

In questo caso, ancora, una funzione a trabocchetto permette di avere successo. Un esempio: A sceglie un intero n come prodotto di h fattori primi: $n = p_1 p_2 \ldots p_h$ e lo comunica a B**,** ma non gli comunica i fattori, né tantomeno quanti sono. Anzi gli chiede se n si può scomporre in un numero pari o in un numero dispari di fattori primi. Il problema è ben posto: è noto infatti che, per il cosiddetto *teorema fondamentale dell'aritmetica*, ogni intero ammette, a meno dell'ordine, una scomposizione *unica* in fattori primi.

Chiaramente B ha due possibilità di risposta, pari o dispari, ciascuna con le stesse probabilità di essere vera: vince il sorteggio se indovina la *parità* di n. È chiaro che B non può affidarsi al calcolo, che coinvolge ancora una fattorizzazione e quindi è computazionalmente inaccessibile. Allo stesso tempo, può controllare di non essere imbrogliato, in quanto dopo la risposta, A è tenuto ad esibire i fattori primi e, se loro prodotto fornisce proprio n, si ha la testimonianza che il sorteggio si è svolto correttamente.

10. Conclusione

Ormai la crittografia non si occupa più soltanto di spie e di generali, ma riguarda tutte le persone che svolgono ogni giorno operazioni a distanza che vogliono mantenere riservate: ad esempio transazioni on line o altre comunicazioni. La crittografia è uscita da un campo, importante ma limitato, che rimane solitamente al di fuori della consapevolezza delle persone. Oggi coinvolge problemi di grande interesse economico, sociale e politico, investe la libertà di espressione di ciascuno e pone problematiche nuove nel campo del diritto.

È presente così un complicato intreccio di applicazioni, nel quale risultano difficili da distinguere le componenti funzionali da quelle propriamente tecniche, gli aspetti operativi di carattere generale da quelli applicativi relativi ad un settore specifico, le valenze ideali da quelle pratiche. Oltretutto, la materia ha una evoluzione così rapida – al passo con le moderne tecniche di comunicazione e di elaborazione dell'informazione – che risulta sempre più difficile sciogliere il groviglio delle competenze e riuscire ad analizzarla in parti separate.

Tutto ciò si riflette, naturalmente, in campo scientifico. Attualmente, la crittografia è un potente settore di ricerca nel quale si intrecciano conoscenze diverse e dai profili irregolari: la teoria dei numeri, sicuramente, ma anche l'algebra astratta delle strutture, e poi argomenti sofisticati di complessità computazionale, statistica e probabilità, le tecniche più raffinate dell'informatica moderna, così come altri settori emergenti e dai contorni non ancora ben definiti e, proprio per questo, nella convinzione di chi scrive, più interessanti. Ma vengono alla mente anche due aspetti importanti che sembrano, ma non sono, ai margini delle considerazioni applicative e scientifiche. Da un parte il fatto che spesso i sistemi crittografici sono posti sotto controllo da parte di qualche autorità che ne decreta il possesso esclusivo, equiparandoli addirittura, talvolta, a strumenti bellici o di assoluta importanza strategica. E così, il campo militare, dal quale la crittografia sembra voler fuoriuscire, tenta di riprendere in molti casi il predominio della situazione. Dall'altra parte, senz'altro più soddisfacente per chi scrive, rimane la convinzione che, alla fine, il fattore umano riesce a prevalere sul mondo tecnico degli automatismi che in molti campi sembra dominarci. Rimane il ricordo che, nel corso della seconda guerra mondiale, un sistema crittografico particolare non è stato decrittato: il linguaggio naturale della tribù *navajo*, usato nella guerra del Pacifico.

NOTE

[1] Si vedano [4] e [11]. Sulla decrittazione della Geheim-Schreiber da parte della *Intelligence* svedese, si può vedere [2].

[2] Si tende a considerare 'legittimo' il comportamento di chi vuole comunicare in maniera riservata il proprio messaggio, e quindi a biasimare l'intercettatore. Ma non esiste, a questo riguardo, alcuna motivazione di carattere "morale" fra chi vuole trasmettere e chi intercetta: si tratta di una sfida a costruire sistemi sempre più sicuri da una parte ed a trovare la maniera di rendere leggibili tutti i messaggi dall'altra.

[3] Pubblicato sui numeri di gennaio e febbraio del *Journal des Sciences Militaires* del 1883. Attualmente reperibile in rete: http://www.petitcolas.net/fabien/kerckhoffs/la_cryptographie_militaire_i.htm

[4] La tabella è assolutamente indicativa. Ho arrotondato per semplicità tutti i valori.

[5] Secondo Singh [15], il più antico documento conosciuto nel quale si parla esplicitamente di frequenze allo scopo di decifrare i testi risale ad al-Kindi, filosofo arabo del IX secolo.

[6] È inutile ricordare come l'Alberti, architetto, matematico, poeta, filosofo e linguista, fosse un autentico 'uomo del Rinascimento'. La descrizione del sistema cifrante è contenuta nella sua opera *De Cifris* del 1466.

[7] Per la decrittazione di Enigma fu utilizzato in particolare un complesso elettromeccanico di calcolo, detto *Colossus*. Molti dei ricercatori che vi lavoravano, fra cui Turing, forse ispirati dal progetto, saranno poi all'origine della problematica della *Intelligenza artificiale*. Una descrizione esauriente del sistema Enigma e delle vicende che hanno portato alla sua decrittazione è contenuta, ad esempio, nel libro di Simon Singh [15] e nella biografia di Turing scritta da Alan Hodges [7].

[8] Oltre a ciò, altre permutazioni dei cavi di collegamento, variate di tempo in tempo, ed altre scelte nell'assetto iniziale della macchina, a discrezione dell'operatore e quindi variabili in ciascun messaggio che veniva trasmesso, rendevano il numero delle possibili configurazioni altissimo ed impossibile da controllare anche con un sistema di calcolo automatico.

[9] Uno dei primi accenni sistematici a un sistema crittografico polialfabetico è contenuto nella sua opera *De furtivis literarum notis, vulgo de ziferis* del 1563.

[10] La terminologia di lingua inglese usa il termine funzioni *trapdoor*.

[11] Secondo le convenzioni stabilite dalla teoria della complessità computazionale, una funzione è facile da calcolare se esiste un algoritmo che impiega un numero di passi che è una funzione polinomiale delle dimensioni dell'*input*. Altrimenti è intrattabile.

[12] Pierre de Fermat, magistrato di professione, è considerato l'iniziatore della moderna "teoria dei numeri". Più noto di questo è il *Grande teorema*, da lui enunciato ma dimostrato solo nel 1995 da Andrew Wiles.

BIBLIOGRAFIA

[1] Bauer, F. L., *Decrypted secrets. Methods and maxims of cryptology,* Springer, Berlino 1997.

[2] Beckman, B., *Codici cifrati* (*Arne Beurling e la crittografia nella II guerra mondiale*), Springer Italia, Milano 2005 (ed. originale *Codebreakers: Arne Beurling and the Swedish crypto-program during World War II*, AMS, Providence RI 2002).

[3] Berardi, L., Beutelspacher, A., *Crittologia*, Franco Angeli, Milano 1996.

[4] Diffie, W., Hellman, M. E., New directions in cryptography, *IEEE Trans. Inf. Theory*, 22(6), 1976, pp. 644-654.

[5] Ferragina, P., Luccio, F., *Crittografia. Principi, algoritmi, applicazioni*, Bollati Boringhieri, Torino 2001.

[6] Giustozzi, C., Monti, A., Zimuel, E., *Segreti, spie, codici cifrati*, Apogeo, Milano 1999.

[7] Hodges, A., *Storia di un enigma: vita di Alan Turing*, Bollati Boringhieri, Torino 1991 (ed. originale *Enigma*, Simon and Schuster, New York 1983).

[8] Koblitz, N., *A course in number theory and cryptography*, Springer, New York 1987.

[9] Leonesi, S., Toffalori, C., *Numeri e crittografia*, Springer Italia, Milano 2006.

[10] Pomerance, C. (a cura di), *Cryptology and computational number theory*, AMS, Providence RI 1990.

[11] Rivest, R., Shamir, A., Adleman, L., A method for obtaining digital signatures and public key cryptosystems, *Comm. ACM,* 1978, pp. 120-126.

[12] Salomaa, A., *Public-key cryptography*, Springer, Berlin 1990.

[13] Sgarro, A., *Crittografia*, Muzzio, Padova 1985.

[14] Shannon, C., Communication theory of secrecy systems, *Bell Systems Techn. J.*, 28(4), 1949, pp. 656-715.

[15] Singh, S., *Codici e segreti*, Rizzoli, Milano 1997 (ed. originale *The code Book*, Doubleday, New York 1999).