Crittografia Classica

Scritture e codici segreti

Paolo D'Arco,
Università di Salerno

Prof. Alfredo De Santis,
Università di Salerno

Contenuti

Capitolo 1

Crittografia Classica

1.1 Le scritture segrete

IN DIVERSE civiltà del passato sono state sviluppate tecniche di trasformazione delle parole aventi il fine di renderne incomprensibile il significato a persone escluse da un gruppo privilegiato. Nella città di Menet Khufu, che sorge sulle sponde del Nilo, è stata ritrovata una delle più antiche testimonianze di alterazione di una scrittura: si tratta di una incisione funeraria di circa 4000 anni fa realizzata sulla tomba di un nobile. In questo caso, l'intento della trasformazione consisteva semplicemente nel conferire *dignità* e *onoreficenza* alla persona defunta. Tale pratica dovette essere molto in voga presso gli egizi visto che diverse incisioni funerarie dell'epoca furono modificate a scopi prettamente onorifici e decorativi.

Nello stesso periodo, tuttavia, cominciarono a comparire anche trasformazioni aventi lo scopo di rendere *misterioso* ed *arcano* il significato delle parole.

La crittografia, arte delle scritture segrete, nasce dall'incontro e dalla maturazione delle due tendenze: trasformazione deliberata delle parole ed esigenza di segretezza. La parola crittografia deriva, infatti, dai termini greci *kryptos*, segreto e *graphos*, scrittura. –

Non tutte le società antiche svilupparono forme di crittografia. La Cina, per esempio, l'unica civiltà antica ad usare una scrittura ideografica, non ne ha mai viste. Le ragioni, a detta degli storici, sono legate alla natura prevalentemente orale delle comunicazioni e al basso tasso di alfabetizzazione. In India, invece, forme di crittografia furono concretamente prat-

icate. In diversi testi indiani, infatti, sono presenti riferimenti a forme di scritture segrete. Nell'*Artha-Sastra*, un testo classico sugli affari di stato, si sottolinea l'importanza delle scritture segrete nei servizi di spionaggio mentre nel *Latila-Vistara*, un libro che esalta le virtù di Budda, si narra di come questi stupisse il proprio insegnante parlando di scritture *perpendicolari, disordinate, etc ....* Nel *Kama-Sutra*, invece, tra le 64 arti (yogas) che la donna deve conoscere e praticare c' è l'arte delle scrittura segreta. La 44-esima e, in particolare, la 45-esima arte (*mlecchita-vikalpa*) trattano di regole di trasformazione delle parole basate essenzialmente sulla sostituzione dei caratteri.

Anche nelle scritture cuneiformi sviluppate in Mesopotamia sono state ritrovate tracce crittografiche. Sia presso gli Assiri che i Babilonesi è stata rinvenuta l'usanza da parte degli scribi di sostituire le parti terminali delle parole con elementi corti e stereotipati detti colofoni. Inoltre, in Iraq, nel periodo finale delle scritture cuneiformi, è stata usata per la prima volta la sostituzione di nomi con numeri.

Fonti preziose di esempi di scritture segrete sono i testi sacri. Nel Vecchio Testamento gli storici hanno evidenziato 3 tipi di trasformazioni: l'*Atbash*, l'*Albam* e l'*Atbah*. La prima è universalmente accettata; le seconde sono maggiormente discusse. L'*Atbash ebraico*, è una tecnica di trasformazione ad alfabeto capovolto: il primo carattere dell'alfabeto viene cioè sostituito con l'ultimo dell'alfabeto, il secondo carattere viene sostituito con il penultimo, e così via. Il nome deriva dalla regola di trasformazione. Infatti la prima lettera dell'alfabeto ebraico è **A**leph, l'ultima è **T**aw, la seconda è **B**eth e la penultima è **Sh**in. Concatenando le iniziali di queste lettere nell'ordine si ottiene la parola Atbash. L'Atbash viene utilizzato nel libro del profeta Geremia per cifrare il nome della città di Babilonia. In realtà non sono chiare le ragioni per cui ciò avvenga visto che nel seguito del testo il nome della città compare in chiaro.

L'*Albam*, invece, richiede che l'alfabeto venga diviso in due parti e che ogni lettera venga sostituita con la corrispondente dell'altra metà. 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 sostituente risulti uguale a 10. Quindi, per esempio, Aleph (prima lettera dell'alfabeto) viene sostituita con Teth (nona lettera dell'alfabeto). Per le restanti lettere dell'alfabeto deve valere una regola simile con somma pari a 28 in decimale (per esempio, la 13-esima lettera viene sostituita con la 15-esima, etc.).

Nel Vecchio Testamento si trova, poi, il crittogramma più antico e famoso della storia:

MENE MENE TEKEL UPHARSIN

Il messaggio comparve su una parete durante un banchetto in onore di re Baldassarre, e premonizzava la fine delle ricchezze dell'impero Babilonese ed il suo smembramento tra i Medi e i Persiani. Nessuno dei saggi di corte riuscì o ebbe il coraggio di decifrarlo e comunicarne il contenuto al re. Pertanto, re Baldassarre chiese a Daniele, un deportato dalla Giudea che si era già conquistato fama di interprete prodigioso di sogni e segreti, di rendergli comprensibile la scritta. Daniele non ebbe difficoltà a farlo e, per questo, fu ricompensato dal re. A buon diritto, può essere considerato il primo crittoanalista della storia.

Molti scrittori dell'età classica hanno fatto cenni o riferimenti a forme di scritture segrete nelle loro opere. Omero nell'*Iliade* è uno dei primi. Qualche centinaio di anni dopo, Erodoto, nelle sue *Histories*, descrive parecchi espedienti di natura steganografica utilizzati per nascondere messaggi. Tra i tanti episodi narrati, è estremamente interessante la storia di Demerato, uno spartano esiliato in Persia che avvisò i suoi conterranei di una imminente invasione pianificata da Serse, re dei Persiani. All'epoca venivano usate per scrivere tavolette di legno ricoperte di cera. Demerato si servì di una di queste. Precisamente, rimosse lo strato di cera, incise il messaggio direttamente sul legno e ricoprì il tutto nuovamente con della cera liquida che, una volta raffreddata, nascondeva perfettamente i caratteri incisi. Quando la tavoletta raggiunse la destinazione nessuno si accorse del messaggio nascosto fino a quando Gorgo, sorella della moglie del re, suggerì di rimuovere la cera della tavoletta. Pertanto, al pari di Daniele, può essere considerata la prima donna crittoanalista della storia.

Il greco Enea il Tattico (400 a.C.), nella sua opera *Sulla difesa delle fortezze* ha scritto, invece, un intero capitolo in cui presenta sofisticate tecniche crittografiche e steganografiche. Si tratta di uno dei manuali crittografici più antichi fino ad oggi rinvenuti. Una delle tecniche ivi descritte ed ampiamente utilizzate anche nel Medioevo, consisteva in un disco con un foro centrale e tanti fori sul bordo quanti erano i caratteri dell'alfabeto. Il disco poteva essere utilizzato per cifrare un messaggio facendo passare un filo, a partire dal centro, per tutti i fori sul bordo che corrispondevano ai caratteri del messaggio in chiaro. La decifratura richiedeva invece che si svolgesse il filo e si segnassero i caratteri "attraversati". La sequenza così ricostruita, letta alla rovescia, rappresentava il messaggio in chiaro.

Tre cifrari famosi ed usualmente presentati nelle storie della crittografia sono invece la scacchiera di Polibio, il Cifrario di Cesare e la Scytala Spartana.

La *Scacchiera di Polibio* risale al secondo secolo a.C. Fondamentalmente si tratta di un sistema di comunicazione per trasmettere messaggi

attraverso segnali luminosi. Il sistema, di cui narra appunto lo storico Polibio, funziona al modo seguente: i due comunicanti condividono una scacchiera di cinque righe e cinque colonne.

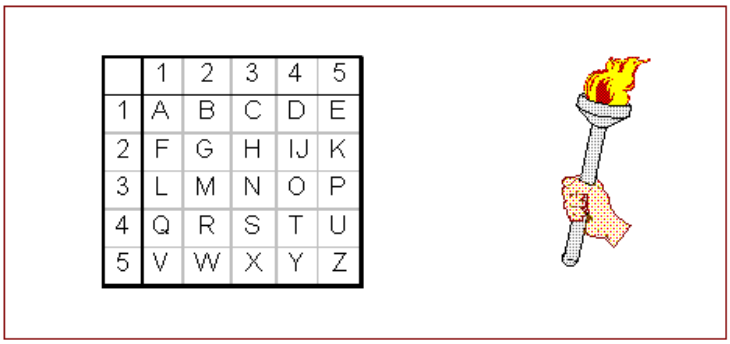


Figure 1.1
La scacchiera di Polibio

Ogni carattere è rappresentato univocamente da una coppia di numeri. Per esempio, la lettera "A" è rappresentata dalla coppia (1,1), la "C" dalla coppia (1,3) e via discorrendo. Pertanto, con due gruppi di cinque torce è possibile trasmettere rispettivamente le posizioni di riga e colonna del carattere. Praticamente, il sistema veniva realizzato facendo portare le torce agli schiavi.

Il *Cifrario di Cesare*, descritto invece dallo storico Svetonio nell'opera *Vitae Caesarorum*, consiste nel *sostituire* ogni lettera del messaggio in chiaro con quella che la segue di tre posizioni nell'alfabeto. Quindi la A deve essere cifrata con la D, la B con la E, e così via. Ovviamente, la regola di decifratura richiede che si applichi la sostituzione inversa (D con A, E con B, etc).

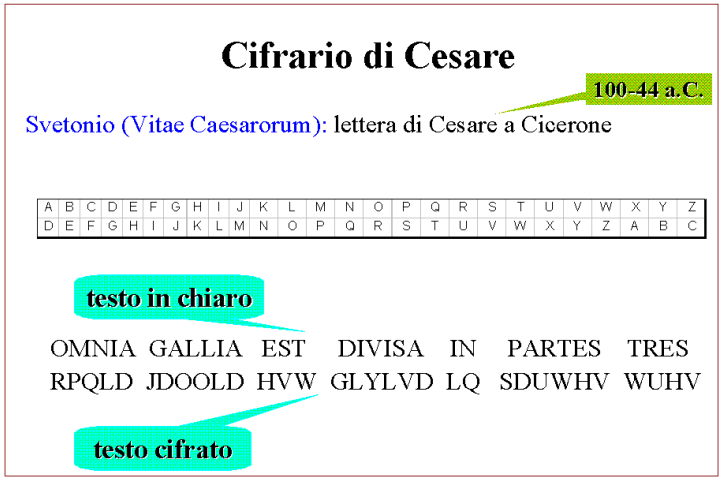


Figure 1.2
Cifrario di Cesare

La crittografia veniva usata non di rado in Roma. Addirittura sembra che uno studioso di grammatica dell'epoca, Valerio Probo, abbia scritto un intero trattato, andato disperso, sulle tecniche di cifratura usate da Giulio Cesare nelle sue comunicazioni riservate.

Infine, la *Scytala Spartana*, descritta dallo storico Plutarco nell'opera *Vitae Parallele*, è costituita da due esemplari identici di un bastone, le scytale appunto, su cui si avvolge un nastro di papiro. Tecnicamente funziona al modo seguente: il cifrante, dopo aver avvolto una striscia di papiro sul bastone in modo da rendere i lembi combacianti, scrive il messaggio in senso longitudinale. Quindi, svolge il nastro e lo fa giungere a destinazione. Il ricevente, riavvolge il nastro di papiro sulla copia del bastone in proprio possesso, e legge il messaggio in chiaro.

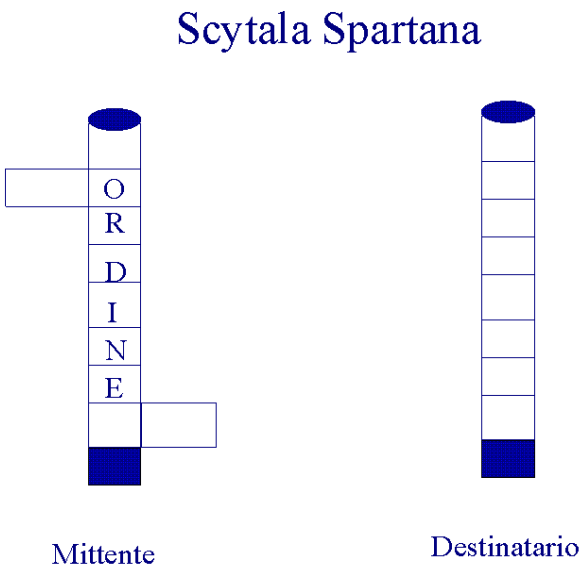


Figure 1.3
Scytala Spartana

Si noti che la scytala non sostituisce i caratteri del messaggio in chiaro ma semplicemente ne *modifica* l'*ordine*. Si narra che questo strumento fosse usato dai governanti spartani, gli efori, per comunicare in modo riservato con i generali dell'esercito, gli strateghi, durante le innumerevoli campagne militari che videro la città protagonista.

Gli storici hanno mostrato che la crittografia è sorta spesso spontaneamente non appena una civiltà ha raggiunto un determinato grado di sviluppo. In luoghi e per esigenze diverse sono state inventate tecniche di scrittura segreta. David Kahn racconta che gli *Yezidis*, una popolazione di circa 25000 abitanti nell'Iraq del Nord, cifrava i propri testi sacri per paura di persecuzioni da parte dei musulmani, così come i *Tibetani* usavano una forma di cifratura per la corrispondenza ufficiale. In *Thailandia*, ancora,

sotto l'influenza indiana, furono messe a punto diverse scritture segrete. Alcune si basavano sulla sostituzione delle lettere dell'alfabeto; un'altra prevedeva la divisione delle lettere in gruppi e richiedeva che si indichicasse ogni lettera con un numero di gruppo ed una sequenza di puntini verticali per specificare la posizione della lettera nel gruppo. Anche nell'arcipelago delle *Maldive* sono state rinvenute due forme di scritture segrete, mentre in *Persia*, all'incirca nel 600 d.C., ebbe luogo il primo uso di scritture segrete a fini politici.

Gli episodi narrati ben mettono in evidenza come l'esigenza di scritture segrete sia cresciuta nel tempo parallelamente alla crescita delle civiltà. Dalle prime tecniche di alterazione delle parole a fini onorifici e decorativi si giunge a sistemi che cominciano a somigliare a veri e propri cifrari. In particolare, per quanto semplici, la scytala e il cifrario di Cesare, realizzano due idee chiave ampiamente utilizzate, come vedremo, nei secoli successivi: *sostituzione* e *trasposizione* dei caratteri.

1.2 Cifrari

LO SCENARIO che consideremo in seguito, può essere così descritto: immaginiamo che due persone, indicate con i nomi di *Alice* e di *Bob*, intendano comunicare in modo riservato attraverso un canale insicuro (corrieri, rete, Internet), reso tale dalla presenza di una terza persona, Oscar, che ascolta la comunicazione ed ha interesse a capire cosa si dicono i due comunicanti. Supponiamo che Alice e Bob condividano uno stesso insieme di messaggi M, noto anche ad Oscar. Per esempio, supponiamo che Alice, Bob ed Oscar parlino la stessa lingua. I messaggi appartenenti ad M vengono detti messaggi *in chiaro*, perchè sono comprensibili da tutti e tre i partecipanti. Un cifrario è una coppia di regole di cifratura e di decifratura che permette, rispettivamente, ad Alice di trasformare un messaggio dell'insieme M in una stringa, apparentemente priva di significato, da trasmettere attraverso il canale insicuro, ed a Bob di recuperare il messaggio originale dalla stringa ricevuta. Alice e Bob sono gli unici in grado di comprendere i messaggi che si scambiano in quanto nella trasformazione dei messaggi usano una informazione segreta, detta *chiave*, che Oscar non possiede. Naturalmente, prima che la comunicazione abbia luogo Alice e Bob debbono accordarsi sulla chiave che utilizzeranno di seguito. In maniera più precisa possiamo indicare un cifrario attraverso una coppia di funzioni $(E_k(), D_k())$, individuata da una specifica chiave k: la funzione di cifratura $E_k()$ trasforma il messaggio in chiaro m in un nuovo messaggio c, detto messaggio *cifrato*, cioè $E_k(m) = c$. Viceversa, la funzione di decifratura $D_k()$ riporta il cifrato c nel messaggio di partenza m, cioè

$D_k(c) = m$.

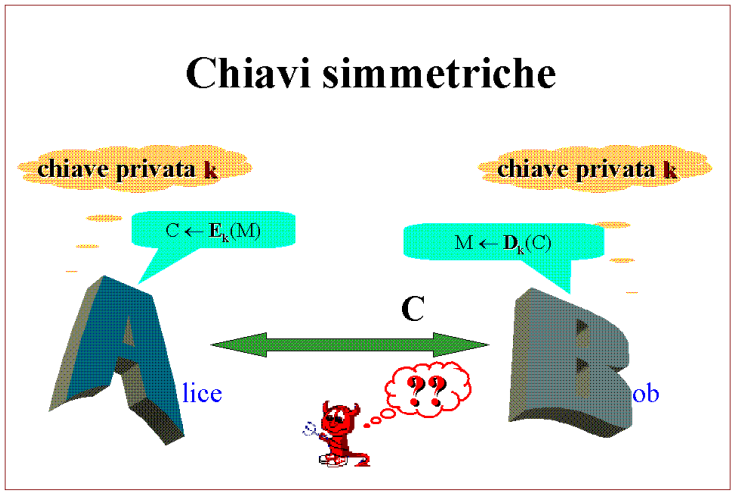


Figure 1.4
Modello di Cifrario

Indicheremo nel seguito con C l'insieme dei possibili messaggi cifrati e con K l'insieme delle possibili chiavi che Alice e Bob possono scegliere. Inoltre supporremo che la forma $(E(), D())$ delle funzioni di cifratura e decifratura sia *universalmente nota*. Pertanto, la sicurezza del cifrario poggia esclusivamente sulla chiave segreta e non sulla conoscenza del metodo usato. Questo principio è noto come principio di Kerckhoffs.

Remark 1.1: Principio di Kerckhoffs

Auguste Kerckhoffs von Nieuwenhof (1835, 1903), filologo olandese, in un importante trattato crittografico dal titolo *La Cryptographie Militaire* (1883), sostenne per primo che nella crittografia strategica, destinata ad usi militari, la sicurezza non deve poggiare sulla segretezza del metodo ma soltanto sulla segretezza della chiave concordata prima che la comunicazione abbia luogo.

Ovviamente, affinchè un cifrario sia utilizzabile, qualunque sia la chiave segreta $k \in K$ su cui Alice e Bob si sono accordati prima della comunicazione e qualunque sia il messaggio m che Alice invia a Bob, l'applicazione al messaggio in chiaro della funzione di cifratura e poi, al cifrato ottenuto, di quella di decifratura, debbono restituire il messaggio in chiaro, cioè deve risultare $D_k(E_k(m)) = m$. Ciò significa che la funzione $E_k()$ deve essere iniettiva. Inoltre, per essere sicuro, il cifrario deve essere *almeno* tale da garantire che Oscar, dall'analisi del cifrato, non possa ricavare il messaggio in chiaro nè tantomeno la chiave segreta k. In quest'ultimo caso potrebbe addirittura interpretare tutti i messaggi che Alice e Bob si scambiano.

Nella comunicazione, il modo più semplice di utilizzare un cifrario è il seguente: supponiamo che il messaggio che Alice intende trasmettere sia $m = m_1 m_2 \cdots m_n$, per qualche intero $n \geq 1$, dove ogni simbolo $m_i \in M$, per $i = 1, \ldots, n$. Alice allora calcola $c_i = E_k(m_i)$, per $i = 1, \ldots, n$, e spedisce la stringa $c = c_1 c_2 \cdots c_n$ sul canale pubblico. Bob, di conseguenza, decifra $c_1 c_2 \cdots c_n$ calcolando per $i = 1, \ldots, n$, $m_i = D_k(c_i)$.

1.3 Cifrari a sostituzione

NEL SEGUITO considereremo un alfabeto costituito da 26 lettere poste in corrispondenza biunivoca con gli interi da 0 a 25 come mostrato nella figura:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 1.5
Corrispondenza caratteri-numeri

Il cifrario di Cesare è un caso particolare di un sistema di cifratura in cui si stabilisce una regola di *sostituzione circolare* dei caratteri del messaggio in chiaro con altri caratteri dello stesso alfabeto.

Le funzioni di cifratura e decifratura descritte, sfruttando la corrispondenza fissata tra lettere e interi, divengono

$$y = x + 3 \bmod 26 \qquad \text{e} \qquad x = y - 3 \bmod 26.$$

Il numero 3, che stabilisce le posizioni che occorre scorrere circolarmente nell'effettuare la sostituzione, è un valore che Alice e Bob condividono. Tuttavia, nulla vieta ad Alice ed a Bob di accordarsi sul numero 7, sul 9 o su qualche altro numero di posizioni nell'intervallo $\{1, \ldots, 25\}$ e tener segreto il numero, che diventa così la chiave.

I cifrari circolari presentano comunque uno svantaggio: l'insieme delle possibili chiavi che i comunicanti possono scegliere risulta estremamente ridotto: solo 25 valori. Pertanto, un avversario in possesso di una stringa cifrata potrebbe tentarne la decifratura provando tutte le possibili sostituzioni, l'una di seguito all'altra. Questo tipo di attacco in crittografia

viene detto *ricerca esaustiva* sullo spazio delle chiavi. Una condizione necessaria affinchè un cifrario risulti sicuro è, quindi, che il numero di possibili chiavi sia molto grande e una ricerca esaustiva risulti impraticabile (link precedente discussione).

In realtà, una sostituzione circolare è un modo semplice per associare ad ogni carattere del messaggio in chiaro un diverso carattere nel messaggio cifrato. Nulla vieta che i due comunicanti possano convenire una sostituzione che non può essere rappresentata attraverso uno scorrimento circolare dell'alfabeto ma che deve essere specificata carattere per carattere. In questo caso la sostituzione consiste in una permutazione generica dell'alfabeto e la chiave segreta che Alice e Bob condividono è proprio la *descrizione* della permutazione. L'insieme delle chiavi è, dunque, l'insieme delle possibili permutazioni su un alfabeto di 26 caratteri, che sono 26!, cioè circa $4 \cdot 10^{26}$. Una ricerca esaustiva su un insieme così grande non è realizzabile in tempi ragionevoli.

Alcuni banchieri fiorentini nel XVI secolo probabilmente avevano intuito la potenza di questo metodo. Infatti sembra che le lettere di credito venissero protette nella spedizione attraverso un cifrario a sostituzione in cui il mittente e il ricevente si erano precedentemente accordati su una particolare permutazione dei caratteri dell'alfabeto.

Leon Battista Alberti, figura illustre del Rinascimento Italiano, fu l'autore di uno dei primi cifrari che sostituisce i caratteri del messaggio in chiaro attraverso una permutazione a caso dell'alfabeto. L'Alberti descrisse il proprio cifrario nel trattato *Modus Scribendi in Ziferas*, offrendone una rappresentazione in termini di due dischi concentrici, inseriti uno nell'altro. Il disco esterno rappresenta le lettere del messaggio in chiaro. Quello interno rappresenta le lettere del cifrato. I caratteri del disco interno sono posizionati a caso. Ruotandolo, in modo da far coincidere una delle lettere con la lettera A del disco esterno si stabilisce la sostituzione da effettuare. Infatti, ogni lettera del disco esterno va sostituita con la corrispondente di quello interno. La decifratura del messaggio richiede l'operazione inversa; una volta fissata la posizione dei due dischi, i caratteri del messaggio cifrato, che sono rappresentati dal disco interno, vanno sostituiti con quelli del disco esterno corrispondenti. La figura che segue rende esplicite le operazioni di cifratura e decifratura. Il cifrario viene detto *dei dischi cifranti*.

Figure 1.6
I Dischi cifranti

Circa un secolo dopo Giovan Battista Della Porta presentò, un cifrario a dischi simile a quello dell'Alberti ma con una complicazione in più: l'alfabeto del cifrato (i caratteri del disco interno) è *distinto* da quello del messaggio in chiaro ed è rappresentato da simboli di fantasia.

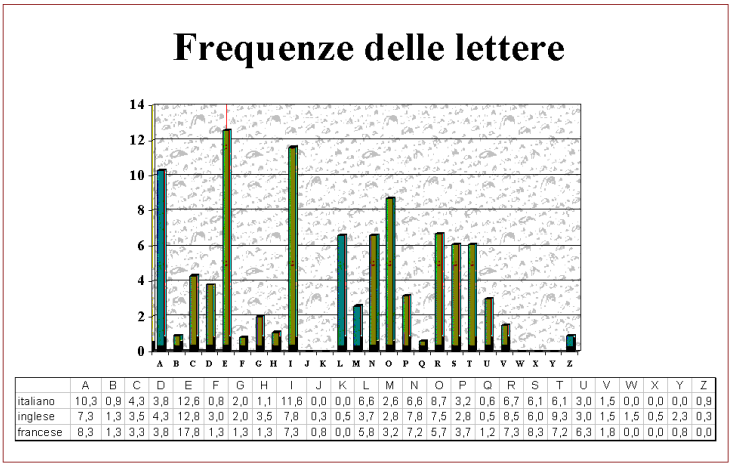
Giovan Battista Della Porta, nato a Napoli nel 1535, è un'altra figura eclettica del Rinascimento italiano (tra l'altro fu uno dei fondatori dell'*Accademia dei Lincei*). Il suo contributo all'arte della crittografia è presente nel trattato *De Furtivis Literarum Notis*.

Una versione linearizzata dei cifrari a dischi è il cosiddetto regolo di Saint-Cyr, città francese in cui aveva sede un'importante accademia militare. L'idea è la seguente: il regolo è costituito da due asticelle, l'una lunga la metà dell'altra. La prima viene detta *cursore* ed è etichettata con le 26 lettere dell'alfabeto del messaggio in chiaro. La seconda viene chiamata *statore* e vi è riportato due volte di seguito l'alfabeto cifrante. Il funzionamento è identico a quello delle macchine dell'Alberti e del Della Porta: al momento della cifratura, il cursore viene posizionato sullo statore in modo tale da far corrispondere la lettera A del cursore con un simbolo dello statore che individua la sostituzione. Naturalmente, la decifratura del messaggio richiede lo stesso posizionamento del cursore sullo statore.

Figure 1.7
Regolo di Saint-Cyr

1.4 Crittoanalisi: frequenze delle lettere

IN REALTÀ anche un insieme di chiavi molto grande *non garantisce* la sicurezza del cifrario. Il problema nasce dal fatto che le strutture dei linguaggi naturali posseggono delle *asimmetrie frequentistiche* intrinseche che possono essere sfruttate per rompere i cifrari a sostituzione. Precisamente, le parole di un linguaggio non sono stringhe casuali dell'alfabeto. Piuttosto, esistono caratteri più frequenti di altri. Le vocali **a** ed **e**, per esempio, ricorrono più spesso delle consonanti **v** e **z** nella lingua italiana. A partire da una stima delle frequenze dei caratteri singoli dell'alfabeto nelle parole di un linguaggio, dei bigrammi (coppie di caratteri) e dei trigrammi (triple di caratteri) è possibile, procedendo per tentativi ed errori, individuare la permutazione che è stata usata nella cifratura. Ovviamente, le frequenze dipendono dal "tipo" di testo considerato. Le frequenze di lettere, bigrammi e trigrammi di questa pagina sono sostanzialmente differenti dalle frequenze di lettere, bigrammi e trigrammi di un libro di matematica.



	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
italiano	10,3	0,9	4,3	3,8	12,6	0,8	2,0	1,1	11,6	0,0	0,0	6,6	2,6	6,6	8,7	3,2	0,6	6,7	6,1	6,1	3,0	1,5	0,0	0,0	0,0	0,9
inglese	7,3	1,3	3,5	4,3	12,8	3,0	2,0	3,5	7,8	0,3	0,5	3,7	2,8	7,8	7,5	2,8	0,5	8,5	6,0	9,3	3,0	1,5	1,5	0,5	2,3	0,3
francese	8,3	1,3	3,3	3,8	17,8	1,3	1,3	1,3	7,3	0,8	0,0	5,8	3,2	7,2	5,7	3,7	1,2	7,3	8,3	7,2	6,3	1,8	0,0	0,0	0,8	0,0

Figure 1.8
Frequenze delle lettere nell'alfabeto italiano

Un esempio mirabile di applicazione dell'analisi delle frequenze alla rottura di un cifrario si trova nell'opera di Edgard Allan Poe *Lo scarabeo d'oro*. Legrand, il protagonista del racconto, trova una pergamena apparentemente non scritta. Accidentalmente, la pergamena viene esposta ad una fonte di calore e, magicamente, su di essa comincia a prender forma un teschio. Prolungando l'esposizione, oltre ad emergere chiaramente il teschio compare anche un messaggio cifrato. Attraverso una ricerca guidata da supposizioni plausibili, tentativi e un po' di fortuna, Legrand riesce a decifrare il messaggio e a recuperare il tesoro sepolto dal capitano Kidd.

Dal punto di vista crittografico la tecnica utilizzata da Legrand per scardinare il messaggio cifrato che ha rinvenuto nella pergamena è proprio un'*analisi di tipo frequentistico*. A partire da quelle parti del cifrato che ricorrono più volte e possono rappresentare lettere più frequenti e parti comuni del discorso, Legrand riesce a carpire, lettera dopo lettera, l'intera sostituzione che il cifrante aveva utilizzato.

In termini crittografici il racconto di Edgard Allan Poe dimostra che un buon cifrario deve in qualche modo cercare di mettere fuori gioco le asimmetrie frequentistiche intrinseche nei linguaggi naturali. Occorre cioè trovare metodi per *mascherare* il fatto che la **a** compare più spesso della **z** o che certi bigrammi appaiono spesso mentre altri non figurano mai in nessuna frase.

Due tecniche che sono state utilizzate in passato per alterare le frequenze sono gli *omofoni* e le *nulle*. L'idea alla base degli omofoni è la seguente: individuare quante sono le lettere maggiormente ricorrenti, ampliare l'alfabeto cifrante aggiungendo un certo numero di extra-simboli, ed effettuare la cifratura dei caratteri più frequenti con più di un carattere. Per esempio, se si stabilisce di sostituire la lettera **a** con **f** e **!**, il cifrante può sostituire **a** una volta con **f** e un'altra con **!**, scegliendo a caso ogni volta

tra uno dei due. Così facendo, la frequenza del simbolo che cifra la **a** è pressappoco dimezzata, divisa tra quella di **f** e quella di **!**.

Quindi gli omofoni permettono di abbassare le frequenze delle lettere più comuni. Le nulle, invece, servono per alzare quelle delle lettere meno frequenti. L'idea, in questo caso, è semplicemente di aggiungere nel messaggio in chiaro le lettere meno frequenti in posizioni tali da non inficiare la comprensione del messaggio originale, alzando, nello stesso tempo, la frequenza delle corrispondenti lettere.

L'analisi delle frequenze è una invenzione degli Arabi. Intorno al 700 d.C., infatti, questa civiltà ha vissuto uno dei suoi momenti di massimo splendore. L'arte, le scienze e la cultura in genere ricevettero un forte impulso. *Le mille e una notte* venne scritta in questo periodo. Anche la crittografia venne ampiamente utilizzata. Gli arabi furono i primi a cifrare interamente la propria documentazione fiscale e a mettere a punto tecniche crittoanalitiche basate sullo studio delle frequenze. Abu Yusuf ibn Ishaq al-Kindi, il *filosofo degli arabi* come venne soprannominato, vissuto nel IX secolo, scrisse una lunga monografia sull'argomento, ritrovata nel 1987 in un archivio dell'impero ottomano ad Istambul. È probabile che questa tecnica per rompere i cifrari monoalfabetici sia stata indipendentemente inventata in Europa nel Medioevo ma non è da escludere che sia invece stata in qualche modo importata.

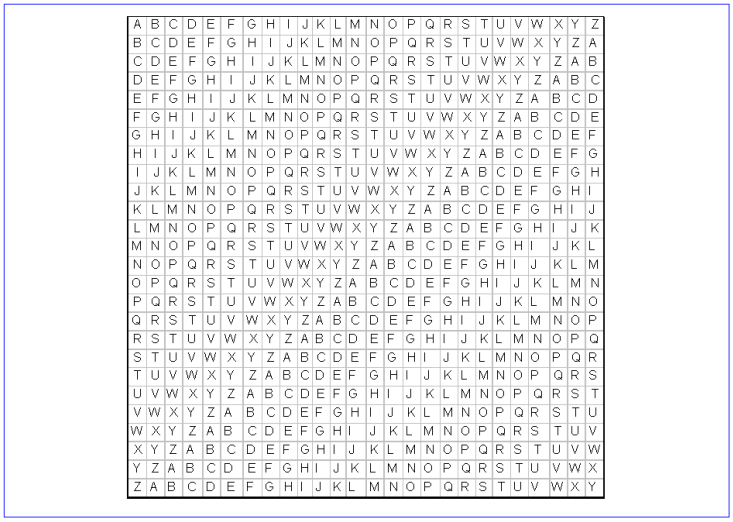
1.5 Cifrari polialfabetici

L'ANALISI delle frequenze è possibile con i cifrari a sostituzione perchè una volta fissata la corrispondenza tra una lettera dell'alfabeto in chiaro e una dell'alfabeto cifrante, essa non viene più modificata. E' come se ogni lettera dell'alfabeto possedesse una *identità* ed una *forma*. La sostituzione monoalfabetica cambia la forma con cui la lettera si presenta nel testo ma non la sua identità che può essere individuata attraverso l'analisi delle frequenze. Ovviamente, se la stessa lettera può essere sostituita in punti diversi del cifrato con lettere *diverse*, ciò non è più possibile. La dipendenza frequentistica viene rotta e, quindi, l'identità si perde. Cifrari che realizzano questo tipo di sostituzione vengono detti *polialfabetici*, in contrapposizione ai precedenti, detti monoalfabetici.

Uno dei più famosi cifrari polialfabetici è il cifrario di Vigenere. Vigenere, vissuto tra il 1523 e il 1596 era un diplomatico francese che raccolse ed espose le conoscenze crittografiche del tempo nell'opera *Traicte des chiffres*.

Il cifrario adopera un quadro di caratteri, detto quadro di Vigenere, e una *parola chiave*, e prevede la divisione del messaggio in chiaro in blocchi

della stessa lunghezza della chiave.



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

Figure 1.9
Quadro di Vigenere

Le lettere della prima colonna corrispondono alle lettere della parola chiave mentre quelle della prima riga corrispondono alle lettere del messaggio in chiaro. L'operazione di cifratura di ogni blocco in cui il messaggio viene originariamente diviso, avviene al modo seguente: ogni lettera del blocco in chiaro viene sostituita da quella all'interno del quadro che si trova nel *punto di intersezione* della colonna individuata dalla lettera in chiaro con la riga associata alla lettera della parola chiave che deve essere usata in quella posizione. L'operazione di decifratura richiede ovviamente il passo inverso.

Se ci si riflette, il cifrario di Vigenere è una sequenza di semplici cifrari a sostituzione circolare. La lunghezza della chiave stabilisce il periodo del cifrario, cioè dopo quanto tempo lo stesso cifrario a sostituzione circolare viene riutilizzato. La stessa lettera del messaggio in chiaro viene sostituita con lettere diverse a seconda del cifrario che in quella posizione viene utilizzato.

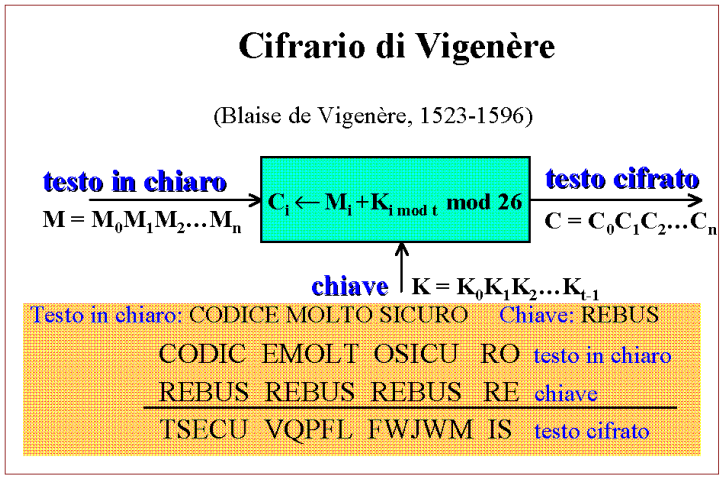


Figure 1.10
Esempio d'uso del cifrario

Utilizzando la corrispondenza tra lettere e numeri stabilita in precedenza, il cifrario di Vigenere puó essere descritto formalmente come segue.

Sia m un intero positivo fissato e sia l'insieme dei messaggi M=C=$(\mathbf{Z}_{26})^m$. Per una chiave $k = (k_1, k_2, \ldots, k_m) \in K = (\mathbf{Z}_{26})^m$, definiamo la funzione di cifratura come

$$e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$$

e quella di decifratura come

$$d_k(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m),$$

dove le operazioni di somma e sottrazione sono in Z_{26}.

Come detto il messaggio viene partizionato in blocchi di m caratteri e ogni blocco viene cifrato con la stessa chiave. Se l'ultimo blocco ha meno di m elementi allora viene completato con caratteri che non alterano il significato del messaggio. Lo spazio delle chiavi ha cardinalità uguale a 26^n.

Per molto tempo il cifrario di Vigenere è stato ritenuto inattaccabile ed i migliori crittoanalisti dell'epoca hanno invano cercato una tecnica per scardinarlo. Tuttavia, nel 1863, Friedrich Kasiski, un ufficiale prussiano in pensione pubblicò un trattato crittografico in cui illustrava una tecnica per demolire il cifrario. L'idea è la seguente: poichè il cifrario è periodico, ogni volta che parti del messaggio in chiaro sono uguali e vengono cifrate con la stessa porzione della parola chiave, le corrispondenti parti cifrate risultano uguali. Ragion per cui, procedendo a ritroso, il crittoanalista, dall'analisi delle parti ripetute del cifrato ed, in particolare, *dalla loro distanza* può inferire la lunghezza della parola chiave. Precisamente, la lunghezza della chiave segreta deve essere un *divisore comune* delle distanze tra le parti identiche del testo cifrato. Una volta stabilita la lunghezza

della parola chiave, il crittoanalista può decomporre il testo cifrato in tante sottosequenze quante sono le lettere della chiave e analizzarle singolarmente, attraverso la tecnica di analisi delle frequenze. Ogni sottosequenza è, infatti, cifrata attraverso un semplice cifrario a sostituzione circolare.

Da un punto di vista storico occorre precisare che Kasiski è stato il primo a pubblicare la tecnica di attacco descritta al cifrario di Vigenere ma sembra che indipendentemente fosse giunto allo stesso risultato qualche anno prima Charles Babbage.

La rottura del cifraio di Vigenere è stata una delle più interessanti sfide della crittografia classica vinte dai crittoanalisti. Oltre al metodo di Kasiski-Babbage, successivamente furono descritte altre tecniche di attacco tra cui spicca per efficienza quella dell'americano William Friedmann, uno dei più importanti crittoanalisti del secolo passato. A Friedmann si deve, tra l'altro, anche l'introduzione del termine *crittoanalisi*.

La storia della crittografia classica, per quanto concerne i cifrari polialfabetici, ha visto prima e dopo l'invenzione del cifrario di Vigenere altre soluzioni che possono essere presentate o come casi particolari o come sviluppi di questo cifrario. Una variante estremamente semplice è dovuta a Johannes Trithemius (Tritemio), abate benedettino del quattrocento, che propose uno schema di cifratura basato sullo stesso quadro di Vigenere. La differenza fondamentale è che mentre nella versione di Vigenere l'uso del quadro è retto dalla parola chiave, nello schema di Tritemio la chiave corrisponde alla stringa "abcd ...xyz": precisamente, il cifrante usa la prima riga per cifrare il primo carattere del messaggio in chiaro, la seconda per il secondo etc, ricominciando daccapo in presenza di un messaggio più lungo di 26 lettere. Storicamente il quadro di Tritemio precede quello di Vigenere per cui la paternità andrebbe attribuita a lui.

Il conte Gronsfeld propose ancora una variante semplificata dello schema di Vigenere, in cui il quadro contiene solo dieci righe. Quindi le parole chiave sono vincolate ai primi dieci caratteri dell' alfabeto.

L'ammiraglio Sir Francis Beaufourt descrisse invece due modifiche del cifrario di Vigenere, in cui i cambiamenti sono apportati alle regole di cifratura e di decifratura (il quadro è lo stesso).

A Giovan Battista Belaso, invece, un nobile bresciano vissuto nel XVI secolo, si deve l'invenzione del cifrario ad *autochiave*. Ripensiamo per un attimo al cifrario di Vigenere. Il messaggio in chiaro viene diviso in blocchi e ogni blocco viene cifrato con la parola chiave. L'idea del cifrario ad autochiave è quella di costruire una chiave lunga quanto il messaggio che occorre cifrare cosicchè ogni blocco viene cifrato con elementi diversi. L'idea consiste nel concatenare la parola chiave iniziale, che viene usata per cifrare il primo blocco, con lo stesso messaggio in chiaro. La stringa così ottenuta serve per cifrare l'intero messaggio. La decifratura procede

in modo naturale: la parola chiave viene usata per decifrare il primo blocco del messaggio e, a sua volta, il blocco decifrato viene usato come chiave per decifrare il blocco successivo e così via.

Seppur astuta ed ingegnosa, la tecnica dell'autochiave non è molto robusta. Gli scritti crittografici di G.B. Belaso furono innovativi e per molti versi anticipatori di idee sviluppate pienamente soltanto negli anni seguenti. La sua opera più importante, *Il vero modo di scrivere in cifra*, venne pubblicata a Brescia nel 1564.

Remark 1.2: Sostituzione Monoalfabetica e Polialfabetica

Per sostituzione monoalfabetica *storicamente* si intende una sostituzione in cui un carattere dell'alfabeto viene sostituito sempre con lo stesso simbolo nel corrispondente cifrato, mentre con polialfabetica si intende una sostituzione in cui ogni carattere del messaggio in chiaro viene cifrato con simboli diversi a seconda della posizione in cui si trova. In realtà, anche un cifrario polialfabetico può essere visto come un cifrario a sostituzione monoalfabetica in cui l'alfabeto è costituito da tutte le possibili sequenze di caratteri della stessa lunghezza della chiave. Pertanto, i concetti di sostituzione mono e polialfabetica sono relativi alla *struttura* dell'alfabeto di riferimento.

1.6 Permutazione delle posizioni

TUTTI i crittosistemi che abbiamo discusso finora coinvolgono la sostituzione: caratteri del testo in chiaro vengono sostituiti, nel testo cifrato, con caratteri diversi. L' idea di un cifrario a permutazione delle posizioni è di non modificare i caratteri del testo in chiaro, ma di cambiare le loro *posizioni* (il principio é lo stesso della Scytala Spartana).
Formalmente, sia m un intero positivo fissato e sia $M = (\mathbf{Z}_{26})^m$. Inoltre, sia K l'insieme di tutte le permutazioni di $\{1,\ldots,m\}$.

Scelta una permutazione $\pi \in K$, la funzione di cifratura risulta

$$e_\pi(x_1,\ldots,x_m) = (x_{\pi(1)},\ldots,x_{\pi(m)})$$

e la funzione di decifratura

$$d_\pi(y_1,\ldots,y_m) = (y_{\pi^{-1}(1)},\ldots,y_{\pi^{-1}(m)}),$$

dove π^{-1} indica la permutazione inversa di π.

Per esempio, sia (2,3,1) la permutazione scelta, cioè

$$\pi(1) = 2 \qquad \pi(2) = 3 \qquad \pi(3) = 1$$

e sia LETTERE UGUALI ORDINE DIVERSOX il messaggio da cifrare.

La chiave scelta richiede di dividere il testo in chiaro in gruppi di tre caratteri e di permutarli nell'ordine stabilito, cioé la prima lettera occupa il secondo posto della tripla, la seconda lettera il terzo posto, la terza il primo. Per esempio, la prima tripla LET, diventa TLE. Cosí procedendo il messaggio cifrato diviene:

TLERTEGEULUARIONDIIEDRVEXSO.

Un interessante cifrario, dovuto ancora a G.B. Belaso, che sfrutta l'idea della permutazione funziona al modo seguente. Fissata una parola chiave, il messaggio in chiaro viene diviso in blocchi della stessa lunghezza della chiave e disposti in una matrice avente una riga per ogni blocco. Precisamente, la prima riga contiene la chiave, la seconda riga il primo blocco del messaggio in chiaro, la terza riga il secondo blocco e via dicendo. Il cifrato viene generato considerando i blocchi che si ottengono permutando le colonne della tabella secondo l'ordine stabilito dall'ordine naturale dei caratteri della chiave. Una versione leggermente più complicata è stata usata nel secolo scorso per crittare comunicazioni telegrafiche.

1.7 Nomenclatori e Dizionari

NEL CORSO della storia i cifrari hanno svolto un ruolo cardine nell'ambito delle attività diplomatiche. Più di una volta, vicende personali e pubbliche sono state direttamente legate alla sorte di un cifrario. Nel '500 e nel '600 le corrispondenze segrete furono molto fitte e presso le grandi potenze dell'epoca erano presenti gruppi di lavoro, le cosiddette *camere nere*, dediti all'arte della crittografia e della crittoanalisi. Molto famosi erano quelli del Vaticano, il gruppo Parigino ed il temutissimo gruppo Viennese.

Nel ′500 si diffuse l'uso dei *nomenclatori* che, a detta degli storici, fecero la propria comparsa sulla scena crittografica nei primi anni del′300. Un nomenclatore è essenzialmente un cifrario a sostituzione che si serve di omofoni e di simboli aggiuntivi per rappresentare/cifrare alcuni dei termini più comuni nella corrispondenza. Solitamente, l'alfabeto del cifrato è diverso da quello in chiaro: ogni lettera dell'alfabeto in chiaro può essere sostituita con una tra diverse lettere dell'alfabeto in cifra. Inoltre, come dicevamo, a parole frequenti, corrispondono simboli specifici. Tali simboli, oltre che cifrare le relative parole, permettono anche di ridurre la lunghezza della comunicazione (abbreviazioni).

Figura : *Nomenclatore*

Alla rottura di un nomenclatore è legato un episodio della storia molto triste: la condanna al patibolo della regina di Scozia Maria Stuarda. Mentre quest'ultima era richiusa a Chartley Hall, nello Staffordshire, un gruppo di sudditi capeggiati dal nobile Babington ordiva un piano per la sua liberazione. Le comunicazioni tra Maria Stuarda ed il gruppo di Babington venivano cifrate tramite un nomenclatore. Purtroppo i messaggi furono intercettati e decifrati dal ministro inglese Walsingham che si avvalse del supporto di esperti crittoanalisti dell'epoca. In particolare, con un messaggio in cui dava l'assenso all'omicidio della cugina Elisabetta, regina d'Inghilterra, Maria Stuarda firmò la sua condanna a morte.

Da un punto di vista crittografico l'episodio è interessante anche perchè evidenzia un altro problema di fondamentale importanza nelle comunicazioni: *l'autenticazione* dei messaggi, cioè la possibilità di stabilire con certezza l'origine del messaggio. Precisamente, Walsingham ed i suoi crittoanalisti, quando capirono i propositi di Babington e vennero a capo del sistema di cifratura, intercettarono il messaggio di approvazione di Maria Stuarda al piano dei cospiratori e aggiunsero una postilla cifrata con lo stesso sistema in cui ella chiedeva esplicitamente a Babington i nomi dei fautori del piano. In tal modo i cospiratori potetterono essere individuati. L'episodio mostra che la cifratura non *autentica automaticamente* il trasmittente al ricevente.

L'idea del cifrario a dizionario per molti versi è simile a quello dei nomenclatori ed, in particolare, all'uso di simboli predefiniti per rappresentare parole frequenti. In questo caso, i due comunicanti condividono un dizionario diviso in due colonne: nella prima sono riportate le parole del testo in chiaro, mentre nella seconda sono presenti quelle del cifrato (dizionario a lista semplice).

L'operazione di cifratura consiste nel sostituire le parole della prima colonna con le corrispondenti della seconda. L'operazione di decifratura richiede la sostituzione inversa. Naturalmente, se le righe del dizionario sono ordinate rispetto alle parole della prima colonna, la decifratura risulta lunga e tediosa. Pertanto, spesso i cifrari a dizionario sono divisi in due metà (dizionario a lista doppia). Nella seconda, le righe sono ordinate rispetto alle parole della seconda metà. Per avere un'idea, si pensi ad un dizionario bilingue odierno (Italiano - Inglese, Inglese - Italiano).

Anche i cifrari a dizionario sono stati ampiamente usati, specie durante le due guerre mondiali. Uno degli episodi più importanti è rappresentato dal cosiddetto codice Zimmermann (prima guerra mondiale). Le vicende sono le seguenti: i servizi segreti inglesi intercettarono un messaggio del ministro tedesco Zimmermann avente il fine di sollecitare il presidente del Messico ad un eventuale appoggio, qualora gli Stati Uniti fossero entrati in guerra. Nel messaggio si chiedeva, inoltre, al presidente messi-

cano una mediazione con i governanti giapponesi per ulteriori allargamenti dell'alleanza. Ovviamente le partecipazioni, a conclusione del conflitto, sarebbero state debitamente ricompensate. L'interpretazione del messaggio, cifrato attraverso un cifrario a dizionario a lista doppia, è una delle motivazioni che spinsero gli Stati Uniti a ritenere oramai troppo pericolose le manovre tedesche e a partecipare alla prima guerra mondiale.

Due curiosi esempi di cifrari a dizionario sono ascrivibili al già noto abate benedettino Tritemio e agli indiani Navajo. Il primo, nel quattrocento, inventò un cifrario in cui le lettere del messaggio in chiaro erano sostituite da parole "sacre", aventi il fine di formare una falsa preghiera. Le cosiddette *Ave Marie* di Tritemio raccolgono una lista ordinata di trecentosei "alfabeti segreti", ciascuno contenente 26 parole, una per ogni lettera dell'alfabeto latino. La cifratura richiedeva che si sostituisse ogni lettera del testo in chiaro con la parola associata a quella lettera nell'alfabeto corrispondente. Dunque, il primo carattere del messaggio doveva essere sostituito con la parola associata a quel carattere nel primo alfabeto, il secondo carattere del messaggio doveva essere sostituito con la parola associata a quel caratte nel secondo alfabeto e via dicendo. La scelta delle parole negli alfabeti era tale da garantire che il testo cifrato complessivo avesse senso compiuto.

Gli indiani Navajo sono invece stati usati nel corso della seconda guerra mondiale. Due di essi, venivano posti agli estremi della trasmissione per cifrare e decifrare i messaggi che le due parti intendevano scambiarsi. In questo caso, il "vocabolario" Navajo, usato nella comunicazione, garantiva la sicurezza in ragione della sua scarsissima conoscenza. Gli americani preferirono gli indiani della riserva Navajo a varie altre tribù sia perchè la loro lingua è priva di qualsiasi legame con gli idiomi asiatici ed europei, sia perchè i rapporti tra i Navajo e il mondo "esterno" erano stati praticamente inesistenti.

1.8 Cifrari poligrafici

TUTTI i cifrari a sostituzione monoalfabetici e polialfabetici, trattano un carattere alla volta e sono detti pertanto monografici. Un cifrario poligrafico, invece, sostituisce simultaneamente *un gruppo di caratteri* con un altro gruppo. Nell'ottocento furono proposti diversi cifrari poligrafici. Gli esempi più significativi sono il cifrario di Playfer, usato sia durante la prima che la seconda guerra mondiale, e i cifrari Bifido e Trifido di Delastelle. Tuttavia, l'idea di un cifrario poligrafico è antichissima e affonda le radici nel sistema di segnalazione descritto dallo storico Polibio.

Il cifrario di Playfer usa una scacchiera, molto simile a quella di Polibio,

in cui le 25 lettere (la Q viene esclusa) vengono disposte a caso. Alternativamente, la scacchiera poteva essere costruita utilizzando una parola chiave per le prime entrate della matrice con l'aggiunta delle lettere restanti nell'ordine naturale.

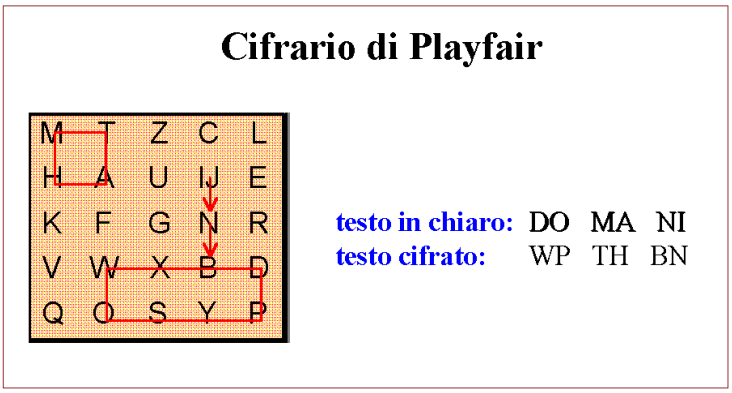


Figure 1.11
Cifrario di Playfer

La regola di cifratura viene applicata a *coppie* di caratteri e distingue tre casi, a seconda che questi occupino le stessa riga, la stessa colonna o si trovino in righe e colonne differenti. Nel primo e nel secondo caso, la coppia di caratteri in chiaro viene sostituita dai due caratteri successivi nella scacchiera i.e., per le righe la coppia WB diventa XD, FG diventa GN, mentre per le colonne, UX diventa GS e RP diventa DL. Se uno dei caratteri si trova all'estremo di una riga o colonna il successivo viene considerato il carattere che si trova all'altro estremo (ordinamento circolare). Nel caso in cui, invece, i caratteri siano su righe e colonne diverse, la tecnica di sostituzione è la seguente: poichè i due caratteri individuano la diagonale di un quadrato, essi vengono sostituiti con i caratteri che giacciono alle estremità dell'altra diagonale. Per esempio, NT diventa FC, mentre TN diventerebbe CF.

E' immediato notare che con questa tecnica non possono essere cifrate le doppie, ma l'inconveniente può essere facilmente aggirato introducendo nel messaggio in chiaro delle nulle.

Come già accaduto per il quadro di Vigenere, la cui paternità spetterebbe a Tritemio, il cifrario di Playfer, in realtà si deve ad un'altra persona: Charles Wheatstone, illustre scienziato e progettista di uno dei primi telegrafi. In realtà i due erano vicini di casa e buoni amici.

Anche i cifrari di Felix Marie Delastelle, rappresentante della grande scuola francese vissuto tra il 1840 e i 1902, usano una scacchiera con venticinque lettere disposte a caso. Il Bifido spezza il messaggio in gruppi di 5 lettere e realizza la cifratura attraverso i seguenti passi: prima di tutto forma, per ogni gruppo, una tabellina di tre righe e cinque colonne. Nella

prima riga dispone i caratteri del messaggio in chiaro, nella seconda e nella terza, rispettivamente, i numeri di riga e di colonna nella scacchiera dei caratteri inseriti nella prima riga. Quindi riporta su una linea una sequenza di coppie di numeri ottenute considerando prima i numeri della seconda riga della tabellina e poi quelli della terza. Le coppie così ottenute, per tutti i blocchi del messaggio in chiaro, possono essere sostituite dai caratteri che individuano nella scacchiera. La sequenza di caratteri generata rappresenta il cifrato. L'operazione di decifratura naturalmente richiede i passi inversi.

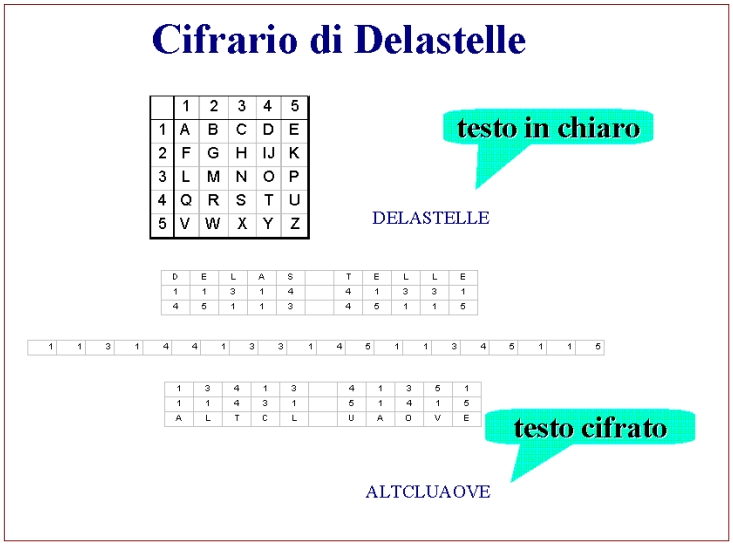


Figure 1.12
Cifrario di Delastelle

Il cifrario è detto bifido per il fatto che le coordinate dei caratteri sono coppie. Il modello Trifido funziona allo stesso modo, con l'unica variante che, invece di una scacchiera bidimensionale, i caratteri sono disposti in una scacchiera tridimensionale e, quindi, sono individuati da tre coordinate.

Con i cifrari di Playfer e quelli di Delastelle si giunge alle soglie del Novecento. È già stato inventato il telegrafo e la società delle comunicazioni globali comincia a prender forma. Parimenti, comincia a delinearsi l'esigenza di strumenti di cifratura dei messaggi maggiormente idonei alle sfide che i nuovi strumenti tecnologici prospettano.

1.9 Le macchine cifranti

UNA MACCHINA cifrante è semplicemente un dispositivo di natura meccanica o elettromeccanica che trasforma, attraverso una manipolazione

stabilita dal congegno, un messaggio in chiaro in un messaggio cifrato, e viceversa. L'idea di un cifrario meccanico nasce nel secolo XVIII sull'onda dei successi e dell'entusiasmo per il "meccanico" che l'invenzione dei primi telai aveva portato con sè. La possibilità di automatizzare operazioni tediose o faticose viene esplorata in svariate attività. Tra queste, anche in crittografia.

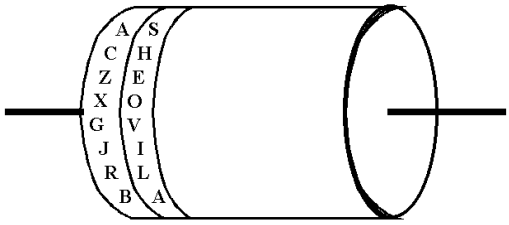
Una caratteristica tecnica che accomuna quasi tutte le macchine cifranti progettate tra la fine del '700 e la seconda guerra mondiale è l'uso di dischi rotanti.

Il primo esempio di questo tipo di macchine è il cilindro di Jefferson. L'autore non necessita di molte presentazioni: uno degli autori della Dichiarazione d'Indipendenza e successivamente Presidente degli Stati Uniti d'America.

La sua macchina era costituita da 36 dischi, imperniati su di un asse, in grado di ruotare liberamente. Ogni disco riportava le 26 lettere dell'alfabeto sul bordo esterno, in un ordine differente l'uno rispetto all'altro. La cifratura di un messaggio avveniva al modo seguente. Il messaggio veniva prima di tutto diviso in blocchi di 36 caratteri. Per ogni blocco, i dischi della macchina venivano ruotati in modo tale da far comparire allineati su una riga i caratteri del blocco. Una volta effettuata l'operazione, si sceglieva a caso un'altra riga, e si considerava la corrispondente sequenza di 36 lettere come il messaggio cifrato. Il ricevente, che possedeva un cilindro identico a quello del trasmittente, non doveva far altro che ruotare i dischi in modo tale da far comparire il cifrato allineato su una riga. Compiuta questa operazione, doveva analizzare le restanti righe. Una sola avrebbe presentato una sequenza di senso compiuto: il messaggio in chiaro. Alternativamente, il trasmittente ed il ricevente potevano accordarsi anticipatamente sulla riga in cui sarebbe comparso il messaggio in chiaro durante la decifratura.

Cilindro di Thomas Jefferson

Cilindro di 15cm e 36 dischi di legno



Numero possibili ordinamenti dei dischi = $36! \approx 3.72 \cdot 10^{41}$

Figure 1.13
Cilindro di Jefferson

Le macchine a rotori, realizzate nel primo novecento, sono ben più complesse del cilindro di Jefferson e sono di natura elettromeccanica. Da un punto di vista concettuale esse realizzano un cifrario a sostituzione polialfabetico simile al cifrario di Vigenere. La differenza principale sta nel fatto che il cifrario di Vigenere ha in genere un periodo breve, uguale alla lunghezza della chiave, mentre nelle macchine a rotori il periodo può anche prevedere milioni di sostituzioni. Ragion per cui, è come se ad ogni carattere del messaggio in chiaro venisse applicata una sostituzione diversa.

Tecnicamente l'architettura e il funzionamento tipici sono i seguenti: un rotore è un disco ricoperto di materiale isolante che ha su entrambe le facce 26 contatti etichettati con le 26 lettere dell'alfabeto. Una macchina è realizzata interconnettendo più rotori in modo tale che i contatti delle facce adiacenti siano collegati.

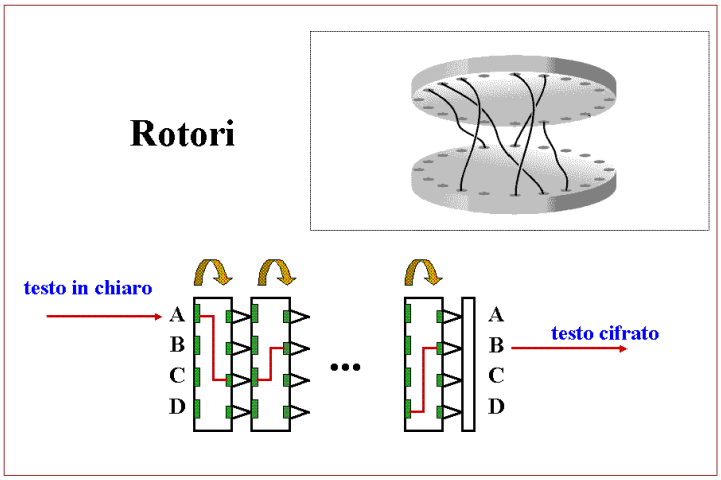


Figure 1.14
Struttura di un rotore

Precisamente, come mostrato in figura, i contatti dei rotori contigui sono in "qualche modo" incrociati. Il primo rotore viene chiamato statore perchè nell'operazione di cifratura viene tenuto fisso. Ogni volta che sullo statore viene attivato un contatto, il segnale elettrico si propaga attraverso i rotori intermedi fino a raggiungere il rotore d'uscita che mostra un solo contatto attivo, il carattere cifrato.

Supponiamo che entrambi i comunicanti abbiano una macchina a rotori nella stessa configurazione iniziale, cioè una macchina in cui le disposizione dei contatti tra i rotori adiacenti siano le stesse. L'operazione di cifratura avviene al modo seguente: per la prima lettera del messaggio in chiaro viene attivato il contatto corrispondente sullo statore. Il segnale elettrico si propaga attraverso i contatti interni giungendo sul disco d'uscita

ove si legge il carattere cifrato. A questo punto, il primo rotore viene ruotato di una unità. Per comodità diremo che effettua uno scatto. Quindi si procede alla cifratura del secondo carattere. Ancora, il primo rotore scatta. Quindi si procede alla cifratura del terzo carattere, il rotore scatta nuovamente e così via. Dopo le prime 26 cifrature oltre a scattare il primo rotore di una unità scatta anche il secondo di una unità. In realtà il meccanismo prevede che il primo rotore effettui uno scatto ad ogni cifratura, il secondo ad ogni 26 cifrature, il terzo ad ogni $26 * 26$ cifrature e via discorrendo. Facendo scattare ad ogni passo i rotori della macchina, si modificano le *relazioni* tra i contatti interni e, quindi, si cambia la sostituzione che viene applicata al carattere in ingresso. L'operazione di decifratura, richiede che le funzioni del disco di ingresso e di uscita siano invertite. Precisamente, i caratteri vengono inseriti sulla faccia esterna del rotore d'uscita e il carattere che si ottiene sul disco di ingresso rappresenta il carattere in chiaro. Ovviamente, gli scatti vanno effettuati esattamente nello stesso ordine in cui sono stati effettuati in fase di cifratura, dal primo disco verso l'ultimo.

Il prototipo descritto modellizza diverse macchine a rotori effettivamente realizzate nel secolo scorso. Una delle più famose è senza dubbio l'Enigma, usata nella seconda guerra mondiale dai tedeschi e rotta dagli inglesi grazie al contributo di un grande logico matematico, Alan Turing. L'enigma disponeva di una tastiera che permetteva di fornire i caratteri allo statore e di un disco finale chiamato invertitore. Il cifrato, raggiunto l'invertitore, veniva rispedito verso lo statore, percorrendo in senso inverso i rotori. Una volta raggiunto lo statore veniva poi visualizzato su un pannello luminoso. In tal modo la decifratura era semplificata. Ogni carattere definiva un percorso univoco statore-invertitore-statore Pertanto, riportando la macchina nella configurazione iniziale e digitando i caratteri cifrati uno di seguito all'altro, faceva si che questi effettuassero il percorso statore-invertitore-statore nella direzione inversa. In tal modo, sul pannello luminoso compariva il messaggio in chiaro. Durante le guerra vennero prodotte più versioni di Enigma che presentavano opzioni e differenti livelli di complessità.

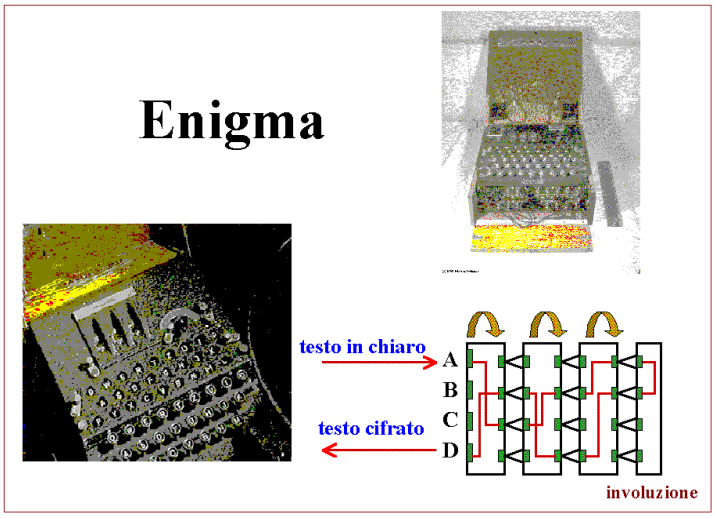


Figure 1.15
Enigma

Scardinare l'Enigma è stato uno dei più grandi successi ottenuti dai crittoanalisti nel secolo scorso. In particolare, l'attacco degli inglesi utilizzava grosse macchine, chiamate *bombe*, ed era stato messo a punto perfezionando e generalizzando i risultati ottenuti prima della II guerra mondiale da studiosi polacchi che si erano cimentati nell'impresa.

1.10 One time pad

NEL 1917 , Gilbert Vernam, un impiegato della AT&T, mise a punto un sistema di cifratura per messaggi rappresentati in binario che risulta teoricamente inattaccabile.

Prima di tutto, i due comunicanti costruiscono una stringa di *bit casuali*, lunga quanto il messaggio da cifrare. Un modo per generare questa stringa consiste nel lanciare una moneta, una volta per ogni bit del messaggio, e memorizzare un 1 se esce testa e uno 0 se esce croce. La concatenazione di questi bit forma una stringa totalmente casuale, essendo i lanci della moneta indipendenti l'uno dall'altro ed essendo, in ogni lancio, la probabilità di avere testa esattamente uguale a quella di avere croce. Questa stringa rappresenta la *chiave* del cifrario.

L'operazione di cifratura consiste nel calcolare l'or esclusivo bit per bit del messaggio in chiaro e della stringa casuale. L'operazione di decifratura funziona esattamente come la cifratura: il messaggio in chiaro viene recuperato facendo l'or esclusivo bit per bit del messaggio cifrato con la chiave.

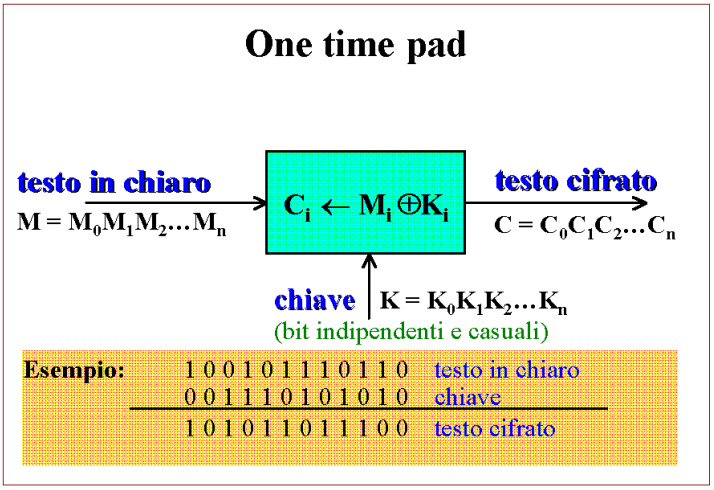


Figure 1.16
Cifrario di Vernam

La proprietà fondamentale del cifrario di Vernam è la cosiddetta sicurezza perfetta. Intuitivamente, un cifrario è perfetto se l'indecisione nello stabilire qual è il testo in chiaro X senza conoscere il testo cifrato Y è la stessa che si ha sul testo in chiaro X conoscendo il testo cifrato Y.

Il cifrario di Vernam è perfetto se la chiave di cifratura viene utilizzata una sola volta. Per tale ragione, viene detto *one-time-pad*. Infatti, poichè la chiave è una stringa totalmente casuale, anche il messaggio cifrato risulta una stringa totalmente casuale. Pertanto, le dipendenze frequentistiche, tipiche dei linguaggi naturali, e punto d'appoggio dei crittoanalisti per carpire informazioni sul messaggio in chiaro, vengono a cadere completamente. Un eventuale ascoltatore indiscreto sprovvisto della chiave, dall'analisi del cifrato non riesce ad ottenere alcuna informazione sul messaggio in chiaro

In realtà, quando abbiamo introdotto il concetto di cifrario, non abbiamo specificato che cosa intendevamo per sicuro in modo rigoroso. Certamente Oscar non deve essere in grado di recuperare nè la chiave segreta nè il messaggio. Ma potrebbe recuperarlo in parte. O potrebbe avere *informazioni parziali*.

Matematicamente è difficile cogliere l'intuizione che è alla base del concetto di sicurezza. Tuttavia, Claude Shannon, padre della Teoria dell'Informazione, in un articolo pubblicato nel 1949, dal titolo *Communication Theory of Secrecy Systems*, ha gettato le basi per un'analisi matematica rigorosa della sicurezza dei sistemi di comunicazione. Egli ha dimostrato che un cifrario che esibisce il massimo grado di sicurezza deve utilizzare una chiave almeno tanto lunga quanto il messaggio che si intende trasmettere. Ciò significa essenzialmente due cose: il cifrario di Vernam è impenetrabile dal punto di vista della sicurezza e, nello stesso tempo, non si può fare

di meglio.

Gli storici sostengono che questo cifrario è stato utilizzato nelle comunicazioni riservate ad altissimo rischio: per esempio si dice che venisse usato tra il Presidente degli Stati Uniti e il Presidente delle Repubbliche Socialiste Sovietiche, sulla cosiddetta *linea rossa*, così come sembra che Che Guevara usasse un cifrario di Vernam su *alfabeto decimale* per proteggere le proprie comunicazioni con Fidel Castro.

Tuttavia, come detto, il cifrario di Vernam costa. Ogni volta che Alice e Bob vogliono scambiarsi un messaggio lungo n bit, debbono in precedenza accordarsi su una chiave lunga n bit. Che fare allora? E' possibile ottenere un cifrario "quasi" perfettamente sicuro con chiavi più corte ed usabili più di una volta? E se per caso Alice e Bob non si conoscono? Come possono accordarsi su una chiave? Possono fare altrimenti?

Sul tentativo di offrire risposte concrete a questi interrogativi nasce la Crittografia Moderna. Ma questi interrogativi e tutti gli altri ad esso connessi, sanciscono anche la conclusione di quell'avventura storica di cui abbiamo evidenziato le tappe salienti e che è stata racchiusa sotto il nome di Crittografia Classica.

1.11 Note e ulteriori letture

La storia delle scritture segrete e dei cifrari prodotti fino alla prima metà del secolo scorso è affascinante e, ovviamente, non può essere esaurita in poche pagine. Il lettore interessato ad approfondire sensibilmente le proprie conoscenze in materia può consultare *The Codebreakers*, dello storico David Kahn, opera completa e a dir poco esaustiva sull'argomento.

Un'altra lettura che consigliamo, che copre anche i recenti sviluppi negli studi crittografici, è *Codici & Segreti* di Simon Singh. Questo libro è di piacevole lettura ed è ricco di aneddoti e curiosità storiche.

Per uno sguardo rivolto essenzialmente alla storia della crittografia in Italia consigliamo, invece, la lettura dell'ultimo capitolo di *Crittologia*, scritto da Luigia Berardi e Albrecht Beutelspacher.

Infine, una sintetica ed intelligente panoramica delle tecniche classiche, seppur di qualche anno fa, che consigliamo di leggere è *Codici Segreti* di A. Sgarro.

Nei testi citati è possibile trovare buona parte delle tecniche descritte e degli aneddoti raccontati nonchè abbondanza di riferimenti utili per approfondire gli aspetti che il lettore ha trovato di maggiore interesse.