Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Luigia Berardi, Albrecht Beutelspacher

La storia della crittografia: l'uso dei gruppi ciclici per costruire codici

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **6-A**—*La Matematica nella Società e nella Cultura* (2003), n.1, p. 105–118.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2003_8_6A_1_105_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2003.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol. VI-A, Aprile 2003, 105-118

La storia della crittografia: l'uso dei gruppi ciclici per costruire codici.

Luigia Berardi - Albrecht Beutelspacher

La nascita della crittografia, che è l'arte di nascondere messaggi, si perde nei tempi, infatti il bisogno di trasmettere messaggi segreti è stato sentito non appena nell'uomo si è sviluppata la capacità di comunicare.

La crittografia, dopo aver giocato nelle varie società ruoli diversi, a seconda dei momenti storici, oggi risulta indispensabile in moltissimi ambienti, come, ad esempio, quello politico, commerciale e privato.

In questo articolo mettiamo in luce alcuni momenti significativi della storia della crittografia.

Lo scopo della crittografia è quello di inventare codici sicuri; la sicurezza dei metodi usati è andata aumentando sempre di più col passare del tempo.

• Chiave

In questo contesto un ruolo molto importante è giocato dalla **chiave** del codice. Agli inizi della storia della crittografia venivano usati metodi primordiali che erano quasi senza chiave; la nozione di chiave, diventata centrale nella crittografia, è stata introdotta col passare del tempo. Oggi ogni codice deve poter avere moltissime chiavi.

• Matematica

La matematica, pur essendo stata sempre presente nella crittografia, è apparsa in modo esplicito solo dagli anni '40 in poi; essa serve sia per rompere codici che per costruire buoni codici. È molto in-

teressante osservare che un motivo ricorrente in crittografia è l'uso di strutture cicliche. Ciò si può vedere fin dall'inizio della storia, esattamente nella scitala e, poi, nel codice di Cesare. Nelle macchine cifranti, delle quali elementi fondamentali onnipresenti sono i rotori, la nozione di gruppo ciclico quasi si materializza. Negli algoritmi moderni l'essenza matematica è presente attraverso i gruppi ciclici, ad esempio Z_p^* e il gruppo moltiplicativo di un campo finito, o il gruppo di una curva ellittica.

L'idea della crittografia.

Il modello fondamentale della crittografia prevede un **mittente** A, un **destinatario** B ed un **attaccante** X. Il mittente vuole inviare un messaggio al destinatario in modo segreto; segreto vuol dire che l'attaccante non ha nessuna possibilità di conoscere il messaggio.

Per ottenere ciò ci sono sostanzialmente due metodi, il primo dei quali è la **steganografia** (parola proveniente dal greco, che significa scrittura coperta). Questo modo consiste nel nascondere il messaggio così che l'attaccante non possa notare la sua trasmissione. Ad esempio si può celare il messaggio in un testo più lungo, nel quale il destinatario possa riconoscere le lettere che costituiscono il messaggio.

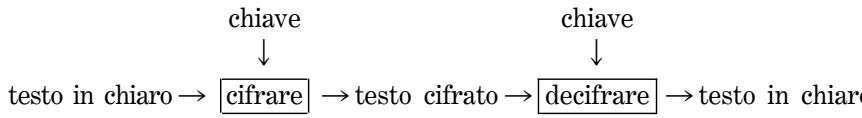
C'è una variante moderna di questo metodo, che consiste nel nascondere il messaggio in una immagine costruita con il computer. Il destinatario deve sapere quali pixel deve prendere in considerazione.

Un altro metodo passato alla storia è basato sull'uso dell'inchiostro simpatico.

Il secondo metodo usato è la crittografia, nella quale si procede in modo completamente diverso.

L'attaccante può vedere che viene trasmesso un messaggio, ma non ha modo di conoscere il messaggio vero; più precisamente, il trasmettitore trasforma il testo in chiaro m in un testo cifrato c e trasmette c. Il ricevitore è in grado di ricostruire m da c. Solo il ricevitore deve essere in grado di eseguire questa operazione, di conseguenza la sua posizione deve essere avvantaggiata rispetto a quella di chiunque altro. Questo vantaggio si realizza con l'uso di una chiave segreta, nota al ricevitore.

I codici della crittografia classica sono costruiti in modo tale che anche il mittente conosca la chiave segreta. Essa è usata dal mittente per cifrare e dal destinatario per decifrare il testo cifrato. Lo schema è quello della figura seguente.



Oggi vengono usati anche altri codici basati su un principio diverso da quello appena detto, più precisamente, in essi per cifrare e decifrare non si usa la stessa chiave (cfr. [1], [2]).

Antichità.

Parliamo ora di due metodi usati nell'antichità, che costituiscono i prototipi di due tipi di cifrari: i **codici a trasposizione** ed i **codici a sostituzione** (cfr. [1]).

Come prototipo dei primi illustriamo la **scitala lacedemonica**, usata a Sparta circa 2500 anni fa, come c'è stato tramandato da Plutarco.

La scitala era un cilindro usato per trasmettere un messaggio in modo segreto. Il metodo consisteva nell'avvolgere intorno alla scitala un nastro, sul quale veniva scritto il messaggio in righe longitudinali.

Finita l'operazione, si svolgeva il nastro, che veniva mandato al destinatario. Il destinatario era in possesso di un cilindro identico a quello usato; riavvolgendo la stringa su di esso, il messaggio si ricomponeva, così che poteva essere letto.

La chiave di questo codice è data dal diametro del cilindro.

Osserviamo che la stringa non avvolta contiene tutte e sole le lettere che compongono il messaggio, ma in un ordine diverso.

Un codice basato su questo principio si chiama a **trasposizione**: noi possiamo interpretare la scitala come sistema con chiave segreta, ma è chiaro che gli spartani non avevano questa nozione.

Codici basati su un principio completamente diverso sono quelli a

sostituzione; in essi ogni lettera del testo in chiaro viene trasformata in un'altra lettera.

Il prototipo storico di questi codici è il **codice di Cesare**, usato da Cesare Augusto, come possiamo leggere nelle Vitae Caesarorum di Svetonio.

Tale codice è basato sull'uso di un **alfabeto in chiaro** ed un **alfabeto segreto**, che sono quelli della figura seguente.

Alf. in chiaro:	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
Alf. segreto:	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

Una qualsiasi lettera del testo in chiaro viene cifrata nella lettera dell'alfabeto segreto che si trova sotto di essa. Ad esempio, la frase *Alea iacta est* diventa *DOHD LDFWD HVW*.

Osserviamo che l'alfabeto segreto usato da Cesare si ottiene shiftando circolarmente le lettere dell'alfabeto in chiaro di tre posizioni a sinistra.

Dal nostro punto di vista è facile interpretare lo shift di tre posizioni come chiave ed, allo stesso tempo, generalizzare il codice usando una chiave data da uno shift di un qualsiasi numero di lettere.

Si può generalizzare ulteriormente il codice di Cesare, ottenendo un **codice monoalfabetico**. Esso consiste nell'uso di un alfabeto segreto ottenuto da quello in chiaro con una permutazione qualsiasi. Segue che, se l'alfabeto in chiaro è di 26 lettere, il numero dei codici monoalfabetici è

$$26! = 403.291.461.126.605.635.584.000.000 \approx 4 \cdot 10^{26}.$$

La crittoanalisi: un'invenzione degli arabi.

Nel 700 d. C. la civiltà islamica era la civiltà più fiorente in molti campi della cultura, come ad esempio la pittura e la scienza. Tale sviluppo era dovuto anche ad una buona amministrazione sociale e politica, che, prevedendo una bassa pressione fiscale, aveva dato un grande impulso a molte attività. In particolare venivano usati sistematicamente i mezzi della crittografia per cifrare importanti documenti ed, in particolare, la documentazione fiscale.

In questo ambito il loro merito maggiore è di aver inventato la **crittoanalisi**, che, oltre ad essere l'arte per rompere i codici segreti, permette di valutare la sicurezza offerta da un codice.

Nelle scuole teologiche sorte nel mondo arabo veniva fatta anche un'analisi linguistica molto accurata dei testi coranici, analisi che richiedeva in particolare la conoscenza della frequenza sia di alcune parole importanti che delle singole lettere. Principalmente a ciò è dovuta la loro predisposizione per la crittoanalisi dei codici monoalfabetici.

Abu Yusuf ibn Ishaq al-Kindi, il filosofo degli arabi, fu il primo a scrivere nel IX secolo un trattato di crittoanalisi dal titolo *Sulla decifrazione dei messaggi crittati*, in cui spiega con grande chiarezza i metodi basilari della crittoanalisi ([5]).

Come facile esempio facciamo la crittoanalisi di un testo cifrato col codice di Cesare.

Nella lingua italiana le lettere più frequenti sono le vocali a, e, i, o, che si presentano con una frequenza di circa il 10% ognuna.

Nell'alfabeto le distanze delle vocali a, e, i, o, prese ordinatamente ed in modo ciclico, sono 4, 4, 6 e 12.

È chiaro che usando un codice monoalfabetico, si conservano non solo le frequenze delle lettere, ma anche le distanze tra le lettere.

Allora, per fare la crittoanalisi, si procede come segue.

- Si determinano le quattro lettere più frequenti del testo cifrato, che, per quanto detto, corrispondono alle lettere a, e, i, o del testo in chiaro.

- Supponiamo che le lettere più frequenti in un testo cifrato siano k, o, s, y. Le loro distanze sono 4, 4, 6, 12, ordinatamente. L'alfabeto segreto si ottiene shiftando in modo che k si trovi sotto la a e, di conseguenza, o sotto la e, s sotto la i ed y sotto la o.

Osserviamo che in molte lingue, come ad esempio l'inglese, il tedesco, il francese, c'è una lettera molto più frequente di tutte le altre; nelle lingue citate tale lettera è la e. In questi casi basta determinare la lettera più frequente del testo cifrato.

La rinascita della crittografia.

I codici monoalfabetici non offrivano una sicurezza accettabile; ciò fu particolarmente chiaro dopo le scoperte degli arabi relative alla crittoanalisi. Nel rinascimento si fa un grosso passo avanti, inventando i codici polialfabetici.

I nomi principali in questo ambito sono Leon Battista Alberti (1404-1472), Giovan Battista Della Porta (1535-1615), Gerolamo Cardano (1501-1576), Johann von Heidemberg da Trittenheim (noto in Italia come Tritemio) (1462-1516) e Blaise de Vigenere (1523-1596) (cfr.[1]).

Leon Battista Alberti fu il primo a mettere in evidenza un ordine ciclico, inventando i cosiddetti cerchi dell'Alberti, rimasti in uso per circa cinque secoli. I cerchi dell'Alberti sono due dischi concentrici, dei quali uno un po' più piccolo dell'altro.

Lungo il bordo del disco più esterno è riportato l'alfabeto nell'ordine naturale, mentre lungo il bordo del disco più interno sono riportate le lettere in un ordine casuale prefissato.

Per cifrare una lettera, si trova tale lettera nel disco più esterno e la si sostituisce con la lettera corrispondente ad essa nel disco più interno.

L'idea nuova è di ruotare il disco interno rispetto a quello esterno in modo da usare diversi alfabeti segreti per cifrare lo stesso testo in chiaro.

È ovvio che in questo modo si ottiene un appiattimento delle frequenze delle lettere del testo segreto; di conseguenza la crittoanalisi descritta non funziona più.

Più in dettaglio, ogni disco porta sul bordo 24 caselle; nel disco più esterno si trovano oltre le lettere dell'alfabeto in chiaro, escluse le lettere h, j, k, q, w, y, i numeri 1, 2, 3 e 4. Il disco interno contiene 24 lettere disposte casualmente; la lettera w non compare ed $u = v$.

Il mittente ed il destinatario scelgono una lettera dell'alfabeto in chiaro, tale lettera è detta **indice** e costituisce la chiave segreta.

Come prima lettera del testo cifrato si scrive la lettera dell'alfabeto segreto corrispondente all'indice scelto, così si comunica

al destinatario l'alfabeto segreto scelto. Si cifra poi un numero arbitrario di lettere del testo in chiaro.

Quando si vuole cambiare l'alfabeto segreto, si sceglie uno dei quattro numeri presenti nel disco esterno e si cifra tale numero. Fatto ciò, si ruota il disco fino a quando la lettera che ha cifrato il numero scelto vada sotto l'indice fissato. In questo modo si ha un altro alfabeto segreto. Tale cambio si può ripetere quando si vuole e quante volte si vuole.

Il pregio di questo codice, come dei codici polialfabetici in genere, è quello di rendere più o meno uguali le frequenze delle lettere. È da notare inoltre che i cerchi dell'Alberti costituiscono il prototipo di quasi tutte le macchine cifranti realizzate fino ad oggi.

Il difetto di esso è quello di avere poche chiavi, esattamente 24; di conseguenza è molto facile rompere il codice usando il metodo esaustivo.

Circa un secolo dopo, nel 1587, Blaise de Vigenere, un diplomatico francese, usando anche alcune idee di Della Porta ed altri, mette a punto un codice polialfabetico che ha avuto molto successo.

L'idea è di usare in ordine ciclico diversi alfabeti segreti, che sono individuati da una parola, detta **parola chiave**.

Si usa il quadrato di Vigenere, che consiste dei 26 alfabeti di Cesare in ordine alfabetico.

Prima di cifrare si scrive la parola chiave il numero di volte necessario in modo che ad ogni lettera del testo in chiaro corrisponda una lettera della parola chiave.

La cifratura di una lettera è determinata dalla lettera in chiaro e dalla corrispondente lettera della parola chiave. Precisamente, la lettera cifrata è la lettera che si trova sulla riga che comincia con la lettera della parola chiave e sulla colonna che comincia con la lettera in chiaro. In altre parole, per cifrare si usa l'alfabeto che comincia con la lettera della parola chiave corrispondente, così come appare dal seguente esempio.

Parola chiave R E B U S R E B U S R E B U S R E B U S R E B U
Testo chiaro L a m a t e m a t i c a r i s u l t a u t i l e
Testo cifrato C E N U L V Q B N A T E S C K L P U U M K M M Y

Figura 1. – Blaise de Vigenere. Incisione di Thomas de Leu. Cliché Bibliothèque Nationale de France, Paris.

Notiamo che il quadrato di Vigenere è una diversa presentazione della tabella dell'addizione in Z_{26}. Infatti, se identifichiamo la A con 0, la B con 1, …, la Z con 25, allora per cifrare si procede come segue.

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

Il quadrato di Vigenere

Traduciamo la lettera del testo in chiaro e la lettera chiave corrispondente in numeri, sommiamo poi tali numeri modulo 26 e, infine, riconvertiamo il numero ottenuto nella corrispondente lettera.

Per decifrare si compie l'operazione in senso inverso, cioè alla lettera cifrata si sottrae la lettera chiave corrispondente, sempre modulo 26.

I limiti dei codici polialfabetici.

I codici polialfabetici hanno resistito per secoli, infatti sono stati forzati solo nella metà del 1800, per opera di Charles Babbage e di Friedrich Wilhelm Kasiski, indipendentemente.

Descriviamo la crittoanalisi del codice di Vigenere, che consiste di due passi principali.

1) Supponiamo di conoscere la lunghezza h della parola chiave. Di conseguenza si sa che dopo h lettere la sequenza degli alfabeti usati si ripete; in altre parole le lettere che occupano i posti n^{ro} 1, $h+1$, $2h+1$, … sono state cifrate usando lo stesso alfabeto di Cesare. Quindi usando per le lettere dette l'analisi statistica già descritta possiamo conoscere l'alfabeto usato e quindi la lettera della parola chiave. Analogamente si procede con l'insieme delle lettere che occupano i posti n^{ro} 2, $h+2$, $2h+2$, … e così via.

2) Vogliamo ora determinare la lunghezza della parola chiave. Allo scopo viene esaminata ed usata la struttura del testo cifrato.

Sappiamo che in genere una stessa lettera presente più di una volta nel testo in chiaro non viene cifrata sempre nella stessa lettera, a maggior ragione, se una parola compare più di una volta nel testo in chiaro, dà luogo a sequenze diverse del testo cifrato.

Ciò non avviene solo se in corrispondenza di una lettera che compare due volte nel testo in chiaro, si trova la stessa lettera chiave. Inoltre, se una parola compare due volte e, in corrispondenza della prima sua lettera si trova la stessa lettera della parola chiave, allora si ottengono due sequenze cifrate uguali tra loro.

Proprio su questa osservazione si basa il **test di Kasiski**. Infatti, in primo luogo, si cercano nel testo cifrato le sequenze uguali. Supponiamo che le sequenze uguali siano dovute al fatto appena detto, cioè che la lettera chiave che si trova in corrispondenza della prima lettera delle sequenze uguali sia la stessa, in altre parole che la «distanza» tra le due sequenze uguali sia un multiplo della lunghezza della parola chiave. È chiaro che l'ipotesi fatta è tanto più realistica quanto più lunghe sono le sequenze uguali tra loro.

Dopo aver trovato le sequenze di almeno tre lettere uguali tra loro, si calcola il massimo comun divisore delle loro distanze. Molto probabilmente tale massimo comun divisore è la lunghezza della parola chiave.

Il codice insuperabile.

La crittoanalisi dei codici polialfabetici è possibile solo se la parola chiave è corta rispetto al testo; conseguenza di questa osservazione è che bisogna usare parole chiave più lunghe possibile. Inoltre, se una parola chiave ha una struttura, ad esempio se una lettera si ripete molte volte, una crittoanalisi è ancora possibile; quindi per avere un codice sicuro, si deve usare una sequenza casuale di lettere avente la stessa lunghezza del testo in chiaro.

Questo si può fare prendendo come alfabeto un qualunque insieme munito di una struttura di gruppo. Finora abbiamo considerato sempre l'alfabeto naturale, cioè Z_{26}, ora fissiamo come alfabeto Z_2, cioè l'insieme dei bits $\{0, 1\}$, in altre parole l'alfabeto binario. In questo ordine di idee si ottiene l'**one-time pad**, inventato da Gilbert S. Vernam nel 1917.

Supponiamo che il testo in chiaro e la chiave siano rispettivamente le sequenze di bits $a_1 a_2 \ldots$ e $k_1 k_2 \ldots$. Il testo cifrato si ottiene sommando modulo 2, bit a bit, il bit del testo in chiaro ed il bit corrispondente della parola chiave, cioè $c_1 = a_1 \oplus k_1$, $c_2 = a_2 \oplus k_2$, ...

Si dimostra che, se $k_1 k_2 \ldots$ è una sequenza casuale, ad esempio ottenuta da lanci ripetuti di una moneta, allora il codice è **perfetto**, cioè un attaccante, avendo tutte le informazioni possibili su una parte del testo cifrato, non riesce a dedurre nessuna informazione neanche su un solo bit seguente. Ciò vuol dire che il codice è inviolabile.

Ma non è tutto oro quel che luce, infatti per usare il codice di Vernam il mittente deve inviare al destinatario la chiave in modo segreto. Essendo la chiave lunga quanto il testo in chiaro, segue che l'one-time pad può essere usato solo in occasioni veramente speciali.

L'one-time pad costituisce il modello di molti codici usati nella pratica, esattamente i codici a flusso, nei quali la sorgente casuale per i bit della chiave viene sostituita da una sorgente pseudocasuale.

È chiaro che la sicurezza del codice si riduce ed è data dalla sicurezza che offre la sorgente pseudocasuale (cfr. [1], [3] cap. 6).

Matematica materializzata.

Nella prima metà del 1900 i codici sono stati realizzati con macchine cifranti, sia meccaniche che elettromeccaniche. Il cuore di esse è un insieme di «rotori», cioè dischi, interconnessi tra loro con lo stesso principio usato nel contachilometri di una macchina.

Descriviamo da vicino la macchina più famosa, l'**ENIGMA**, inventata nel 1918 da Arthur Scherbius.

Nel suo esterno appaiono, oltre ad una tastiera, anche le 26 lettere, ordinate come in una tastiera, ognuna delle quali è collegata con una lampadina. Premendo un tasto con la lettera in chiaro, si accende una delle 26 lettere, che è la lettera cifrata.

Sempre all'esterno si vedono, collegati tra loro, tre o più rotori, la cui funzione è quella di cifrare. Ogni rotore ha due facce, su ognuna delle quali compaiono tutte le lettere dell'alfabeto. Ogni lettera di una faccia è collegata elettricamente con una lettera dell'altra faccia; in altre parole, in ogni rotore si realizza una permutazione delle lettere.

Ogni rotore è collegato elettricamente con i rotori successivi.

Quando viene premuto un tasto della tastiera, quella lettera, tradotta in un impulso elettrico, va nel primo rotore, poi nel secondo e quindi nel terzo, seguendo i collegamenti prefissati. Dal terzo rotore va al riflessore, che dà in uscita una lettera diversa da quella in entrata. Tale lettera ricompie tutto il cammino fatto, seguendo un altro percorso, dando come risultato finale la lettera cifrata.

Dopo il passaggio di una lettera, il primo rotore ruota di un posto, così che la lettera successiva non viene cifrata dal primo rotore con lo stesso alfabeto.

Quando il primo rotore ha compiuto una rotazione di 26 posti, comincia a ruotare di un posto alla volta il secondo rotore e poi il terzo.

La chiave dell'ENIGMA consiste essenzialmente nella posizione dei tre rotori; poiché ogni rotore può assumere 26 posizioni, le chiavi possibili sono 17576.

L'ENIGMA, usata moltissimo dai tedeschi durante la seconda guerra mondiale, fu forzata dai polacchi e poi dagli inglesi; ma ciò ri-

mase un segreto e gli inglesi continuarono a decrittare messaggi cifrati dei tedeschi. Solo trenta anni più tardi la cosa diventò di dominio pubblico (cfr. [1]).

L'era del computer.

Per rompere l'ENIGMA c'è stato bisogno di fare molte statistiche; questo lavoro fu svolto dagli inglesi in Bletchley Park, dove lavorava qualche migliaio di persone, delle quali alcune svolgevano un lavoro intellettuale, come, ad esempio, Alan Turing, ed altre, molte di più, un semplice lavoro di routine.

Appare chiaro che questo tipo di lavoro è ideale per un computer, di conseguenza non è casuale che i primi computer, i Colossus, siano stati costruiti ed usati per rompere i codici.

È anche vero che i computer di oggi sono strumenti con una grande capacità di fare analisi statistiche; di conseguenza i codici che si usano devono essere di gran lunga migliori di quelli di qualche decennio fa.

Per l'uso di Internet e dei computer in genere, c'è bisogno di codici che garantiscano un buon livello di sicurezza, ad esempio per la compera ed il pagamento via Internet bisogna avere una sicurezza altissima. Fortunatamente, il computer è in grado anche di realizzare algoritmi con un buon livello di sicurezza.

La qualità degli algoritmi crittografici odierni non dipende solo dalla esperienza dell'ideatore, anzi è basata sempre più su strutture matematiche. Ad esempio, il 2 ottobre 2000 è stato scelto il successore del DES, che è stato chiamato AES (Advanced Encryption Standard). La struttura matematica usata nell'AES è il campo di Galois $GF(2^8)$, che contiene come elementi tutti i bytes. Internamente si usano metodi ingenui per moltiplicare e computare l'inverso dei bytes (cfr. [6]).

Concludiamo mettendo in luce che la crittografia è una scienza aperta, ciò vuol dire che, non esistendo codici usabili nella pratica, per i quali si possa dimostrare matematicamente che sono sicuri, ci saranno sempre delle sorprese. Anche l'AES non può essere un algoritmo duraturo per sempre. Se avrà una vita lunga come

quella del DES, un quarto di secolo, per l'AES sarà un successo.

In altre parole la crittografia costituisce per i matematici un campo di ricerca senza fine.

BIBLIOGRAFIA

[1] L. BERARDI - A. BEUTELSPACHER, *Crittologia*, FrancoAngeli, Milano, (1996).
[2] L. BERARDI - A. BEUTELSPACHER, *Crittografia a chiave pubblica: La matematica pura applicata al mondo reale*, di prossima pubblicazione su Bollettino U.M.I.-A, La Matematica nella Società e nella Cultura.
[3] A. J. MENEZES - P. C. VAN OORSCHOT - S. A. VANSTONE, *Handbook of Applied Cryptography*, CRC Press (1997).
[4] D. KAHN, *The Codebreakers*, Scribner, New York (1996).
[5] S. SINGH, *Codici & Segreti*, Rizzoli (1999).
[6] http://www.nist.gov/aes

L. Berardi, Dipartimento di Ingegneria Elettrica
I-67040 Monteluco di Roio (L'Aquila). E-mail: berardi@ing.univaq.it

A. Beutelspacher, Mathematisches Institut, Justus-Liebig-Universitat
Arndtstr. 2 D-35392 Giessen. E-mail: albrecht.beutelspache@math.uni-giessen.de