Protocolli per la sicurezza: come possiamo effettuare transazioni sicure su canali non sicuri come Internet e come possiamo proteggere le informazioni sulla carta di credito da commercianti fraudolenti? Discuteremo vari protocolli, tra cui SSL e SET.

Moneta elettronica: le carte di credito e altri strumenti simili sono comodi, ma non garantiscono l'anonimato. Sicuramente una forma elettronica della moneta sarebbe utile, almeno per alcune persone. Tuttavia tutto ciò che è elettronico può essere copiato. Vedremo un esempio di un sistema di moneta elettronica che garantisce l'anonimato, ma identifica i falsari.

Giochi: com'è possibile lanciare una moneta o giocare a poker con persone che non sono nella stessa stanza? Distribuire le carte, per esempio, presenta problemi. Vedremo come alcune idee crittografiche possano risolvere questi problemi.

Capitolo 2

Crittosistemi classici

Nel corso della storia, per l'uomo è sempre stato importante avere dei metodi che permettessero di camuffare i suoi messaggi rendendoli incomprensibili agli occhi degli avversari. In questo capitolo verranno presentati alcuni dei più vecchi crittosistemi in uso prima dell'avvento del computer. Questi crittosistemi sono troppo deboli per poter essere ancora usati oggi, soprattutto avendo a disposizione il calcolatore, ma illustrano bene molte idee importanti della crittologia.
Per trattare questi semplici crittosistemi si adotteranno le seguenti convenzioni.

- Il *testo in chiaro* sarà scritto in lettere minuscole, mentre il *TESTO CIFRATO* sarà scritto in lettere maiuscole (tranne nei problemi al calcolatore).
- A ogni lettera dell'alfabeto sarà assegnato un numero:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

q	r	s	t	u	v	w	x	y	z
16	17	18	19	20	21	22	23	24	25

  Come si vede, alla lettera a viene assegnato il numero 0, mentre alla lettera z viene assegnato il numero 25. Questa convenzione (diversa da quella abituale in cui a corrisponde a 1 e z a 26) è standard nei crittosistemi elementari che verranno considerati.

- Gli spazi e la punteggiatura sono omessi. Anche se questa convenzione può sembrare fastidiosa, è quasi sempre possibile ricollocare gli spazi nel testo in chiaro dopo la decifrazione. Se si lasciassero gli spazi, si avrebbero ovviamente due possibilità. Essi potrebbero essere lasciati come spazi, e allora si avrebbero talmente tante informazioni sulla struttura del messaggio che la decifrazione

diventerebbe semplice. Oppure potrebbero essere cifrati, e allora spicchebbero nell'analisi delle frequenze (a meno che il messaggio abbia in media almeno otto lettere a parola) semplificando ancora la decifrazione.

Osservazione. In questo capitolo verranno usati alcuni concetti della teoria dei numeri, in particolar modo l'aritmetica modulare. Chi non ha familiarità con le congruenze, dovrebbe leggere i primi tre paragrafi del Capitolo 3 prima di continuare.

2.1 Cifrari a scorrimento

Uno dei più antichi crittosistemi è spesso attribuito a Giulio Cesare. Se Cesare avesse voluto inviare il testo in chiaro

gallia divisa est in partes tres

rendendolo inintelligibile a Bruto, avrebbe fatto scorrere in avanti ogni lettera di tre posizioni, mandando la a in D, la b in E, la c in F e così via fino ad arrivare alle ultime lettere dell'alfabeto che sarebbero state mandate nelle prime: la x in A, la y in B e la z in C. Pertanto il testo cifrato sarebbe stato

JDOOLDGLYLVDHVWLQSDUWHVWUHV.

La decifrazione sarebbe avvenuta facendo scorrere indietro di tre posizioni ogni lettera (e cercando di immaginare dove reinserire gli spazi).
In generale si etichettano le lettere mediante gli interi da 0 a 25 e si sceglie come chiave un intero κ con $0 \leq \kappa \leq 25$. Il processo di cifratura è dato dalla funzione

$$x \mapsto x + \kappa \pmod{26}$$

mentre il processo di decifrazione è dato dalla funzione inversa

$$x \mapsto x - \kappa \pmod{26}.$$

Cesare, per esempio, usava $\kappa = 3$.
Ecco il modo in cui funzionano i quattro tipi di attacco.

1. **Solo testo cifrato.** Eva possiede solo il testo cifrato. La sua strategia migliore consiste in una ricerca esaustiva, poiché ci sono solo 26 chiavi possibili. Se il messaggio non si riduce a poche lettere (questo sarà più chiaro dopo aver discusso l'entropia), è improbabile che ci sia più di un messaggio dotato di senso che possa essere il testo in chiaro. Se si hanno dei dubbi in proposito, si provi a trovare qualche coppia di parole di quattro o cinque lettere che siano ottenibili l'una dall'altra per scorrimento delle lettere (si veda l'Esercizio 1). Se il messaggio è sufficientemente lungo, un altro possibile attacco consiste nel contare la frequenza delle varie lettere. La lettera e è la più frequente nella maggioranza dei testi inglesi. Se la lettera L compare più di frequente nel testo cifrato, allora, essendo $e = 4$ e $L = 11$, una congettura ragionevole è $\kappa = 11 - 4 = 7$. Tuttavia, per i cifrari a scorrimento questo metodo richiede più tempo della ricerca esaustiva e inoltre per funzionare richiede molte più lettere nel messaggio (un testo breve, come quello considerato, potrebbe non contenere uno dei simboli più comuni, alterando così il conteggio statistico).

2. **Testo in chiaro noto.** Se si conosce una lettera del testo in chiaro con la corrispondente lettera nel testo cifrato, allora si può dedurre la chiave. Per esempio, se si sa che $t(= 19)$ viene cifrata in $D(= 3)$, allora la chiave è $\kappa \equiv 3 - 19 \equiv -16 \equiv 10 \pmod{26}$.

3. **Testo in chiaro scelto.** Scelta la lettera a come testo in chiaro, allora il testo cifrato fornisce la chiave. Per esempio, se il testo cifrato è H, allora la chiave è 7.

4. **Testo cifrato scelto.** Scelta la lettera A come testo cifrato, allora il testo in chiaro è l'opposto della chiave. Per esempio, se il testo in chiaro è h, la chiave è $-7 \equiv 19 \pmod{26}$.

2.2 Cifrari affini

I cifrari a scorrimento possono essere generalizzati e leggermente rafforzati nel modo seguente. Scelti due interi α e β, con $\text{MCD}(\alpha, 26) = 1$, si considera la *funzione affine*

$$x \mapsto \alpha x + \beta \pmod{26}.$$

Per esempio, se $\alpha = 9$ e $\beta = 2$, si ha $x \mapsto 9x + 2$. Presa la lettera $h(= 7)$ come testo in chiaro, essa viene cifrata in $9 \cdot 7 + 2 \equiv 65 \equiv 13 \pmod{26}$, ossia nella lettera N. Usando la stessa funzione, si ha

affine $\mapsto$ *CVVWPM.*

Come avviene la decifrazione? Se stessimo lavorando con i numeri razionali invece che con gli interi modulo 26, si potrebbe porre $y = 9x + 2$ e risolvere rispetto ad x, ottenendo $x = \frac{1}{9}(y - 2)$. A questo punto, però, visto che stiamo lavorando modulo 26, bisogna reinterpretare $\frac{1}{9}$. Poiché $\text{MCD}(9,26) = 1$, esiste un inverso moltiplicativo di 9 (mod 26) (se questo non è chiaro, si legga il Paragrafo 3.3). Infatti, essendo $9 \cdot 3 \equiv 1 \pmod{26}$, tale inverso è dato da 3, che può pertanto essere usato al posto di $\frac{1}{9}$. Quindi

$$x \equiv 3(y - 2) \equiv 3y - 6 \equiv 3y + 20 \pmod{26}.$$

Per esempio, la lettera $V(= 21)$ è mandata in $3 \cdot 21 + 20 \equiv 83 \equiv 5 \pmod{26}$, che corrisponde alla lettera f. Analogamente, il testo cifrato *CVVWPM* è decifrato in *affine*.
Se si considera la funzione $13x + 4$ come funzione di cifratura, allora si ha

input $\mapsto$ *ERRER* e *alter* $\mapsto$ *ERRER.*

Con questa funzione è impossibile decifrare i messaggi, poiché diversi testi in chiaro producono lo stesso testo cifrato. La procedura di cifratura deve essere iniettiva e questo non accade nel caso appena visto. Ma più precisamente, cosa va storto in questo esempio? Risolvendo $y = 13x + 4$, si ottiene $x = \frac{1}{13}(y - 4)$. Ma $\frac{1}{13}$ non esiste modulo 26 poiché $\text{MCD}(13, 26) = 13 \neq 1$. Più in generale, si può mostrare che $\alpha x + \beta$ è una funzione iniettiva modulo 26 se e solo se $\text{MCD}(\alpha, 26) = 1$. In questo caso, si ha $x \equiv \alpha^* y - \alpha^* \beta \pmod{26}$, dove $\alpha\alpha^* \equiv 1 \pmod{26}$. Pertanto, anche il processo di decifrazione è descritto da una funzione affine.

La chiave per questo metodo di cifratura è la coppia (α, β). Ci sono 12 scelte possibili per α con $\text{MCD}(\alpha, 26) = 1$ mentre ce ne sono 26 per β (poiché si lavora modulo 26, è sufficiente considerare α e β compresi tra 0 e 25). Quindi, in tutto, ci sono $12 \cdot 26 = 312$ scelte possibili per la chiave.
Vediamo i possibili attacchi.

1. **Solo testo cifrato.** Anche se una ricerca esaustiva tra tutte le 312 chiavi sarebbe più lunga della corrispondente ricerca nel caso del cifrario a scorrimento, essa potrebbe essere svolta molto semplicemente con un computer. Una volta che si sono provate tutte le possibilità per la chiave, un testo cifrato abbastanza breve, diciamo di circa 20 caratteri, probabilmente corrisponderà a un solo testo in chiaro dotato di significato, permettendo quindi la determinazione della chiave. Si può anche usare l'analisi delle frequenze, benché questo richieda testi molto più lunghi.

2. **Testo in chiaro noto.** Con un po' di fortuna, la conoscenza di due lettere del testo in chiaro e delle due corrispondenti lettere del testo cifrato è sufficiente per trovare la chiave. In ogni caso, il numero di possibilità per la chiave è ridotto di molto e qualche lettera in più potrebbe dare la chiave.

   Per esempio, se il testo in chiaro inizia con *if* e il corrispondente testo cifrato è *PQ*, allora questo significa che 8 $(= i)$ viene mandato in 15 $(= P)$ e 5 in 16. Quindi si hanno le equazioni

$$\begin{aligned} 8\alpha + \beta &\equiv 15 \pmod{26} \\ 5\alpha + \beta &\equiv 16 \pmod{26}. \end{aligned}$$

   Sottraendo si ha $3\alpha \equiv -1 \equiv 25 \pmod{26}$, che ammette l'unica soluzione $\alpha = 17$. Usando la prima equazione, si ottiene $8 \cdot 17 + \beta \equiv 15 \pmod{26}$ e quindi $\beta = 9$.

   Se invece il testo in chiaro *go* corrisponde al testo cifrato *TH*, si ottengono le equazioni

$$\begin{aligned} 6\alpha + \beta &\equiv 19 \pmod{26} \\ 14\alpha + \beta &\equiv 7 \pmod{26}. \end{aligned}$$

   Sottraendo si ha $-8\alpha \equiv 12 \pmod{26}$. Poiché $\text{MCD}(-8, 26) = 2$, si hanno due soluzioni: $\alpha = 5$ e $\alpha = 18$. I valori corrispondenti di β sono entrambi 15 (non è una coincidenza, è sempre così quando i coefficienti di α nelle equazioni sono pari). Pertanto si hanno due candidati per la chiave: $(5, 15)$ e $(18, 15)$. Tuttavia, essendo $\text{MCD}(18, 26) \neq 1$, il secondo è da scartare e quindi la chiave è $(5, 15)$.

   La precedente procedura funziona, a meno che il massimo comune divisore che si ottiene non sia 13 (o 26). In questo caso, se possibile, bisogna usare un'altra lettera del messaggio.

   Se si conosce solo una lettera del testo in chiaro, ancora si ottiene una relazione tra α e β. Per esempio, se si sa solo che g nel testo in chiaro corrisponde a T nel testo cifrato, allora si ha $6\alpha + \beta \equiv 19 \pmod{26}$. Ci sono 12 possibilità per α e ognuna di esse dà una corrispondente β. Quindi una ricerca esaustiva tra le 12 chiavi produce la chiave corretta.

3. **Testo in chiaro scelto.** Scelto ab come testo in chiaro, il primo carattere del testo cifrato sarà $\alpha \cdot 0 + \beta = \beta$ e il secondo sarà $\alpha + \beta$. Quindi si può trovare la chiave.

4. **Testo cifrato scelto.** Scelto AB come testo cifrato, si ottiene una funzione di decifrazione della forma $x = \alpha_1 y + \beta_1$. Si può risolvere rispetto a y e ottenere la chiave di cifratura. Ma questo non è importante, visto che si ha la funzione di decifrazione, che è ciò che si vuole.

2.3 Cifrario di Vigenère

Una variante dei cifrari a scorrimento, inventata nel sedicesimo secolo, viene spesso attribuita a Vigenère, benché i suoi metodi di cifratura fossero molto più sofisticati. Nel ventesimo secolo questo crittosistema fu ritenuto sicuro da molti, anche se Babbage e Kasiski avevano già mostrato come attaccarlo nel diciannovesimo secolo. Negli anni venti del secolo scorso, Friedman ha sviluppato ulteriori metodi per violare cifrari di questo tipo.
La chiave per la cifratura è un vettore, scelto nel modo seguente. Prima si sceglie la lunghezza della chiave, per esempio 6. Poi si sceglie un vettore di questa lunghezza le cui componenti sono interi compresi tra 0 e 25, per esempio $k = (21, 4, 2, 19, 14, 17)$. Spesso la chiave corrisponde a una parola facile da ricordare. Nel nostro caso, la parola è *vector*. La sicurezza del sistema dipende dal fatto che non sono note né la parola chiave né la sua lunghezza.
Per cifrare un messaggio usando la chiave k del nostro esempio, si prende prima la lettera del testo in chiaro e la si fa scorrere di 21 posizioni. Poi si fa scorrere la seconda lettera di 4, la terza di 2 e così via. Una volta che si arriva alla fine della chiave, si ricomincia da capo dalla sua prima componente, cosicché la settima lettera è fatta scorrere di 21 posizioni, l'ottava lettera di 4 e così via. Ecco un esempio di cifratura:

(testo in chiaro)	*h*	*e*	*r*	*e*	*i*	*s*	*h*	*o*	*w*	*i*	*t*	*w*	*o*	*r*	*k*	*s*
(chiave)	21	4	2	19	14	17	21	4	2	19	14	17	21	4	2	19
(testo cifrato)	*C*	*I*	*T*	*X*	*W*	*J*	*C*	*S*	*Y*	*B*	*H*	*N*	*J*	*V*	*M*	*L*

Un attacco di testo in chiaro noto ha successo se è noto un numero sufficiente di caratteri, poiché la chiave si ottiene semplicemente sottraendo il testo in chiaro al testo cifrato modulo 26. Un attacco di testo in chiaro scelto che usi il testo in chiaro $aaaaa\cdots$ dà immediatamente la chiave, mentre un attacco di testo cifrato scelto con $AAAAA\cdots$ dà l'opposto della chiave. Si supponga di avere solo il testo cifrato. Per molto tempo si è pensato che il metodo fosse sicuro contro un attacco di solo testo cifrato, ma anche in questo caso è facile trovare la chiave.
La crittanalisi sfrutta il fatto che nella maggior parte dei testi in lingua inglese le frequenze delle lettere non sono uguali. Per esempio, la lettera *e* si presenta molto più frequentemente della lettera x. Queste frequenze sono state tabulate in [Beker-Piper] e sono riportate nella Tabella 2.1.
Naturalmente, si possono avere delle variazioni, anche se di solito è necessario un notevole sforzo per ottenerle. Il libro *Gadsby* di Ernest Vincent Wright non contiene la lettera *e*. Ancora più incredibilmente, anche il libro *La Disparition* di George Perec,

a	b	c	d	e	f	g	h	i
0,082	0,015	0,028	0,043	0,127	0,022	0,020	0,061	0,070
j	k	l	m	n	o	p	q	r
0,002	0,008	0,040	0,024	0,067	0,075	0,019	0,001	0,060
s	t	u	v	w	x	y	z	
0,063	0,091	0,028	0,010	0,023	0,001	0,020	0,001	

Tabella 2.1 Frequenze delle lettere nella lingua inglese

scritto in francese, non contiene alcuna *e* (qui, oltre i problemi con i verbi e le parole in generale, devono essere evitati quasi tutti i nomi e gli aggettivi femminili). Esiste anche una traduzione inglese di Gilbert Adair, *A Void*, in cui non appare mai la lettera *e*. In generale, però, si può supporre che quanto riportato sopra dia una stima grossolana di ciò che accade normalmente nel caso in cui si abbia un testo formato da varie centinaia di caratteri.

Se si avesse un semplice cifrario a scorrimento, allora una qualunque lettera, per esempio *e*, apparirebbe sempre come la medesima lettera cifrata con la stessa frequenza con cui appare *e* nel testo originale. Di conseguenza un'analisi delle frequenze probabilmente rivelerebbe la chiave. Tuttavia, nel precedente esempio di cifrario di Vigenère, la lettera *e* appare sia come I che come X. Se si fosse usato un testo in chiaro più lungo, allora *e* sarebbe probabilmente stata cifrata come ognuna delle lettere Z, I, G, X, S, V, corrispondenti agli scorrimenti 21, 4, 2, 19, 14, 17. Ma le occorrenze di Z in un testo cifrato potrebbero derivare non soltanto da *e*. Anche la lettera v è cifrata come Z quando la sua posizione nel testo è tale da farla scorrere di 4. Analogamente, anche x, g, l, i possono aumentare la presenza della Z nel testo cifrato. Così la frequenza di Z è una combinazione delle frequenze delle lettere e, v, x, g, l, i provenienti dal testo in chiaro. Pertanto è molto più difficile dedurre qualcosa dal conteggio delle frequenze. Infatti, in genere le frequenze si appiattiscono avvicinandosi a $1/26$ per ognuna delle lettere del testo cifrato. Quanto meno, esse dovrebbero avvicinarsi molto di più a questo valore rispetto alla distribuzione originale delle lettere inglesi.

Ecco ora un esempio un po' più sostanzioso. Per il testo cifrato

```
VVHQWVVRHMUSGJGTHKIHTSSEJCHLSFCBGVWCRLRYQTFSVGAHW
KCUHWAUGLQHNSLRLJSHBLTSPISPRDXLJSVEEGHLQWKASSKUWE
PWQTWVSPGOELKCQYFNSVWLJSNIQKGNRGYBWLWGOVIOKHKAZKQ
KXZGYHCECMEIUJOQKWFWVEFQHKIJRCLRLKBIENQFRJLJSDHGR
HLSFQTWLAUQRHWDMWLGUSGIKKFLRYVCWVSPGPMLKASSJVOQXE
GGVEYGGZMLJCXXLJSVPAIVWIKVRDRYGFRJLJSLVEGGVEYGGEI
APUUISFPBTGNWWMUCZRVTWGLRWUGUMNCZVILE
```

le frequenze sono

A	B	C	D	E	F	G	H	I	J	K	L	M
8	5	12	4	15	10	27	16	13	14	17	25	7
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	5	9	14	17	24	8	12	22	22	5	8	5

Non ci sono lettere la cui frequenza è significativamente maggiore di quella delle altre. Come osservato in precedenza, questo deriva dal fatto che ogni lettera proviene da più lettere durante il processo di cifratura.

Come si decifra il messaggio? Ci sono due cose da fare: trovare la lunghezza della chiave e trovare la chiave. In quello che segue, prima si mostrerà come trovare la lunghezza della chiave e poi verrà dato un modo per trovare la chiave stessa. Dopo aver spiegato perché il metodo per trovare la chiave funziona, verrà descritto un secondo modo per trovare la chiave.

2.3.1 Come trovare la lunghezza della chiave

Si scrive il testo cifrato su una striscia lunga di carta e si ripete la medesima operazione su una seconda striscia lunga di carta. Si colloca una striscia appena sopra l'altra, ma spostata di un certo numero di posizioni (la potenziale lunghezza della chiave). Per esempio, per uno spostamento di 2 posizioni si ha

```
      V V H Q W V V R H M U S G J G T H
V V H Q W V V R H M U S G J G T H
                              *

T H K I H T S S E J C H L S F C B G V
K I H T S S E J C H L S F C B G V

G V W C R L R Y Q T F S V G A H W K ...
W C R L R Y Q T F S V G A H W K ...
      *
```

Si segna uno $*$ ogni volta che una lettera sulla prima striscia è uguale a quella sottostante sulla seconda striscia e si conta il numero totale delle corrispondenze. Nella parte di testo riportato qui sopra si hanno due corrispondenze. Se si continua per l'intero testo cifrato, se ne contano 14. Se si ripete questa operazione per spostamenti successivi, si ottengono i seguenti dati

spostamenti:	1	2	3	4	5	6
corrispondenze:	14	14	16	14	24	12

Il numero maggiore di corrispondenze si ha per uno spostamento di 5 posizioni. Come verrà spiegato più avanti, questa è la migliore ipotesi per la lunghezza della chiave. Questo metodo è molto rapido, anche senza un computer, e di solito fornisce la lunghezza della chiave.

2.3.2 Come trovare la chiave: primo metodo

Se si è trovato che la lunghezza della chiave è 5, come nel nostro esempio, si va a vedere quale lettera appare più di frequente nella 1ª, 6ª, 11ª, ... posizione. Nel nostro esempio si ha

A	B	C	D	E	F	G	H	I	J	K	L	M
0	0	7	1	1	2	9	0	1	8	8	0	0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	0	4	5	2	0	3	6	5	1	0	1	0

La lettera più frequente è G, anche se J, K e C le sono molto vicine. Tuttavia, $J = e$ significherebbe uno spostamento di 5 e quindi $C = x$. Questo porterebbe a una frequenza insolitamente elevata per x nel testo cifrato. Analogamente, $K = e$ significherebbe $P = j$ e $Q = k$ ed entrambe le lettere avrebbero una frequenza troppo elevata. Infine, $C = e$ richiederebbe $V = x$, che è improbabile. Pertanto, si decide che $G = e$ e che il primo elemento della chiave sia $2 = c$.
Andando a vedere la 2ª, 7ª, 12ª, ... posizione, si trova che G appare 10 volte e S appare 12 volte, mentre le altre lettere appaiono un numero decisamente inferiore di volte. Se $G = e$, allora $S = q$, che non dovrebbe apparire ben 12 volte nel testo in chiaro. Quindi $S = e$ e il secondo elemento della chiave è $14 = o$.
Andando a vedere la 3ª, 8ª, 13ª, ... posizione, si ottengono le frequenze

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	0	3	3	1	3	5	1	0	4	10	0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	1	2	3	5	3	0	2	8	7	1	0	1

Se fosse $L = e$, allora si avrebbero dei problemi. Per esempio, $R = k$ e $E = x$ avrebbero una frequenza troppo elevata e $A = t$ avrebbe una frequenza troppo bassa. Analogamente, $V = e$ e $W = e$ sono poco probabili. La scelta migliore è $H = e$ e quindi il terzo elemento della chiave è $3 = d$.
La 4ª, 9ª, 14ª, ... posizione portano ad avere $4 = e$ come quarto elemento della chiave. E infine la 5ª, 10ª, 15ª, ... posizione portano ad avere $18 = s$ come ultimo elemento della chiave. La nostra ipotesi per la chiave è pertanto

$$\{2,14,3,4,18\} = \{c,o,d,e,s\}.$$

Come visto nel caso della 3ª, 8ª, 13ª, ... lettera (questo accade anche nella 5ª, 10ª, 15ª, ... posizione), se si prende una lettera ogni cinque si ha un campione di lettere molto più piccolo su cui eseguire il conteggio delle frequenze. In un campione piccolo la lettera più frequente potrebbe non essere la e. Ma è comunque probabile che le lettere con frequenza alta appaiano spesso e che quelle con frequenza bassa appaiano di rado. Come nel caso presente, questo è di solito sufficiente per identificare la corrispondente componente della chiave.
Una volta che si è trovata una chiave potenziale, la si testa usandola per decifrare. Dovrebbe essere facile stabilire se è corretta.

Nel nostro esempio, la chiave ipotizzata è (2,14,3,4,18). Se si decifra il testo cifrato usando questa chiave, si ottiene

```
themethodusedforthepreparationandreadingofcodemessagesis
simpleintheextremeandatthesametimeimpossibleoftranslatio
nunlessthekeyisknowntheeasewithwhichthekeymaybechangedis
anotherpointinfavoroftheadoptionofthiscodebythosedesirin
gtotransmitimportantmessageswithouttheslightestdangeroft
heirmessagesbeingreadbypoliticalorbusinessrivalsetc
```

Questo passo è tratto da un breve articolo apparso su *Scientific American, Supplement* LXXXIII (27/1/1917), pagina 61. In questo articolo si da una breve spiegazione del cifrario di Vigenère e nel passo in questione viene espressa un'opinione sulla sua sicurezza.

Prima di passare al secondo metodo per trovare la chiave, verrà data una spiegazione del perché la procedura appena vista trova la lunghezza della chiave. Per evitare confusione, quando si usa la parola "scorrimento" per una lettera, ci si riferisce a ciò che accade durante il processo di cifratura di Vigenère. Quando, invece, quando muoviamo una striscia di carta a destra o a sinistra rispetto all'altra, usiamo la parola "spostamento". Si dispongano le frequenze delle lettere inglesi in un vettore:

$$\mathbf{A}_0 = (0{,}082, 0{,}015, 0{,}028, \ldots, 0{,}020, 0{,}001).$$

Sia $\mathbf{A}_i$ il vettore che si ottiene facendo scorrere $\mathbf{A}_0$ di i posizioni verso destra. Per esempio,

$$\mathbf{A}_2 = (0{,}020, 0{,}001, 0{,}082, 0{,}015, \ldots).$$

Il prodotto scalare di $\mathbf{A}_0$ con se stesso è

$$\mathbf{A}_0 \cdot \mathbf{A}_0 = (0{,}082)^2 + (0{,}015)^2 + \cdots = 0{,}066.$$

Naturalmente, anche $\mathbf{A}_i \cdot \mathbf{A}_i$ è uguale a 0,066 poiché si ha la stessa somma di prodotti, a partire da un termine diverso. Tuttavia, i prodotti scalari $\mathbf{A}_i \cdot \mathbf{A}_j$ sono molto inferiori quando $i \neq j$, assumendo valori da 0,031 a 0,045:

$\lvert i-j \rvert$	0	1	2	3	4	5	6
$\mathbf{A}_i \cdot \mathbf{A}_j$	0,066	0,039	0,032	0,034	0,044	0,033	0,036

$\lvert i-j \rvert$	7	8	9	10	11	12	13
$\mathbf{A}_i \cdot \mathbf{A}_j$	0,039	0,034	0,034	0,038	0,045	0,039	0,042

Il prodotto scalare dipende solo da $|i-j|$. Le componenti dei vettori $\mathbf{A}_i$ sono le stesse di quelle di $\mathbf{A}_0$, ma fatte scorrere. Nel prodotto scalare $\mathbf{A}_i \cdot \mathbf{A}_j$, la componente i-esima di $\mathbf{A}_0$ è moltiplicata per la componente j-esima, la componente $(i+1)$-esima per la componente $(j+1)$-esima e così via. Ogni elemento è pertanto moltiplicato per l'elemento spostato di $j-i$ posizioni da esso. Quindi il prodotto scalare dipende solo dalle differenze $i-j$. Tuttavia, invertendo i ruoli di i e j e osservando che $\mathbf{A}_i \cdot \mathbf{A}_j = \mathbf{A}_j \cdot \mathbf{A}_i$, si ha che $i-j$ e $j-i$ danno gli stessi prodotti scalari e quindi il

prodotto scalare dipende solo da $|i-j|$. Nella tabella precedente, è stato sufficiente calcolare i prodotti solo fino a $|i-j|=13$. Per esempio, poiché $i-j=17$ corrisponde a uno scorrimento di 17 posizioni in una direzione o equivalentemente a uno scorrimento di 9 posizioni nella direzione opposta, si ha che $i-j=9$ dà lo stesso prodotto scalare. La ragione per cui $\mathbf{A}_0 \cdot \mathbf{A}_0$ è maggiore degli altri prodotti scalari è che i numeri grandi sono accoppiati con numeri grandi e quelli piccoli sono accoppiati con numeri piccoli. Negli altri prodotti scalari, i numeri grandi sono accoppiati un po' a caso con gli altri numeri, diminuendo il loro effetto. Per un'altra motivazione per cui $\mathbf{A}_0 \cdot \mathbf{A}_0$ risulta maggiore degli altri prodotti scalari, si veda l'Esercizio 9.

Supponiamo che la distribuzione delle lettere nel testo in chiaro sia simile a quella dell'inglese, espressa dal vettore $\mathbf{A}_0$ precedente. Si consideri a caso una lettera nella striscia superiore del testo cifrato. Essa corrisponde a una lettera casuale dell'inglese fatta scorrere di una certa quantità i (corrispondente a un elemento della chiave). La lettera sotto di essa corrisponde a una lettera casuale dell'inglese fatta scorrere di una certa quantità j.

Per esempio, se $i=0$ e $j=2$, la probabilità che la lettera che compare nella cinquantesima posizione sia A è data dalla prima componente di $\mathbf{A}_0$, ossia 0,082. La lettera direttamente sotto, sulla seconda striscia, è stata fatta scorrere dal testo in chiaro originale di $j=2$ posizioni. Se questa lettera di testo cifrato è A, allora la corrispondente lettera di testo in chiaro era y, che compare nel testo in chiaro con probabilità 0,020. Si noti che 0,020 è la prima componente del vettore $\mathbf{A}_2$. La probabilità che la lettera nella cinquantesima posizione sulla prima striscia e la lettera direttamente sotto siano entrambe la lettera A è $0{,}082 \cdot 0{,}020$. Analogamente, la probabilità che entrambe le lettere siano B è $0{,}015 \cdot 0{,}001$. Continuando in questo modo fino a Z, si ha che la probabilità che le due lettere siano uguali è

$$0{,}082 \cdot 0{,}020 + 0{,}015 \cdot 0{,}001 + \cdots + 0{,}001 \cdot 0{,}001 = \mathbf{A}_0 \cdot \mathbf{A}_2.$$

In generale, quando gli scorrimenti di cifratura sono i e j, la probabilità che le due lettere siano uguali è $\mathbf{A}_i \cdot \mathbf{A}_j$. Quando $i \neq j$, questo prodotto è circa 0,038, ma se $i=j$ allora è 0,066.

Si è nel caso in cui $i=j$ esattamente quando le lettere che stanno una sopra l'altra sono state fatte scorrere della stessa quantità durante il processo di cifratura, ossia quando la striscia superiore è spostata di una quantità uguale alla lunghezza della chiave (o un multiplo della lunghezza della chiave). Quindi, in questo caso, ci si aspetta un numero maggiore di coincidenze.

Per uno spostamento di 5 posizioni nel precedente testo cifrato, ci sono 326 confronti e 24 corrispondenze. Per il ragionamento precedente, ci si dovrebbe aspettare circa $326 \cdot 0.066 = 21{,}5$ corrispondenze, che è vicino al valore effettivo.

2.3.3 Come trovare la chiave: secondo metodo

Usando le idee precedenti, è possibile ottenere un secondo metodo per determinare la chiave, che sembra funzionare un po' meglio su campioni piccoli, anche se richiede qualche calcolo in più.

Si consideri ancora il precedente esempio. Per trovare il primo elemento della chiave, si contano le occorrenze delle lettere che si trovano in 1ª, 6ª, 11ª, ... posizione, come

prima, e poi le si dispongono in un vettore:

$$\mathbf{V} = (0,0,7,1,1,2,9,0,1,8,8,0,0,3,0,4,5,2,0,3,6,5,1,0,1,0)$$

(la prima componente è il numero delle occorrenze di A, la seconda è il numero di occorrenze di B e così via). Se si divide per 67, ossia per il numero totale delle lettere contate, si ottiene il vettore

$$\mathbf{W} = (0,0,0{,}1045,0{,}0149,0{,}0149,0{,}0299,\ldots,0{,}0149,0).$$

Si pensi un attimo a come è costruito questo vettore. Poiché si sa che la lunghezza della chiave è 5, le lettere che si trovano in 1ª, 6ª, 11ª, ... posizione all'interno del testo cifrato sono state fatte scorrere tutte della stessa quantità, pari a 2, come si vedrà a breve. Quindi rappresentano un campione casuale di lettere inglesi, tutte fatte scorrere della stessa quantità. Le loro frequenze, date dal vettore $\mathbf{W}$, dovrebbero approssimare il vettore $\mathbf{A}_i$, dove i è lo scorrimento indotto dal primo elemento della chiave.

Il problema ora è determinare i. Si ricordi che $\mathbf{A}_i \cdot \mathbf{A}_j$ è maggiore quando $i=j$ e che $\mathbf{W}$ approssima $\mathbf{A}_i$. Se si calcolano i prodotti scalari $\mathbf{W} \cdot \mathbf{A}_j$ per $0 \leq j \leq 25$, il valore massimo dovrebbe presentarsi per $j=i$. Nel nostro caso i prodotti scalari sono

$$0{,}0250,\ 0{,}0391,\ 0{,}0713,\ 0{,}0388,\ 0{,}0275,\ 0{,}0380,\ 0{,}0512,\ 0{,}0301,\ 0{,}0325,$$
$$0{,}0430,\ 0{,}0338,\ 0{,}0299,\ 0{,}0343,\ 0{,}0446,\ 0{,}0356,\ 0{,}0402,\ 0{,}0434,\ 0{,}0502,$$
$$0{,}0392,\ 0{,}0296,\ 0{,}0326,\ 0{,}0392,\ 0{,}0366,\ 0{,}0316,\ 0{,}0488,\ 0{,}0349$$

Il valore più grande è il terzo, ossia 0,0713, e corrisponde a $\mathbf{W} \cdot \mathbf{A}_2$. Di conseguenza possiamo ipotizzare che il primo scorrimento sia di 2 posizioni. Esso corrisponde alla lettera chiave *c*.

Si può usare lo stesso metodo per trovare il terzo elemento della chiave. Si calcola un nuovo vettore $\mathbf{W}$, usando le frequenze per le lettere che compaiono in 3ª, 8ª, 13ª, ... posizione, che sono state tabulate in precedenza:

$$\mathbf{W} = (0,0{,}0152,0,0{,}0454,0{,}0454,0{,}0152,\ \ldots,0,0{,}0152).$$

I prodotti scalari $\mathbf{W} \cdot \mathbf{A}_i$ per $0 \leq i \leq 25$ sono

$$0{,}0372,\ 0{,}0267,\ 0{,}0395,\ 0{,}0624,\ 0{,}04741,\ 0{,}0279,\ 0{,}0319,\ 0{,}0504,\ 0{,}0378,$$
$$0{,}0351,\ 0{,}0367,\ 0{,}0395,\ 0{,}0264,\ 0{,}0415,\ 0{,}0427,\ 0{,}0362,\ 0{,}0322,\ 0{,}0457,$$
$$0{,}0526,\ 0{,}0397,\ 0{,}0322,\ 0{,}0299,\ 0{,}0364,\ 0{,}0372,\ 0{,}0352,\ 0{,}0406$$

Il maggiore di questi valori è il quarto, ossia 0,0624, e corrisponde a $\mathbf{W} \cdot \mathbf{A}_3$. Pertanto la migliore ipotesi è che il primo scorrimento sia 3. Esso corrisponde alla lettera chiave *d*. Gli altri tre elementi della chiave possono essere trovati in modo simile e ancora si ottiene *c, o, d, e, s* come chiave.

In entrambi i casi il prodotto scalare più grande è significativamente maggiore degli altri. Ciò ha permesso di trovare il valore corretto senza dover fare troppi tentativi. Pertanto questo secondo metodo è superiore al primo, anche se il primo metodo è molto più semplice da eseguire a mano.

Perché questo secondo metodo è più accurato del primo? Per ottenere il prodotto scalare maggiore, molti dei valori più grandi in $\mathbf{W}$ devono coincidere con i valori più grandi in $\mathbf{A}_i$. Nel primo metodo, si era tentato di far corrispondere solo la e e poi si era andati a vedere se le scelte per le altre lettere erano ragionevoli. Il presente metodo fa tutto questo in un passo solo.
In conclusione, ecco il metodo per trovare la chiave. Supponendo di aver già determinato la lunghezza n della chiave, si procede, per $i = 1, \ldots, n$, nel modo seguente.

1. Si calcolano le frequenze delle lettere nelle posizioni i modulo n e si costruisce il vettore $\mathbf{W}$.
2. Per ogni $j = 0, \ldots, 25$, si calcola $\mathbf{W} \cdot \mathbf{A}_j$.
3. Si pone $k_i = j_0$ per il valore massimo di $\mathbf{W} \cdot \mathbf{A}_j$.

La chiave è probabilmente $\{k_1, \ldots, k_n\}$.

2.4 Cifrari a sostituzione

Uno dei crittosistemi più popolari è il cifrario a sostituzione. Il principio è semplice: ogni lettera dell'alfabeto viene sostituita con un'altra lettera (anche la stessa). Più precisamente, si sceglie una permutazione dell'alfabeto e la si applica al testo in chiaro. I cifrari a scorrimento e i cifrari affini sono entrambi esempi di cifrari a sostituzione. Invece i cifrari di Vigenère e di Hill (si vedano i Paragrafi 2.3 e 2.7) non lo sono, poiché essi permutano blocchi di lettere e non semplicemente una lettera alla volta.
Tutti "sanno" che i cifrari a sostituzione possono essere violati mediante un'analisi delle frequenze. Tuttavia, il processo è molto più complicato di quanto ci si possa aspettare.
Si consideri il seguente esempio. Thomas Jefferson ha un messaggio potenzialmente sedizioso che vuole inviare a Ben Franklin. Poiché chiaramente non vuole che gli Inglesi siano in grado di leggerne il testo qualora lo intercettassero, lo cifra usando un cifrario a sostituzione. Fortunatamente, Ben Franklin conosce la permutazione che è stata usata e quindi può ottenere il messaggio originale semplicemente invertendo tale permutazione (naturalmente, Franklin era molto intelligente e forse sarebbe riuscito a decifrare il messaggio anche senza conoscere la chiave).
Ora facciamo finta di lavorare per la Government Code and Cypher School nell'Inghilterra del 1776 e che, dopo essere stato intercettato, ci venga dato il seguente messaggio da decifrare.

```
LWNSOZBNWVWBAYBNVBSQWVWOHWDIZWRBBNPBPOOUWRPAWXAW
PBWZWMYPOBNPBBNWJPAWWRZSLWZQJBNWIAXAWPBSALIBNXWA
BPIRYRPOIWRPQOWAIENBVBNPBPUSREBNWVWPAWOIHWOIQWAB
JPRZBNWFYAVYIBSHNPFFIRWVVBNPBBSVWXYAWBNWVWAIENBV
ESDWARUWRBVPAWIRVBIBYBWZPUSREUWRZWAIDIREBNWIATYV
BFSLWAVHASUBNWXSRVWRBSHBNWESDWARWZBNPBLNWRWDWAPR
JHSAUSHESDWARUWRBQWXSUWVZWVBAYXBIDWSHBNWVWWRZVIB
IVBNWAIENBSHBNWFWSFOWBSPOBWASABSPQSOIVNIBPRZBSIR
VBIBYBWRWLESDWARUWRBOPJIREIBVHSYRZPBISRSRVYXNFAI
RXIFOWVPRZSAEPRIKIREIBVFSLWAVIRVYXNHSAUPVBSVWWUU
SVBOICWOJBSWHHWXBBNWIAVPHWBJPRZNPFFIRWVV
```

In questo testo ci sono 520 lettere. Dall'analisi delle frequenze si ha

W	B	R	S	I	V	A	P	N	O	...
76	64	39	36	36	35	34	32	30	16	...

Le frequenze appropriate delle lettere in inglese sono state date nel Paragrafo 2.3. Ne riportiamo alcune nella Tabella 2.2.

e	t	a	o	i	n	s	h	r
0,127	0,091	0,082	0,075	0,070	0,067	0,063	0,061	0,060

Tabella 2.2 Frequenze delle lettere più comuni in inglese

Questo permette di ipotizzare con ragionevole fiducia che W corrisponde a e (benché B sia un'altra possibilità). Ma cosa si può dire delle altre lettere? Si può ipotizzare che le lettere B, R, S, I, V, A, P, N, con magari un'eccezione o due, coincidano probabilmente, a meno dell'ordine, con le lettere t, a, o, i, n, s, h, r. Ma un semplice conteggio delle frequenze non è sufficiente per determinare la giusta corrispondenza. Ciò che bisogna fare ora è dare un'occhiata ai digrammi, o coppie di lettere. Si dispongono i risultati come nella Tabella 2.3 (qui si considerano solo le lettere più frequenti, anche se sarebbe meglio metterle tutte). L'elemento 1 sulla riga W e sulla colonna N dice che la combinazione WN appare 1 volta nel testo. L'elemento 14 sulla riga N e sulla colonna W dice che NW appare 14 volte.

	W	B	R	S	I	V	A	P	N
W	3	4	12	2	4	10	14	3	1
B	4	4	0	11	5	5	2	4	20
R	5	5	0	1	1	5	0	3	0
S	1	0	5	0	1	3	5	2	0
I	1	8	10	1	0	2	3	0	0
V	8	10	0	0	2	2	0	3	1
A	7	3	4	2	5	4	0	1	0
P	0	8	6	0	1	1	4	0	0
N	14	3	0	1	1	1	0	7	0

Tabella 2.3 Conteggio dei digrammi.

Si è già deciso che $W = e$. Tuttavia, se avessimo esteso la tavola in modo da includere anche le lettere con frequenza bassa, si sarebbe visto che W è accostata anche a molte di queste lettere, esattamente come accade a e. Questo rafforza la congettura fatta. Le vocali a, i, o tendono a evitarsi. Se si guarda la riga R, si vede che R non precede S, I, A, N molto spesso. Ma uno sguardo alla colonna R mostra che R segue S, I, A piuttosto spesso. Questo porta a pensare che R non sia nessuna delle vocali a, i, o. V e N sono da escludere poiché è improbabile che una delle vocali a, i, o preceda $W = e$ molto spesso. Continuando in questo modo, si vede che più verosimilmente a, i, o sono S, I, P in qualche ordine.

La lettera n ha la proprietà che circa l'80% delle lettere che la precedono sono vocali. Poiché ormai W, S, I, P sono state identificate con delle vocali, R e A risultano essere i candidati più probabili. Tuttavia, bisogna aspettare un attimo prima di decidere qual è quello giusto.
Poiché la lettera h appare spesso prima di e e raramente dopo di essa, si ha $N = h$.
Poiché il digramma più comune è th, si ha $B = t$.
Tra le lettere frequenti, restano r e s e dovrebbero essere V e una delle lettere A o R.
Poiché r si accompagna maggiormente con le vocali e s si accompagna maggiormente con le consonanti, si ha che s è rappresentata da V mentre r è rappresentata da A o R.
La combinazione rn dovrebbe apparire più volte della combinazione nr. Quindi, poiché AR è più frequente di RA, si può ipotizzare che $A = r$ e $R = n$.
Continuando questa analisi si arriva a determinare che $S = o$ (to è molto più comune di ot), $I = i$ e $P = a$ sono le scelte più verosimili. Si è così ottenuta una ragionevole congettura per 382 dei 520 caratteri del testo:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y	B	N	V	B	S
	e	h	o			t	h	e	s	e	t	r		t	h	s	t	o

Q	W	V	W	O	H	W	D	I	Z	W	R	B	B	N	P	B	P	···
	e	s	e			e		i		e	n	t	t	h	a	t	a	···

A questo punto, le lettere rimanenti possono essere inserite usando la conoscenza della lingua, le frequenze medie (l, d, ...) e procedendo per tentativi. Per esempio, nella prima riga una buona congettura è $Y = u$ poiché in questo modo si ha la parola *truths*. Naturalmente, bisogna fare molti tentativi e bisogna provare molte ipotesi finché non si trova quella giusta.
Poiché la discussione precedente voleva semplicemente mostrare lo spirito del metodo, i rimanenti dettagli verranno tralasciati. Il messaggio decifrato, con gli spazi (ma senza la punteggiatura), è il seguente testo tratto dalla Dichiarazione di Indipendenza:

> *we hold these truths to be self evident that all men are created equal that they are endowed by their creator with certain unalienable rights that among these are life liberty and the pursuit of happiness that to secure these rights governments are instituted among men deriving their just powers from the consent of the governed that whenever any form of government becomes destructive of these ends it is the right of the people to alter or to abolish it and to institute new government laying its foundation on such principles and organizing its powers in such form as to seem most likely to effect their safety and happiness*

2.5 Sherlock Holmes

La crittografia è apparsa più volte nella letteratura. Per esempio, compare nelle opere di Edgar Allan Poe (*Lo scarabeo d'oro*), William Thackeray (*La storia di Henry Esmond*), Jules Verne (*Viaggio al centro della Terra*) e Agatha Christie (*I quattro indiziati* nella raccolta *Miss Marple e i tredici problemi*).

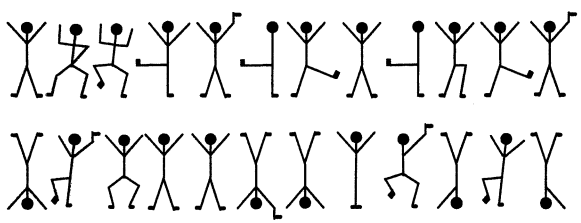
Qui di seguito riassumeremo *I pupazzi ballerini*, una delle tredici storie del ciclo *Il ritorno di Sherlock Holmes*, un breve racconto di Arthur Conan Doyle nel quale Sherlock Holmes usa la sua famosa intelligenza per violare un sistema cifrato. Poiché non riusciremo a rendere giustizia alla storia, invitiamo il lettore a leggere il racconto nella sua interezza.
Mr. Hilton Cubitt, che di recente ha sposato Elsie Patrick, spedisce una lettera a Sherlock Holmes. Si tratta di un pezzo di carta con raffigurati degli omini danzanti che ha trovato nel suo giardino a Riding Thorpe Manor:

Due settimane dopo, Cubitt trova un'altra serie di omini disegnati col gesso sulla porta del suo capanno degli attrezzi:

Due mattine più tardi appare il disegno

e tre giorni dopo appare il messaggio:

Cubitt porta una copia di tutti questi disegni a Holmes, il quale passa i due giorni successivi a fare una gran quantità di calcoli. All'improvviso, Holmes fa un salto sulla sedia su cui era seduto, colto da un'illuminazione. Senza perdere un solo istante invia un lungo telegramma e poi si mette ad aspettare, dicendo a Watson che probabilmente andranno a far visita a Cubitt il giorno seguente. Passano due giorni senza che il telegramma riceva risposta alcuna. Alla fine arriva una lettera di Cubitt con un'altro messaggio:



Holmes lo studia e poi, preoccupato, dice che devono recarsi a Riding Thorpe Manor il più presto possibile. Poco dopo, arriva anche la risposta al telegramma. Holmes la legge e dice che la faccenda si è fatta ancora più urgente. Il giorno dopo, quando Holmes e Watson arrivano a casa di Cubitt, vi trovano la polizia. Cubitt è morto, qualcuno gli ha sparato. Hanno sparato anche a Elsie, sua moglie, che ora si trova in condizioni critiche (anche se si salverà). Holmes fa un mucchio di domande e poi chiede che venga portato un biglietto a un certo Mr. Abe Slaney presso la vicina Elrige's Farm. A questo punto Holmes spiega a Watson e alla polizia come ha decifrato i messaggi. Come prima cosa, aveva supposto che le bandierine che alcuni degli omini tenevano in mano servissero a indicare la fine delle parole. Poi aveva notato che la figura più comune era

e quindi aveva supposto che fosse la *E*. In questo modo, il quarto messaggio diventava *–E–E–* e poteva quindi essere *LEVER, NEVER, SEVER*. Ma visto che il messaggio era con molta probabilità la risposta di una sola parola a un messaggio precedente, aveva scelto *NEVER*. Poi aveva osservato che

aveva la forma *E– – –E* e che poteva essere *ELSIE*. Il terzo messaggio era quindi *– – –E ELSIE*. Aveva fatto vari tentativi e alla fine era giunto alla conclusione che *COME ELSIE* fosse l'unica soluzione sensata. A quel punto il primo messaggio era *–M –ERE – –E SL–NE–*. Aveva supposto che la prima lettera fosse *A* e che la terza lettera fosse *H*, in modo da avere il messaggio *AM HERE A–E SLANE–* che poteva essere ragionevolmente completato in *AM HERE ABE SLANEY*. Allora il secondo messaggio era *A– ELRI–ES*. Naturalmente, aveva intuito che questo messaggio indicava il luogo in cui si trovava Slaney. L'unico modo ragionevole di completare la frase sembrava portare a *AT ELRIGES*. Dopo aver decifrato questi due messaggi, aveva inviato un telegramma a un suo amico del Police Bureau di New York, che aveva risposto dicendo che Abe Slaney era "il più pericoloso truffatore di Chicago". Infine, aveva decifrato l'ultimo messaggio di Cubitt come *ELSIE –RE–ARE TO MEET THY GO–*. Immaginato che *P, P, D* fossero le rispettive lettere mancanti, si era reso conto che la faccenda era molto seria e per questo motivo si era deciso a partire immediatamente per Riding Thorpe Manor.

Non appena Holmes finisce la sua spiegazione, la polizia vorrebbe precipitarsi a Elrige ad arrestare Slaney. Holmes tuttavia dice che non è necessario perché Slaney sta per arrivare. E così, quando effettivamente poco dopo Slaney si presenta, in men che non si dica si ritrova ammanettato dalla polizia. Aspettando di essere portato via, confessa di aver sparato (dice per una sorta di autodifesa) e rivela che quella scrittura era stata inventata dal padre di Elsie Patrick a uso della sua banda, il Joint, a Chicago. Slaney era fidanzato con Elsie e doveva sposarla quando lei, per scappare dal mondo dei gangster, era fuggita a Londra. Alla fine Slaney era riuscito a rintracciarla e aveva

spedito i messaggi segreti. Ma perché Slaney era caduto nella trappola che gli era stata tesa da Holmes? Holmes mostra il messaggio che aveva scritto:

Utilizzando le lettere che aveva decifrato, aveva composto un messaggio che diceva *COME HERE AT ONCE*. Slaney era sicuro che quel messaggio provenisse da Elsie poiché era convinto che nessuno che non facesse parte del Joint fosse in grado di scrivere messaggi di quel tipo. Così si era precipitato all'incontro che lo aveva portato alla cattura.

Commenti

Ciò che Holmes ha fatto è stato risolvere un semplice cifrario a sostituzione, benché lo abbia fatto con davvero pochi elementi. Come con la maggior parte di questi cifrari, sia l'analisi delle frequenze sia la conoscenza della lingua risultano molto utili. Anche un po' di fortuna aiuta, sia nella forma di congetture azzeccate sia nella distribuzione delle lettere. Ineluttabilmente la *E* è risultata la lettera più frequente. Infatti, essa compare 11 volte tra i 38 caratteri del primo dei quattro messaggi. Questo è stato per Holmes un buon inizio. Se Elsie si fosse chiamata Carol e Abe Slaney si fosse chiamato John Smith, la decifrazione probabilmente sarebbe stata più difficile.

L'autenticazione è molto importante nella crittografia. Se Eva viola il crittosistema di Alice, allora può farsi passare per Alice nelle comunicazioni con Bob. Difendersi da cose del genere è importante. Il giudice diede ad Abe Slaney parecchi anni per riflettere su questo punto.

Il lettore attento avrà notato che abbiamo un po' imbrogliato nel decifrare i messaggi. Lo stesso simbolo rappresenta la *V* in *NEVER* e le *P* in *PREPARE*. Questo è presumibilmente dovuto a un errore di stampa che è apparso in ogni versione stampata del racconto a partire dalla prima pubblicazione nel 1903. Nel testo originale, la *R* in *NEVER* è scritta come la *B* in *ABE*. Questo errore è stato corretto nelle edizioni successive, anche se, in alcune di esse, la prima *C* del messaggio scritto da Holmes ha un braccio in più che la fa assomigliare alla *M*. Se questi errori fossero stati presenti nei testi con cui stava lavorando, Holmes avrebbe incontrato molte più difficoltà nel decifrarli e avrebbe giustamente concluso che il Joint aveva bisogno di usare delle tecniche di correzione degli errori nelle sue trasmissioni. Infatti, un qualche tipo di correzione degli errori dovrebbe essere usato con quasi ogni protocollo crittografico.

2.6 I cifrari Playfair e ADFGX

I cifrari Playfair e ADFGX furono usati nella prima guerra mondiale rispettivamente dagli Inglesi e dai Tedeschi. Per gli standard moderni essi sono sistemi piuttosto deboli, anche se a quei tempi la loro violazione ha richiesto un notevole sforzo.

Il sistema Playfair fu inventato nel 1854 circa da Sir Charles Wheatstone, che gli diede questo nome in onore del suo amico, il Barone Playfair di St. Andrews, che era riuscito

1 blocchi 2 lettere

a convincere il governo a usarlo. Oltre che nella prima guerra mondiale, fu usato dalle forze britanniche anche nella guerra boera.
La chiave è una parola, per esempio *playfair*. Le lettere ripetute sono eliminate, ottenendo *playfir* e le lettere rimanenti sono usate come inizio di una matrice 5×5. Gli spazi restanti nella matrice sono riempiti con le rimanenti lettere dell'alfabeto, trattando i e j come una sola lettera:

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

Si supponga che il testo in chiaro sia *meet at the schoolhouse*. Si rimuovono gli spazi e si divide il testo in gruppi di due lettere. Se c'è una lettera doppia che appare come uno dei gruppi, si inserisce una x e si raggruppa di nuovo. Se necessario, si aggiunge un'ulteriore x alla fine per completare l'ultimo gruppo. Il nostro testo in chiaro diventa

me et at th es ch ox ol ho us ex.

Ora si usa la matrice per cifrare ogni gruppo di due lettere secondo il seguente schema.

- Se le due lettere non sono sulla stessa riga o sulla stessa colonna, si sostituisce ogni lettera con la lettera che si trova sulla medesima riga e sulla colonna dell'altra lettera. Per esempio, *et* diventa *MN*, poiché M si trova sulla stessa riga di e e sulla stessa colonna di t, e N si trova sulla stessa riga di t e sulla stessa colonna di e.
- Se le due lettere sono sulla stessa riga, si sostituisce ogni lettera con la lettera immediatamente alla sua destra, con la convenzione che la matrice torna su se stessa passando dall'ultima colonna alla prima. Per esempio, *me* diventa *EG*.
- Se le due lettere sono sulla stessa colonna, si sostituisce ogni lettera con la lettera immediatamente sotto, con la convenzione che la matrice torni su se stessa passando dall'ultima riga alla prima. Per esempio, *ol* diventa *VR*.

Nel nostro esempio, il testo cifrato è

EG MN FQ QM KN BK SV VR GQ XN KU.

Per decifrarlo basta invertire la procedura.

Il sistema soccombe a un attacco basato sull'analisi delle frequenze, poiché le frequenze dei vari digrammi (combinazioni di due lettere) in inglese sono state tabulate. Naturalmente, basta cercare i digrammi più comuni, che dovrebbero corrispondere ai digrammi più comuni in inglese: *th, he, an, in, re, es, ...* Inoltre, una lieve modifica permette di ottenere i risultati più rapidamente. Per esempio, entrambi i digrammi *re* e *er* sono molto comuni. Se le coppie *IG* e *GI* sono comuni nel testo cifrato, allora una buona congettura è che *e, i, r, g* formino gli angoli di un rettangolo nella matrice.

Un'altra debolezza è che ogni lettera del testo in chiaro ha solo cinque possibili lettere corrispondenti nel testo cifrato. Inoltre, a meno che la parola chiave non sia lunga, le ultime righe della matrice sono prevedibili. Osservazioni come queste permettono di violare il sistema con un attacco di solo testo cifrato. Per maggiori dettagli su questa crittanalisi, si veda [Gaines].

Il cifrario ADFGX funziona nel modo seguente. Si dispongono le lettere dell'alfabeto in una matrice 5×5, in un qualche ordine, trattando le lettere i e j come se fossero una sola lettera, e si etichettano le colonne della matrice con le lettere A, D, F, G, X. Per esempio, la matrice potrebbe essere

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

Ogni lettera del testo in chiaro viene sostituita con l'etichetta della sua riga e della sua colonna. Per esempio, s diventa FA e z diventa DG. Se il testo in chiaro è

Kaiser Wilhelm

allora il risultato di questo passo iniziale è

XA FF GG FA AG DX GX GG FD XX AG FD GA.

Fin qui, si tratta di un cifrario a sostituzione camuffato. Il passo successivo incrementa sensibilmente la complessità. Si sceglie una parola chiave, per esempio *Rhein*. Si etichettano le colonne di una matrice mediante le lettere della parola chiave e si mette il risultato del passo iniziale in un'altra matrice:

R	H	E	I	N
X	A	F	F	G
G	F	A	A	G
D	X	G	X	G
G	F	D	X	X
A	G	F	D	G
A				

Ora si riordinano le colonne in modo che le corrispondenti etichette risultino ordinate alfabeticamente:

E	H	I	N	R
F	A	F	G	X
A	F	A	G	G
G	X	X	G	D
D	F	X	X	G
F	G	D	G	A
				A

Infine, il testo cifrato si ottiene leggendo le colonne dall'alto verso il basso (omettendo le etichette) in ordine:

$$FAGDFAFXFGFAXXDGGGXGXGDGAA.$$

Se si conosce la parola chiave, la decifrazione è semplice. Si può determinare la lunghezza di ogni colonna a partire dalla lunghezza della parola chiave e dalla lunghezza del testo cifrato. Le lettere sono poste in colonne, che sono riordinate in modo da coincidere con la parola chiave. Infine si usa la matrice originale per recuperare il testo in chiaro.
La matrice iniziale e la parola chiave erano cambiate di frequente, rendendo la crittanalisi molto difficoltosa, poiché per ogni combinazione era disponibile solo una quantità limita di testo cifrato. Tuttavia, il sistema fu attaccato con successo dal crittanalista francese Georges Painvin e dal Bureau du Chiffre, che furono in grado di decifrare un numero sostanziale di messaggi.
Ecco una delle tecniche che furono usate. Si supponga che due testi cifrati differenti, intercettati più o meno allo stesso tempo, concordino su molti caratteri iniziali. Un'ipotesi ragionevole è che i due testi in chiaro concordino su molte parole. Questo significa che gli elementi iniziali delle colonne dell'uno sono uguali a quelli dell'altro. Si cerca nei testi cifrati per trovare altri posti in cui concordano. Questi rappresentano probabilmente l'inizio delle colonne. Se questo è corretto, si conoscono le lunghezze delle colonne. Si dividono i testi cifrati in colonne in base a queste lunghezze. Per il primo testo cifrato, alcune colonne saranno di una data lunghezza e altre saranno più lunghe di uno. Le colonne più lunghe rappresentano le colonne che dovrebbero essere all'inizio, mentre le altre colonne dovrebbero essere in fondo. Si ripete la stessa cosa anche per il secondo testo cifrato. Se una colonna è lunga per entrambi i testi cifrati, è molto vicina all'inizio. Se è lunga per un testo cifrato e non per l'altro, va nel mezzo. Se è corta per entrambi, è vicina alla fine. A questo punto, si provano i vari ordinamenti delle colonne rispettando queste restrizioni. Ogni ordinamento corrisponde a un potenziale cifrario a sostituzione. Si usa l'analisi delle frequenze per cercare di risolverli. Si dovrebbe ottenere il testo in chiaro e la matrice di cifratura iniziale.
Le lettere *ADFGX* furono scelte perchè i loro simboli nel codice Morse ($\cdot-$, $-\cdot\cdot$, $\cdot\cdot-\cdot$, $--\cdot$, $-\cdot\cdot\cdot$) erano difficili da confondere. Questo permetteva di evitare errori di trasmissione e rappresenta uno dei primi tentativi di mettere insieme la correzione degli errori con la crittografia. Alla fine, il cifrario *ADFGX* fu sostituito dal cifrario *ADFGVX*, che usava una matrice iniziale 6×6. Ciò permise di usare tutte e 26 le lettere più le 10 cifre.
Per saperne di più sulla crittanalisi del cifrario ADFGX, si veda [Kahn].

2.7 Cifrari a blocchi

In molti dei precedenti crittosistemi, il cambiamento di una lettera nel testo in chiaro cambia esattamente una lettera nel testo cifrato. Nei cifrari a scorrimento, affini e a sostituzione, una data lettera nel testo cifrato proviene sempre esattamente da una lettera del testo in chiaro. Questo facilita notevolmente la ricerca della chiave mediante l'analisi delle frequenze. Nel sistema di Vigenère, l'uso di blocchi di lettere, corrispondenti alla lunghezza della chiave, rende l'analisi delle frequenze più difficoltosa,

ma ancora possibile, poiché non c'è alcuna interazione tra le varie lettere in ogni blocco.
I cifrari a blocchi evitano questi problemi cifrando simultaneamente blocchi di molte lettere o numeri. Il cambiamento di un carattere in un blocco di testo in chiaro dovrebbe cambiare potenzialmente tutti i caratteri nel corrispondente blocco di testo cifrato.
Il cifrario Playfair del Paragrafo 2.6 è un semplice esempio di cifrario a blocchi, poiché prende blocchi di due lettere e li cifra in blocchi di due lettere. Il cambiamento di una lettera di una coppia in chiaro cambia sempre almeno una lettera, e in genere entrambe le lettere, della coppia cifrata. Tuttavia, blocchi di due lettere sono troppo piccoli per essere sicuri, poiché, per esempio, un'analisi delle frequenze di solito ha successo.
Molti dei moderni crittosistemi che saranno trattati più avanti nel libro sono cifrari a blocchi. Per esempio, DES opera su blocchi di 64 bit. AES usa blocchi di 128 bit. RSA usa blocchi di varie centinaia di bit, in base al modulo usato. Le lunghezze di questi blocchi sono tutte sufficienti a garantire la sicurezza contro attacchi come l'analisi delle frequenze.
Il modo standard di usare un cifrario a blocchi è quello di convertire i blocchi di testo in chiaro in blocchi di testo cifrato, uno indipendentemente dall'altro e uno alla volta. Questo modo è chiamato modalità ECB (*Electronic Codebook Mode*). Tuttavia, ci sono anche modi che permettono di usare la retroazione dei blocchi di testo cifrato nella cifratura di blocchi successivi di testo in chiaro. Questo porta alla modalità CBC (*Cipher Block Chaining Mode*) e alla modalità CFB (*Cipher Feedback Mode*), che verranno discussi nel Paragrafo 4.5.
In questo paragrafo, discuteremo il cifrario di Hill, che è un cifrario a blocchi inventato nel 1929 da Lester Hill. Sembra che non sia mai stato molto usato in pratica. La sua importanza risiede nel fatto che probabilmente è la prima volta che nella crittografia si usano i metodi algebrici (algebra lineare e aritmetica modulare). Come vedremo più avanti, i metodi algebrici ora occupano una posizione centrale nella crittografia.
Si scelga un intero n, per esempio $n = 3$. La chiave è una matrice M di tipo $n \times n$ a coefficienti interi modulo 26. Per esempio

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}.$$

Il messaggio è scritto come una serie di vettori riga. Per esempio, se il messaggio è *abc*, lo si trasforma in un singolo vettore riga (0,1,2). Per cifrare si moltiplica[1] il vettore per la matrice e si riduce modulo 26:

$$(0,1,2)\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \equiv (0,23,22) \pmod{26}.$$

Quindi il testo cifrato è *AXW*. Il fatto che la prima lettera *a* rimanga inalterata è un fatto casuale, non un difetto del metodo.

[1] Tradizionalmente la matrice appare a destra nella moltiplicazione. Moltiplicare a sinistra porterebbe a una teoria del tutto analoga.

Per decifrare occorre che il determinante di M soddisfi la condizione

$$\mathrm{MCD}(\det(M), 26) = 1.$$

Questo significa che esiste una matrice N a coefficienti interi tale che $MN \equiv I \pmod{26}$, dove I è la matrice identità $n \times n$.
Nel nostro esempio, $\det(M) = -3$ e l'inversa di M è

$$N = -\frac{1}{3}\begin{pmatrix} -14 & 11 & -3 \\ 34 & -25 & 6 \\ -19 & 13 & -3 \end{pmatrix}.$$

Poiché 17 è l'inverso di -3 modulo 26, possiamo sostituire $-1/3$ con 17 e ridurre modulo 26:

$$N = \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix}.$$

Il lettore può verificare che $MN \equiv I \pmod{26}$. Per maggiori informazioni sul calcolo dell'inversa di una matrice modulo n, si veda il Paragrafo 3.8.
La decifrazione viene effettuata moltiplicando per N nel modo seguente

$$(0, 23, 22)\begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix} \equiv (0, 1, 2) \pmod{26}.$$

Nel metodo generale con una matrice $n \times n$, si spezza il testo in chiaro in blocchi di n caratteri e si trasforma ogni blocco in un vettore di n interi compresi tra 0 e 25 usando la corrispondenza $a = 0$, $b = 1$, ..., $z = 25$. Per esempio, con la matrice M precedente, il testo in chiaro

blockcipher

(dopo aver aggiunto una x per riempire l'ultimo spazio) diventa

1 11 14 2 10 2 8 15 7 4 17 23.

Ora si moltiplica ogni vettore per M, si riduce il risultato modulo 26 e infine si torna alle lettere:

$$(1, 11, 14)M = (199, 183, 181) \equiv (17, 1, 25) \pmod{26} = RBZ$$

$$(2, 10, 2)M = (64, 72, 82) \equiv (12, 20, 4) \pmod{26} = MUE$$

e così via. Nel nostro caso il testo cifrato è

RBZMUEPYONOM.

Si vede facilmente che cambiando una lettera del testo in chiaro di solito verranno cambiate n lettere del testo cifrato. Per esempio, se *block* viene cambiato in *clock*, le prime tre lettere del testo cifrato cambiano da *RBZ* a *SDC*. Tutto questo rende

l'analisi delle frequenze meno utile, tranne in alcuni casi in cui n è piccolo. Le frequenze dei **digrammi** (combinazioni di due lettere) e dei **trigrammi** (combinazioni di tre lettere) sono state calcolate. Oltre, il numero delle combinazioni diventa troppo grande (anche se non sarebbe difficile tabulare i risultati per le combinazioni più comuni). Inoltre, le frequenze delle combinazioni sono così basse che risulta difficile ottenere dei dati significativi senza avere una quantità di testo molto grande.
Una volta che si ha il testo cifrato, come lo si decifra? Semplicemente si spezza il testo cifrato in blocchi di lunghezza n, si trasforma ogni blocco in un vettore e si moltiplica ogni vettore a destra per la matrice inversa N. Nel nostro esempio, si ha

$$RBZ = (17, 1, 25) \mapsto (17, 1, 25)N = (755, 427, 66) \equiv (1, 11, 14) = blo,$$

e analogamente per il rimanente testo cifrato.
Il cifrario di Hill è difficile da decifrare usando solo il testo cifrato, ma soccombe facilmente a un attacco di testo in chiaro noto. Se non si conosce n, basta procedere per tentativi fino a quando non si trova il valore giusto. Pertanto si può sempre supporre che n sia noto. Se si hanno n blocchi di testo in chiaro di lunghezza n, allora si può usare il testo in chiaro e il corrispondente testo cifrato per ottenere un'equazione matriciale per M (o per N, che potrebbe essere più utile). Per esempio, supponiamo di sapere che $n = 2$ e di avere il testo in chiaro

howareyoutoday =

7 14 22 0 17 4 24 14 20 19 14 3 0 24

corrispondente al testo cifrato

ZWSENIUSPLJVEU =

25 22 18 4 13 8 20 18 15 11 9 21 4 20

I primi due blocchi danno l'equazione matriciale

$$\begin{pmatrix} 7 & 14 \\ 22 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 25 & 22 \\ 18 & 4 \end{pmatrix} \pmod{26}.$$

Sfortunatamente, la matrice $\begin{pmatrix} 7 & 14 \\ 22 & 0 \end{pmatrix}$ ha determinante -308, che non è invertibile modulo 26 (anche se questa matrice può essere usata per ridurre di molto il numero delle scelte per la matrice di cifratura). Allora si può sostituire, per esempio, l'ultima riga dell'equazione con il quinto blocco in modo da avere

$$\begin{pmatrix} 7 & 14 \\ 20 & 19 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 25 & 22 \\ 15 & 11 \end{pmatrix} \pmod{26}.$$

In questo caso, la matrice $\begin{pmatrix} 7 & 14 \\ 20 & 19 \end{pmatrix}$ è invertibile modulo 26:

$$\begin{pmatrix} 7 & 14 \\ 20 & 19 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 5 & 10 \\ 18 & 21 \end{pmatrix} \pmod{26}.$$

Pertanto si ha

$$M \equiv \begin{pmatrix} 5 & 10 \\ 18 & 21 \end{pmatrix} \begin{pmatrix} 25 & 22 \\ 15 & 11 \end{pmatrix} \equiv \begin{pmatrix} 15 & 12 \\ 11 & 3 \end{pmatrix} \pmod{26}.$$

Poiché il cifrario di Hill è vulnerabile a questo attacco, non può essere ritenuto molto robusto.

Un attacco di testo in chiaro scelto usa la stessa strategia, ma è un po' più veloce. Ancora, se non si conosce n, si provano varie possibilità finché non se ne trova una che va bene. Pertanto si può supporre di conoscere n. Si sceglie il primo blocco di testo in chiaro come $baaa\cdots = 1000\cdots$, il secondo come $abaa\cdots = 0100\cdots$, e così via fino all'n-esimo blocco che verrà scelto come $\cdots aaab = \cdots 0001$. I blocchi di testo cifrato saranno le righe della matrice M.

Per un attacco di testo cifrato scelto, si usa la stessa strategia dell'attacco precedente, dove le scelte ora rappresentano il testo cifrato. Il risultante testo in chiaro darà le righe della matrice inversa N.

In uno dei lavori più importanti sui fondamenti teorici della crittografia [Shannon1], Claude Shannon descrisse due proprietà che un buon crittosistema dovrebbe avere per impedire l'analisi statistica: la **diffusione** e la **confusione**.

Si ha *diffusione* quando cambiando un carattere del testo in chiaro, si cambiano molti caratteri del testo cifrato e, analogamente, cambiando un carattere del testo cifrato, si cambiano molti caratteri del testo in chiaro. Come abbiamo visto, il cifrario di Hill possiede questa proprietà. Questo significa che le statistiche delle frequenze delle lettere, dei digrammi e così via nel testo in chiaro sono diffuse su molti caratteri nel testo cifrato e che quindi è necessario avere molto più testo cifrato per poter attuare un attacco statistico significativo.

Si ha *confusione* quando la chiave non è legata al testo cifrato in modo semplice. In particolare, ogni carattere del testo cifrato dipende da più parti della chiave. Si supponga, per esempio, di avere un cifrario di Hill con una matrice $n \times n$ e di avere una coppia testo in chiaro–testo cifrato di lunghezza n^2 con cui si è in grado di ricavare la matrice di cifratura. Se si cambia un carattere del testo cifrato, allora una colonna della matrice può cambiare completamente (si veda l'Esercizio 12). Naturalmente, sarebbe preferibile che cambiasse l'intera chiave. Quando accade una cosa del genere, il crittanalista probabilmente dovrà ricavare direttamente l'intera chiave, invece che ricavarla pezzo per pezzo.

I cifrari di Vigenère e a sostituzione non possiedono le proprietà di diffusione e di confusione ed è questo il motivo per cui sono così vulnerabili all'analisi delle frequenze.

I concetti di diffusione e confusione giocano un ruolo importante in ogni cifrario a blocchi ben progettato. Naturalmente, uno svantaggio (che è esattamente il vantaggio crittografico) della diffusione è la propagazione degli errori: un piccolo errore nel testo cifrato diventa un grande errore nel messaggio decifrato, che di solito risulta essere illeggibile.

2.8 Numeri binari e ASCII

Quando si ha a che fare con i calcolatori spesso è più naturale rappresentare i dati come stringhe di 0 e 1 invece che come lettere e numeri.

simbolo	!	"	#	$	%	&	'
decimale	33	34	35	36	37	38	39
binario	0100001	0100010	0100011	0100100	0100101	0100110	0100111
(	)	*	+	,	-	.	/
40	41	42	43	44	45	46	47
0101000	0101001	0101010	0101011	0101100	0101101	0101110	0101111
0	1	2	3	4	5	6	7
48	49	50	51	52	53	54	55
0110000	0110001	0110010	0110011	0110100	0110101	0110110	0110111
8	9	:	;	<	=	>	?
56	57	58	59	60	61	62	63
0111000	0111001	0111010	0111011	0111100	0111101	0111110	0111111
@	A	B	C	D	E	F	G
64	65	66	67	68	69	70	71
1000000	1000001	1000010	1000011	1000100	1000101	1000110	1000111

Tabella 2.4 Codifica ASCII di alcuni simboli.

I numeri possono essere convertiti in binario (ossia in base 2). Ricordiamo ora brevemente di cosa si tratta. Di solito, i numeri sono scritti in base 10. Per esempio, 123 significa $1 \cdot 10^2 + 2 \cdot 10^1 + 3$. Il sistema binario usa 2 al posto di 10 e impiega solo le cifre 0 e 1. Per esempio, 110101 in binario rappresenta $2^5 + 2^4 + 2^2 + 1$ (che è uguale a 53 in base 10).

Ogni 0 o 1 è chiamato **bit**. Una rappresentazione che usa 8 bit è chiamata numero a 8 bit, o **byte**. Il numero più grande che può essere rappresentato con 8 bit è 255 e il numero più grande che può essere rappresentato con 16 bit è 65535.

Spesso non abbiamo a che fare solo con numeri. In questo caso, parole, simboli, lettere e numeri vengono tutti rappresentati in binario. Ci sono molti modi possibili per farlo. Uno dei modi standard è l'ASCII (*American Standard Code for Information Interchange*). Ogni carattere è rappresentato mediante 7 bit, in modo da poter rappresentare 128 possibili caratteri e simboli. I computer usano comunemente blocchi da otto bit e per questa ragione, ogni carattere è spesso rappresentato mediante 8 bit. L'ottavo bit viene usato per il controllo di parità, per vedere se si è verificato un errore durante la trasmissione, oppure, come spesso accade, viene usato per estendere l'elenco dei caratteri, in modo da includere simboli come ü ed è.

La Tabella 2.4 dà la codifica ASCII per alcuni simboli standard. Non li useremo mai in questo libro. Essi sono stati inclusi semplicemente per mostrare come un testo possa essere codificato mediante una successione di 0 e 1.

2.9 Stringa monouso

La stringa monouso è un crittosistema inviolabile sviluppato da Gilbert Vernam e Joseph Mauborgne intorno al 1918. Si parte rappresentando il messaggio come una successione di 0 e 1, scrivendo, per esempio, tutti i numeri in binario o in ASCII, come

Pertanto si ha

$$M \equiv \begin{pmatrix} 5 & 10 \\ 18 & 21 \end{pmatrix} \begin{pmatrix} 25 & 22 \\ 15 & 11 \end{pmatrix} \equiv \begin{pmatrix} 15 & 12 \\ 11 & 3 \end{pmatrix} \pmod{26}.$$

Poiché il cifrario di Hill è vulnerabile a questo attacco, non può essere ritenuto molto robusto.

Un attacco di testo in chiaro scelto usa la stessa strategia, ma è un po' più veloce. Ancora, se non si conosce n, si provano varie possibilità finché non se ne trova una che va bene. Pertanto si può supporre di conoscere n. Si sceglie il primo blocco di testo in chiaro come $baaa\cdots = 1000\cdots$, il secondo come $abaa\cdots = 0100\cdots$, e così via fino all'n-esimo blocco che verrà scelto come $\cdots aaab = \cdots 0001$. I blocchi di testo cifrato saranno le righe della matrice M.

Per un attacco di testo cifrato scelto, si usa la stessa strategia dell'attacco precedente, dove le scelte ora rappresentano il testo cifrato. Il risultante testo in chiaro darà le righe della matrice inversa N.

In uno dei lavori più importanti sui fondamenti teorici della crittografia [Shannon1], Claude Shannon descrisse due proprietà che un buon crittosistema dovrebbe avere per impedire l'analisi statistica: la **diffusione** e la **confusione**.

Si ha *diffusione* quando cambiando un carattere del testo in chiaro, si cambiano molti caratteri del testo cifrato e, analogamente, cambiando un carattere del testo cifrato, si cambiano molti caratteri del testo in chiaro. Come abbiamo visto, il cifrario di Hill possiede questa proprietà. Questo significa che le statistiche delle frequenze delle lettere, dei digrammi e così via nel testo in chiaro sono diffuse su molti caratteri nel testo cifrato e che quindi è necessario avere molto più testo cifrato per poter attuare un attacco statistico significativo.

Si ha *confusione* quando la chiave non è legata al testo cifrato in modo semplice. In particolare, ogni carattere del testo cifrato dipende da più parti della chiave. Si supponga, per esempio, di avere un cifrario di Hill con una matrice $n \times n$ e di avere una coppia testo in chiaro–testo cifrato di lunghezza n^2 con cui si è in grado di ricavare la matrice di cifratura. Se si cambia un carattere del testo cifrato, allora una colonna della matrice può cambiare completamente (si veda l'Esercizio 12). Naturalmente, sarebbe preferibile che cambiasse l'intera chiave. Quando accade una cosa del genere, il crittanalista probabilmente dovrà ricavare direttamente l'intera chiave, invece che ricavarla pezzo per pezzo.

I cifrari di Vigenère e a sostituzione non possiedono le proprietà di diffusione e di confusione ed è questo il motivo per cui sono così vulnerabili all'analisi delle frequenze. I concetti di diffusione e confusione giocano un ruolo importante in ogni cifrario a blocchi ben progettato. Naturalmente, uno svantaggio (che è esattamente il vantaggio crittografico) della diffusione è la propagazione degli errori: un piccolo errore nel testo cifrato diventa un grande errore nel messaggio decifrato, che di solito risulta essere illeggibile.

2.8 Numeri binari e ASCII

Quando si ha a che fare con i calcolatori spesso è più naturale rappresentare i dati come stringhe di 0 e 1 invece che come lettere e numeri.

#	$	%	&	'
35	36	37	38	39
0100011	0100100	0100101	0100110	0100111
+	,	-	.	/
43	44	45	46	47
0101011	0101100	0101101	0101110	0101111
3	4	5	6	7
51	52	53	54	55
110011	0110100	0110101	0110110	0110111
;	<	=	>	?
59	60	61	62	63
11011	0111100	0111101	0111110	0111111
C	D	E	F	G
67	68	69	70	71
0011	1000100	1000101	1000110	1000111

Codifica ASCII di alcuni simboli.

in binario (ossia in base 2). Ricordiamo ora breve-
numeri sono scritti in base 10. Per esempio, 123
ma binario usa 2 al posto di 10 e impiega solo le
nario rappresenta $2^5 + 2^4 + 2^2 + 1$ (che è uguale a

esentazione che usa 8 bit è chiamata numero a 8
ıe può essere rappresentato con 8 bit è 255 e il
presentato con 16 bit è 65535.
ı numeri. In questo caso, parole, simboli, lettere
ı binario. Ci sono molti modi possibili per farlo.
rican Standard Code for Information Interchan-
diante 7 bit, in modo da poter rappresentare
uter usano comunemente blocchi da otto bit e
so rappresentato mediante 8 bit. L'ottavo bit
er vedere se si è verificato un errore durante
cade, viene usato per estendere l'elenco dei
ome ü ed è.
lcuni simboli standard. Non li useremo mai
licemente per mostrare come un testo possa
di 0 e 1.

iolabile sviluppato da Gilbert Vernam e
e rappresentando il messaggio come una
utti i numeri in binario o in ASCII, come

discusso nel paragrafo precedente. Tuttavia, il messaggio può anche essere un video digitalizzato o un segnale audio.
La chiave è una successione casuale di 0 e 1 della stessa lunghezza del messaggio. Una volta usata, una chiave viene scartata e non viene usata mai più. La cifratura consiste nel sommare modulo 2, bit a bit, la chiave al messaggio. Questa operazione è spesso chiamata **or esclusivo** ed è indicata con *XOR* (*exclusive or*). In altre parole, si usano le regole $0 + 0 = 0$, $0 + 1 = 1$, $1 + 1 = 0$. Per esempio, se il messaggio è 00101001 e la chiave è 10101100, allora il testo cifrato si ottiene nel modo seguente:

$$\begin{array}{ll} 00101001 & \text{(testo in chiaro)} + \\ \underline{10101100} & \text{(chiave)} = \\ 10000101 & \text{(testo cifrato)} \end{array}$$

La decifrazione usa la stessa chiave. Basta sommare la chiave al testo cifrato: $10000101 + 10101100 = 00101001$.
Una variante consiste nel lasciare il testo in chiaro come una successione di lettere. La chiave è allora una successione casuale di scorrimenti, ognuno tra 0 e 25. La decifrazione usa la stessa chiave, ma sottrae invece di sommare gli scorrimenti.
Questo metodo di cifratura è completamente inviolabile a un attacco di solo testo cifrato. Per esempio, se il testo cifrato è *FIOWPSLQNTISJQL*, allora il testo in chiaro potrebbe essere *wewillwinthewar* oppure *theduckwantsout*. Ognuno di essi è ugualmente probabile, esattamente come ogni altro messaggio della stessa lunghezza. Pertanto il testo cifrato non dà informazioni sul testo in chiaro (tranne che sulla sua lunghezza). Tutto questo sarà chiarito quando verrà discussa la teoria dell'entropia di Shannon, nel Capitolo 18.
Se si ha un pezzo del testo in chiaro, allora si può trovare il corrispondente pezzo della chiave, ma non si potrà dire nulla sul resto della chiave. Nella maggioranza dei casi non è possibile un attacco di testo in chiaro scelto o di testo cifrato scelto. Del resto un attacco di questo tipo rivelerebbe solo la parte della chiave usata durante l'attacco stesso e questa parte di chiave non servirebbe a niente, a meno che non venisse riutilizzata.
Come si implementa questo sistema e dove può essere usato? La chiave può essere generata in anticipo. Naturalmente, c'è il problema di generare una successione di 0 e 1 realmente casuale. Un modo potrebbe essere quello di mettere alcune persone in una stanza a lanciare monete; questa soluzione sarebbe però troppo lenta nella maggior parte dei casi. Si potrebbe anche prendere un contatore Geiger e contare il numero dei clic che produce in un breve lasso di tempo, registrando 0 se questo numero è pari e 1 se è dispari. Esistono altri metodi più veloci, ma non del tutto casuali, che possono essere usati in pratica (si veda il Paragrafo 2.10), anche se generare rapidamente una buona chiave casuale resta difficile. Una volta che la chiave è stata generata, può essere inviata al ricevente da un corriere fidato. Il messaggio può allora essere inviato quando necessario. Si dice che la "linea rossa" tra Washington D.C. e Mosca per le comunicazioni tra i leader degli Stati Uniti e dell'U.R.S.S. durante la Guerra Fredda usasse una stringa monouso.
Uno svantaggio della stringa monouso è che richiede una chiave molto lunga, costosa da produrre e costosa da trasmettere. Una volta che la chiave sia stata usata, è pericoloso riusarla per un secondo messaggio, poiché una qualunque conoscenza, per esempio,

del primo messaggio darebbe una conoscenza del secondo. Quindi nella maggior parte dei casi, si usano vari metodi in cui un piccolo input può generare una successione di 0 e 1 sufficientemente casuale in modo da avere una "approssimazione" di una stringa monouso. La quantità di informazioni portate dal corriere è allora vari ordini di grandezza più piccola dei messaggi che verranno spediti. Un metodo di questo tipo, rapido ma non molto sicuro, è descritto nel Paragrafo 2.11.
Una variante della stringa monouso è stata sviluppata da Maurer, Rabin, Ding e altri. Si supponga di avere a disposizione un satellite che produce e invia successioni casuali di bit a una rapidità tale che nessun computer possa immagazzinare più di una frazione molto piccola dell'output. Alice vuole mandare un messaggio a Bob. Usano un metodo a chiave pubblica come RSA (si veda il Capitolo 6) per accordarsi su un metodo per scegliere alcuni bit dal flusso di bit casuali e usarli per generare una chiave per una stringa monouso. I bit casuali raccolti da Alice e Bob scompaiono prima che Eva abbia il tempo di decifrare la trasmissione a chiave pubblica; in questo modo Eva non può decifrare il messaggio. Infatti, poiché la cifratura usa una stringa monouso, non può mai decifrarlo e così Alice e Bob hanno raggiunto la sicurezza duratura per il loro messaggio. Si noti che la capacità di memorizzazione limitata è un'ipotesi fondamentale per questa procedura, così come la produzione e il campionamento accurato dei flussi di bit.

2.10 Generazione di bit pseudo-casuali

La stringa monouso e molte altre applicazioni crittografiche usano successioni di bit casuali. Prima di usare un algoritmo crittografico, come DES (Capitolo 4) o AES (Capitolo 5), è necessario generare una successione di bit casuali da usare come chiave. Un modo per generare bit casuali può essere quello di usare fenomeni casuali che appaiono in natura. Per esempio, si sa che il rumore termico ai morsetti di un resistore a semiconduttore è una buona sorgente di casualità. Tuttavia, esattamente come lanciare monete per produrre bit casuali non è pratico per le applicazioni crittografiche, quasi tutti i fenomeni fisici non sono pratici a causa della lentezza intrinseca della misura del processo e della difficoltà di assicurarsi che un avversario non osservi il processo stesso. Pertanto sarebbe opportuno avere un metodo per generare la casualità mediante software. Quasi tutti i computer possiedono un metodo per generare numeri casuali facilmente accessibile all'utente. Per esempio, la libreria standard del C contiene una funzione *rand()* che genera numeri pseudocasuali tra 0 e 65535. Questa funzione pseudocasuale prende come input un **seme** e produce in output un flusso di bit.
La funzione *rand()* e molti altri generatori di numeri pseudocasuali si basano su generatori lineari congruenziali. Un **generatore lineare congruenziale** (*linear congruential generator*) produce una successione di numeri $x_1, x_2, \ldots$, dove

$$x_n = ax_{n-1} + b \pmod{m}.$$

Il numero x_0 è il seme iniziale, mentre i numeri a, b e m sono parametri che determinano la ricorrenza. L'uso dei generatori di numeri pseudocasuali basati su generatori lineari congruenziali va bene per scopi sperimentali, ma è altamente sconsigliabile per scopi crittografici. Ciò è dovuto al fatto che chi intercetta alcuni bit può usarli per prevedere

i bit futuri con una probabilità abbastanza elevata (anche se i parametri a, b e m non sono noti). Infatti, è stato dimostrato che ogni generatore polinomiale congruenziale non è crittograficamente sicuro.
Nelle applicazioni crittografiche, si ha bisogno di una fonte di bit che non sia prevedibile. Ora discuteremo due modi di generare questi bit non prevedibili.
Il primo metodo usa le funzioni unidirezionali, ossia funzioni $f(x)$ facili da calcolare, ma per le quali, dato y, è computazionalmente intrattabile risolvere l'equazione $y = f(x)$ rispetto a x. Data una funzione f unidirezionale e dato un seme s casuale, sia $x_j = f(s + j)$ per $j = 1, 2, 3, \ldots$. Se b_j è il bit meno significativo di x_j, allora la successione b_0, b_1, ... sarà una successione pseudo-casuale di bit[2]. Questo metodo di generazione casuale di bit è usato spesso e risulta molto pratico. Le scelte usuali per la funzione unidirezionale sono DES (Capitolo 4) e l'algoritmo SHA (*Secure Hash Algorithm* (Paragrafo 8.3). Per esempio, il generatore crittografico di numeri pseudocasuali del toolkit OpenSSL (usato per le comunicazioni sicure in Internet) si basa su SHA.
Un altro metodo per generare bit casuali è usare un problema intrattabile della teoria dei numeri. Uno dei più comuni generatori di numeri pseudocasuali crittograficamente sicuri è il **generatore di bit pseudo-casuali Blum-Blum-Shub (BBS)**, noto anche come generatore ai residui quadratici. In questo schema, come prima cosa si generano due primi grandi p e q entrambi congruenti a 3 modulo 4. Posto $n = pq$, si sceglie a caso un intero x primo con n. Per inizializzare il generatore BBS, si sceglie il seme iniziale in modo che $x_0 \equiv x^2 \pmod{n}$. Il generatore BBS produce una successione di bit casuali b_1, b_2, ... mediante le seguenti operazioni:

1. $x_j \equiv x_{j-1}^2 \pmod{n}$
2. b_j è l'ultimo bit significativo di x_j.

Esempio. Siano

$$p = 24672462467892469787 \quad \text{e} \quad q = 396736894567834589803,$$

e sia

$$n = 9788476140853110794168855217413715781961.$$

Si consideri

$$x = 873245647888478349013.$$

Il seme iniziale è

$$\begin{aligned} x_0 &\equiv x^2 \pmod{n} \\ &\equiv 884529871047878009708991774601012286317 2. \end{aligned}$$

[2]Poiché in una funzione unidirezionale l'ultimo bit può essere costante, non è detto che questo metodo produca sempre una successione pseudocasuale. Tuttavia, in pratica funziona bene. Infatti il seme iniziale s spesso è generato a partire dalla pressione di un tasto, dall'orologio interno e così via.

I valori di x_1, x_2, ..., x_8 sono

$$\begin{aligned} x_1 &\equiv 71188942811313295227459624554981238224 08 \\ x_2 &\equiv 31451746088888931641513801520607045182 27 \\ x_3 &\equiv 48980077823071562332722331855748994303 55 \\ x_4 &\equiv 39354578189351129223470935461896723103 89 \\ x_5 &\equiv 67509951151009704890176130319874024604 0 \\ x_6 &\equiv 42899148287717401335461906582665151713 26 \\ x_7 &\equiv 44310667114543782608903863855938175216 68 \\ x_8 &\equiv 73368761241950463974142353336750053724 36. \end{aligned}$$

Prendendo l'ultimo bit significativo di ognuno di questi numeri, cosa che si fa facilmente controllando se il numero è dispari o pari, si ottiene la successione $b_1, \ldots, b_8 = 0,1,1,1,0,0,0,0$. ■

Il generatore Blum-Blum-Shub molto probabilmente non è prevedibile. Si veda [Blum-Blum-Shub]. Un problema è che BBS può essere lento da calcolare. Un modo per aumentare la sua velocità è quello di estrarre gli ultimi k bit significativi di x_j. Se $k \leq \log_2 \log_2 n$, questo sembra essere crittograficamente sicuro.

2.11 Successioni LFSR

Nota. *In questo paragrafo, tutte le congruenze sono modulo 2.*

In molte situazioni che coinvolgono le cifrature si presenta il problema di trovare un compromesso tra velocità e sicurezza. Se si vuole un livello di sicurezza molto alto, spesso bisogna sacrificare la velocità e viceversa. Per esempio, nella televisione via cavo si trasmettono molti bit di dati e quindi la velocità di cifratura è importante. La sicurezza invece in genere non è così importante, poiché raramente c'è un vantaggio economico ad allestire un costoso attacco al sistema.
In questo paragrafo, verrà descritto un metodo che può essere usato quando la velocità è più importante della sicurezza.
La successione

$$0100001001011001\overset{\cdots}{1}11100011011101010000100101100111 11$$

può essere descritta dando i valori iniziali

$$x_1 \equiv 0, \quad x_2 \equiv 1, \quad x_3 \equiv 0, \quad x_4 \equiv 0, \quad x_5 \equiv 0$$

e la ricorrenza lineare

$$x_{n+5} \equiv x_n + x_{n+2} \pmod{2}.$$

Più in generale, si consideri una ricorrenza lineare di ordine m

$$x_{n+m} \equiv c_0 x_n + c_1 x_{n+1} + \cdots + c_{m-1} x_{n+m-1} \pmod{2},$$

dove i coefficienti $c_0, c_1, \ldots$ sono interi. Se si danno i **valori iniziali**

$$x_1, \quad x_2, \ldots, \quad x_m,$$

allora tutti i valori successivi di x_n possono essere calcolati usando la ricorrenza. La successione che ne risulta, formata da 0 e 1, può essere usata come chiave di cifratura. Basta scrivere il testo in chiaro come una stringa di 0 e 1 e poi sommare mod 2, bit per bit, la stringa di uguale lunghezza formata dai primi elementi della successione chiave. Per esempio, se il testo in chiaro è 1011001110001111 e la successione chiave è quella data nell'esempio precedente, allora si ha

$$\begin{array}{ll} 1011001110001111 & \text{(testo in chiaro)} + \\ \underline{0100001001011001} & \text{(chiave)} = \\ 1111000111010110 & \text{(testo cifrato)} \end{array}$$

La decifrazione viene eseguita sommando la stringa chiave al testo cifrato esattamente nello stesso modo.

Uno dei vantaggi di questo metodo è che una chiave con un periodo grande può essere generata usando una quantità minima di informazioni. Il periodo lungo porta ad avere un miglioramento rispetto al metodo di Vigenère, dove un periodo corto permetteva di trovare la chiave. Nell'esempio precedente, assegnando il vettore iniziale (0,1,0,0,0) e i coefficienti (1,0,1,0,0) si otteneva una successione di periodo 31, ossia usando 10 bit si producevano 31 bit. Si può dimostrare che la ricorrenza

$$x_{n+31} \equiv x_n + x_{n+3}$$

e qualunque vettore iniziale non nullo produce una successione di periodo $2^{31} - 1 = 2147483647$. Pertanto 62 bit producono una chiave di più di due miliardi di bit. Questo è un gran vantaggio su una stringa monouso, dove tutti i miliardi di bit devono essere inviati in anticipo.

Questo metodo può essere implementato molto facilmente negli hardware che usano un **registro a scorrimento a retroazione lineare (LFSR)** (*Linear Feedback Shift Register*) ed è molto veloce. Nella Figura 2.1 è rappresentato un esempio di un registro a scorrimento a retroazione lineare in un caso semplice. Ricorrenze più complicate sono implementate usando un numero maggiore di registri e di XOR.

A ogni colpo di clock, il bit di ogni cella viene fatto scorrere nelle altre celle come indicato, dove $\oplus$ denota la somma modulo 2 dei bit di input. L'output, dato dal bit x_m, viene sommato al bit successivo di testo in chiaro, per produrre il testo cifrato. Il diagramma nella Figura 2.1 rappresenta la ricorrenza $x_{m+3} \equiv x_{m+1} + x_m$. Una volta assegnati i valori iniziali x_1, x_2, x_3, la macchina produce i bit successivi in modo molto efficiente.

Sfortunatamente il precedente metodo di cifratura soccombe facilmente a un attacco di testo in chiaro noto. Più precisamente, se si conoscono solo alcuni bit consecutivi di testo in chiaro, con i corrispondenti bit di testo cifrato, si può determinare la ricorrenza e quindi calcolare tutti i bit successivi della chiave. Sottraendo modulo 2 (o, equivalentemente, sommando modulo 2) il testo in chiaro dal testo cifrato, si ottengono i bit della chiave. Pertanto per il resto di questa discussione ignoreremo il testo cifrato e il testo in chiaro e supporremo di aver scoperto una porzione della

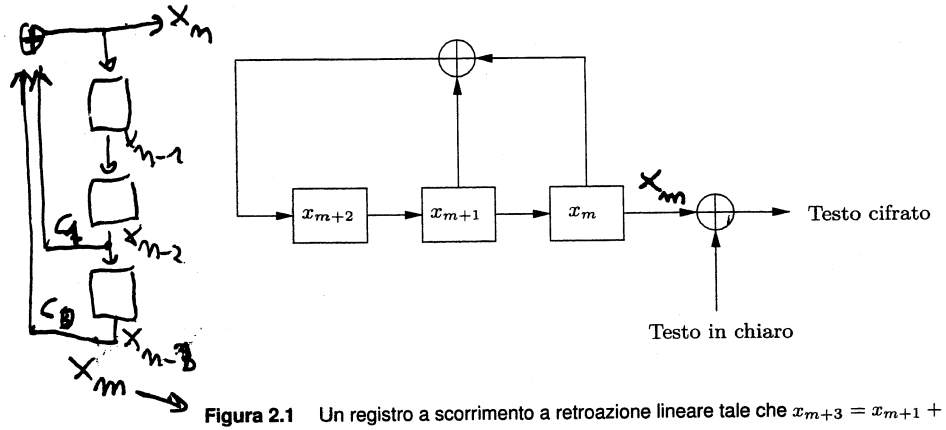


Figura 2.1 Un registro a scorrimento a retroazione lineare tale che $x_{m+3} = x_{m+1} + x_m$.

succession chiave. L'obiettivo è di usare questa porzione di chiave per dedurre i coefficienti della ricorrenza e per calcolare di conseguenza il resto della chiave.

Per esempio, si supponga di conoscere il segmento iniziale 011010111100 della successione 011010111100010011010111... di periodo 15 e si supponga si sapere che essa è generata da una ricorrenza lineare. Allora come si determinano i coefficienti della ricorrenza? Non è necessario neanche conoscere l'ordine. Una ricorrenza di ordine 1 produce una successione costante. Quindi si può considerare una ricorrenza $x_{n+2} = c_0 x_n + c_1 x_{n+1}$ di ordine 2. Poiché si hanno i valori iniziali $x_1 = 0$, $x_2 = 1$, $x_3 = 1$, $x_4 = 0$, si ottiene il seguente sistema

$$\begin{array}{lll} 1 & \equiv c_0 \cdot 0 + c_1 \cdot 1 & \text{(per } n = 1\text{)} \\ 0 & \equiv c_0 \cdot 1 + c_1 \cdot 1 & \text{(per } n = 2\text{)} \end{array}$$

che, in forma matriciale, diventa

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Poiché la soluzione è $c_0 = 1$ e $c_1 = 1$, si ha la ricorrenza $x_{n+2} \equiv x_n + x_{n+1}$. Purtroppo, però, questa ricorrenza non è quella che si sta cercando, essendo $x_6 \not\equiv x_4 + x_5$. Allora si passa a una ricorrenza di ordine 3, che porta all'equazione matriciale

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

Il determinante della matrice dei coefficienti è 0 modulo 2 e l'equazione non ha soluzioni. Questo lo si può vedere facilmente osservando che ogni colonna della matrice ha somma 0 modulo 2, mentre il vettore dei termini noti ha somma 1. Si passa quindi a considerare una ricorrenza di ordine 4, che porta all'equazione matriciale

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

che ha soluzione $c_0 = 1$, $c_1 = 1$, $c_2 = 0$, $c_3 = 0$. La ricorrenza risultante è pertanto

$$x_{n+4} \equiv x_n + x_{n+1}.$$

Essa genera gli elementi rimanenti del frammento di chiave che si conosce e quindi risulta essere la migliore ipotesi per la ricorrenza che genera la successione chiave. Un rapido calcolo mostra che essa è effettivamente la ricorrenza che si stava cercando.
In generale, per una ricorrenza di ordine m si ha l'equazione matriciale

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_m \\ x_2 & x_3 & \cdots & x_{m+1} \\ \vdots & \vdots & \ddots & \vdots \\ x_m & x_{m+1} & \cdots & x_{2m-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix} \equiv \begin{pmatrix} x_{m+1} \\ x_{m+2} \\ \vdots \\ x_{2m} \end{pmatrix}$$

dove i valori di x_1, x_2, ..., x_{2m} devono essere noti. Più avanti si mostrerà che la matrice dei coefficienti è invertibile modulo 2 se e solo se gli elementi x_1, x_2, ..., x_{2m-1} non soddisfano alcuna ricorrenza lineare di ordine inferiore a m.
A questo punto, è chiaro quale sia la strategia per determinare i coefficienti della ricorrenza. Se si conoscono i bit iniziali della chiave, allora si considerano le matrici $m \times m$ (per $m = 2, 3, 4, \ldots$) del tipo precedente e se ne calcolano i determinanti. Se per molti valori consecutivi di m il determinante è 0, allora ci si ferma. L'ultimo m che dà un determinante non nullo (ossia uguale a 1 modulo 2) è probabilmente l'ordine della ricorrenza. Risolta l'equazione matriciale, in modo da ottenere i coefficienti c_0, ..., c_{m-1}, si va a controllare se la successione generata dalla ricorrenza ottenuta coincide con la successione dei bit noti della chiave. Se le due successioni non coincidono, si passa a considerare un valore più grande di m.
La stessa procedura può essere applicata anche nel caso in cui si conosca un certo numero di bit consecutivi della chiave, che però non sono quelli iniziali. Basta usare questi bit come valori iniziali. Una volta trovata la ricorrenza, si può tornare indietro e trovare i bit precedenti.
Un esempio dovrebbe chiarire la situazione. Si supponga di avere la seguente successione di 100 bit:

1001100100111000110001010001111011001111101010100 1
0110110101100001101110010101111000000010001001000 0.

I primi 20 determinanti, a partire da $m = 1$, sono

1,0,1,0,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0.

Una congettura ragionevole è che l'ultimo determinante non nullo si ha in corrispondenza di $m = 8$. Risolvendo la corrispondente l'equazione matriciale, si ottengono i coefficienti

$$\{c_0, c_1, \ldots, c_7\} = \{1,1,0,0,1,0,0,0\}.$$

Quindi si può supporre che la ricorrenza sia

$$x_{n+8} \equiv x_n + x_{n+1} + x_{n+4}.$$

Questa ricorrenza effettivamente genera tutti i 100 termini della successione originale e quindi fornisce la corretta soluzione, almeno in base alla conoscenza che si possiede. Si supponga ora che i 100 bit stiano nel mezzo di una qualche successione e che si vogliano conoscere i bit precedenti. Per esempio, si supponga che la successione parta con x_{17}, cosicché $x_{17} = 1$, $x_{18} = 0$, $x_{19} = 0$, ... Allora si scrive la ricorrenza come

$$x_n \equiv x_{n+1} + x_{n+4} + x_{n+8}$$

(si tenga presente che lavorando modulo 2 si ha $-x_n \equiv x_n$ e $-x_{n+8} \equiv x_{n+8}$). Così, per $n = 16$, si ha

$$x_{16} \equiv x_{17} + x_{20} + x_{24} \equiv 1 + 0 + 1 \equiv 0.$$

Continuando in questo modo, si determinano successivamente x_{15}, x_{14}, ..., x_1.

Proposizione. *Sia x_1, x_2, x_3, ... una successione di bit generata da una ricorrenza lineare modulo 2. Per ogni $n \geq 1$, sia*

$$M_n = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_2 & x_3 & \cdots & x_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ x_n & x_{n+1} & \cdots & x_{2n-1} \end{pmatrix}.$$

Se N è l'ordine minimo della ricorrenza che genera la successione x_1, x_2, x_3, ..., allora $\det(M_N) \equiv 1 \pmod 2$ *e* $\det(M_n) \equiv 0 \pmod 2$ *per ogni $n > N$.*

Dimostrazione. Iniziamo col fare qualche osservazione sull'ordine delle ricorrenze. Se una successione soddisfa una ricorrenza di ordine 3 del tipo $x_{n+3} \equiv x_{n+2}$, è chiaro che essa soddisfa anche una ricorrenza di ordine inferiore del tipo $x_{n+1} = x_n$ (almeno per $n \geq 2$). Tuttavia, esistono altri modi meno ovvi in cui una successione può soddisfare una ricorrenza di ordine inferiore. Si consideri, per esempio, la ricorrenza $x_{n+4} \equiv x_{n+3} + x_{n+1} + x_n$ con i valori iniziali 1, 1, 0, 1. Usando questa ricorrenza si possono calcolare i termini successivi: 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1.... A questo punto si vede facilmente che la successione soddisfa anche la ricorrenza $x_{n+2} \equiv x_{n+1} + x_n$.
Se esiste una ricorrenza di ordine N e se $n > N$, allora una riga della matrice M_n è congruente modulo 2 a una combinazione lineare delle altre righe. Per esempio, se la ricorrenza è $x_{n+3} = x_{n+2} + x_n$, allora la quarta riga è somma della prima e della terza riga. Di conseguenza $\det(M_n) \equiv 0 \pmod 2$ per ogni $n > N$.
Si supponga ora che $\det(M_N) \equiv 0 \pmod 2$. Allora esiste un vettore riga non nullo $\overline{b} = (b_0, \ldots, b_{N-1})$ tale che $\overline{b} M_N \equiv 0$. Questo implica l'esistenza di una ricorrenza per la successione x_1, x_2, x_3, ... di ordine inferiore a N, contro l'ipotesi che N sia l'ordine più piccolo. Di conseguenza, deve essere $\det(M_N) \equiv 1 \pmod 2$.
Si supponga che la ricorrenza di ordine N sia

$$x_{N+n} \equiv c_0 x_n + \cdots + c_{N-1} x_{n+N-1}.$$

Inoltre, per ogni $i \geq 0$, sia

$$M^{(i)} = \begin{pmatrix} x_{i+1} & x_{i+2} & \cdots & x_{i+N} \\ x_{i+2} & x_{i+3} & \cdots & x_{i+N+1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{i+N} & x_{i+N+1} & \cdots & x_{i+2N-1} \end{pmatrix}.$$

In particolare, $M^{(0)} = M_N$. La ricorrenza implica la congruenza

$$M^{(i)} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{N-1} \end{pmatrix} \equiv \begin{pmatrix} x_{i+N+1} \\ x_{i+N+2} \\ \vdots \\ x_{i+2N} \end{pmatrix},$$

dove il vettore a secondo membro è l'ultima colonna di $M^{(i+1)}$.
Per la scelta di $\overline{b}$, si ha $\overline{b}M^{(0)} = \overline{b}M_N = 0$. Se $\overline{b}M^{(i)} = 0$ per qualche i, allora

$$\overline{b} \begin{pmatrix} x_{i+N+1} \\ x_{i+N+2} \\ \vdots \\ x_{i+2N} \end{pmatrix} \equiv \overline{b}M^{(i)} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix} \equiv 0.$$

Quindi $\overline{b}$ annulla l'ultima colonna di $M^{(i+1)}$. Poiché le rimanenti colonne di $M^{(i+1)}$ sono colonne di $M^{(i)}$, si trova che $\overline{b}M^{(i+1)} \equiv 0$. Per induzione, si ottiene $\overline{b}M^{(i)} \equiv 0$ per ogni $i \geq 0$.
Sia $n \geq 1$. La prima colonna di $M^{(n-1)}$ dà

$$b_0 x_n + b_1 x_{n+1} + \cdots + b_{N-1} x_{n+N-1} \equiv 0.$$

Poiché $\overline{b}$ non è il vettore nullo, $b_j \neq 0$ per almeno un j. Sia m il più grande j per cui $b_j \neq 0$, ossia tale che $b_m = 1$. Poiché si sta lavorando modulo 2, si ha $b_m x_{n+m-1} \equiv -x_{n+m-1}$. Quindi si può riscrivere la ricorrenza nella forma

$$x_{n+m-1} \equiv b_0 x_n + b_1 x_{n+1} + \cdots + b_{m-1} x_{n+m-2}.$$

Si ha così una ricorrenza di ordine $m-1$. Poiché $m-1 < N$ e poiché N è per ipotesi l'ordine minimo, si ha una contraddizione. Pertanto l'assunzione che $\det(M_N) \equiv 0$ deve essere falsa e quindi $\det(M_N) \equiv 1$. □

Per concludere faremo qualche commento sul periodo di una successione. Supponiamo che l'ordine della ricorrenza sia m. Comunque scelti, m termini consecutivi della successione determinano tutti gli elementi successivi, e, invertendo la ricorrenza, anche tutti i valori precedenti. Chiaramente, se si hanno m 0 consecutivi, allora tutti i valori successivi e tutti i valori precedenti sono 0. Quindi possiamo escludere questo caso. Ci sono $2^m - 1$ stringhe di 0 e 1 di lunghezza m in cui almeno un termine è diverso da zero. Quindi non appena ci sono più di $2^m - 1$ termini, qualche stringa di lunghezza m deve comparire due volte e quindi la successione si ripete. Il periodo della successione è al più $2^m - 1$.
A una ricorrenza $x_{n+m} \equiv c_0 x_n + c_1 x_{n+1} + \cdots + c_{m-1} x_{n+m-1} \pmod 2$ è sempre associato un polinomio

$$f(T) = T^m - c_{m-1} T^{m-1} - \cdots - c_0.$$

Se $f(T)$ è irriducibile modulo 2 (ossia se non è congruente al prodotto di due polinomi di grado inferiore), allora si può dimostrare che il periodo divide $2^m - 1$. Si ha un caso

interessante quando $2^m - 1$ è primo (questi numeri sono chiamati primi di Mersenne). Se il periodo non è 1, cioè se la successione non è costante, allora il periodo in questo caso speciale deve essere massimo, ossia $2^m - 1$ (si veda il Paragrafo 3.11). L'esempio in cui il periodo è $2^{31} - 1$ è di questo tipo.
Le successioni LFSR sono state ampiamente studiate. Si veda, per esempio, [Golomb] o [van der Lubbe].
Un modo di contrastare l'attacco precedente è quello di usare ricorrenze non lineari, come per esempio

$$x_{n+3} \equiv x_{n+2} x_n + x_{n+1}.$$

Si possono anche combinare non linearmente più LFSR con clock irregolari. Anche se in generale questi sistemi sono più difficili da violare, qui non verranno discussi.

2.12 Enigma

I congegni meccanici di cifratura noti come macchine a rotori furono sviluppati intorno al 1920 da più persone. Il più noto fu progettato da Arthur Scherbius e divenne la famosa macchina Enigma usata dai Tedeschi nella seconda guerra mondiale.
Si credeva che questa macchina fosse estremamente sicura e molti dei tentativi fatti per violare il sistema fallirono. Tuttavia, un gruppo di formato da tre crittologi polacchi, Marian Rejewski, Henryk Zygalski e Jerzy Różycki, riuscì a violare le prime versioni di Enigma durante gli anni trenta del secolo scorso. Le loro tecniche furono passate agli Inglesi nel 1939, due mesi prima che la Germania invadesse la Polonia. Gli Inglesi estesero le tecniche dei Polacchi e decifrarono con successo i messaggi tedeschi per tutta la seconda guerra mondiale.
Il fatto che Enigma fosse stata violata è rimasto segreto per quasi 30 anni dopo la fine della guerra, in parte perché gli Inglesi avevano venduto alle loro ex-colonie alcune macchine Enigma di cui erano venuti in possesso e non volevano che sapessero che il sistema era stato violato.
Qui di seguito daremo una breve descrizione di Enigma e di un attacco sviluppato da Rejewski. Per maggiori dettagli, si veda per esempio [Kozaczuk], che contiene alcune appendici scritte da Rejeweski in cui vengono descritti dettagliatamente gli attacchi a Enigma.
Nella Figura 2.2 è riportato un diagramma schematico della macchina. Per maggiori dettagli, invitiamo il lettore a visitare qualcuno dei numerosi siti web che si possono trovare in Internet, dove si possono vedere fotografie di macchine Enigma e dettagliati diagrammi che mostrano il funzionamento interno di queste macchine.
Nella Figura 2.2, L, M e N sono i rotori. Su un lato di ogni rotore ci sono 26 contatti elettrici fissi, disposti in circolo. Sull'altro lato ci sono 26 contatti a molla, anch'essi disposti in circolo in modo da toccare i contatti fissi del rotore adiacente. All'interno di ogni rotore, i contatti fissi sono collegati ai contatti a molla in modo casuale. Queste connessioni sono differenti in ogni rotore. Ogni rotore ha 26 possibili configurazioni iniziali.
R è il riflettore, che ha 26 contatti a molla, connessi a coppie. K è la tastiera, uguale alla tastiera di una normale macchina per scrivere. S è il pannello dei collegamenti.

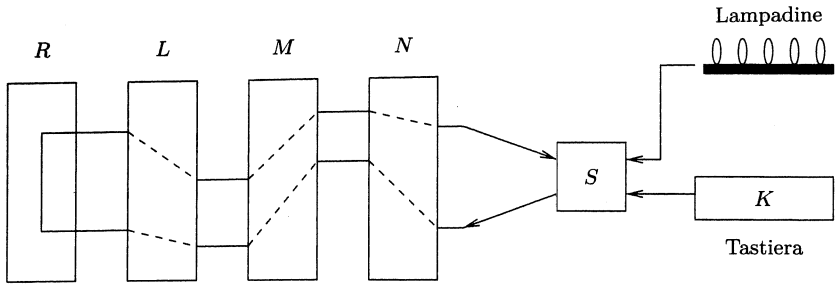


Figura 2.2 Diagramma schematico della macchina Enigma.

Esso ha circa sei coppie di spine che possono essere usate per scambiare sei coppie di lettere.
Quando si preme un tasto, il primo rotore N compie $1/26$ di giro. Poi, a partire dal tasto, l'elettricità passa attraverso S e quindi attraverso i rotori N, M e L. Quando raggiunge il riflettore R, viene rimandata indietro lungo un differente percorso attraverso L, M e N e quindi attraverso S. A questo punto, l'elettricità accende una lampadina che corrisponde a una lettera sulla tastiera, che è la lettera del testo cifrato.
Poiché il rotore N ruota prima di ogni cifratura, si ha qualcosa di molto più complicato di un cifrario a sostituzione. Inoltre, anche i rotori L e M ruotano, anche se molto meno frequentemente, proprio come le ruote di un contachilometri.
La decifrazione usa esattamente lo stesso metodo. Supponiamo che chi invia e chi riceve abbiano delle macchine identiche, entrambe sulle stesse posizioni iniziali. Chi invia cifra il messaggio battendolo sulla tastiera e registrando la successione di lettere indicate dalle lampadine. Questo testo cifrato viene poi mandato a chi riceve, che batte il testo cifrato sulla propria macchina. La successione di lettere indicate dalle lampadine è il messaggio originale. Questo può essere visto come segue. La lampadina "a" e il tasto "a" sono attaccati a un filo che esce dal pannello dei collegamenti. La lampadina "h" e il tasto "h" sono attaccati a un altro filo che esce dal pannello dei collegamenti. Se si preme il tasto "a" e si accende la lampadina "h", allora il percorso elettrico attraverso la macchina collega anche la lampadina "a" al tasto "h". Quindi se si preme il tasto "h", si accende la lampadina "a".
Un ragionamento analogo mostra che nessuna lettera viene mai cifrata in se stessa. A prima vista potrebbe sembrare una buona idea, ma in realtà è una debolezza, poiché permette a un crittanalista di eliminare molte possibilità fin dall'inizio.
La sicurezza del sistema si basa sul tenere segrete le posizioni iniziali dei rotori, la posizione delle spine sul pannello dei collegamenti e il cablaggio interno dei rotori e del riflettore. Le inizializzazioni dei rotori e del pannello dei collegamenti vengono cambiate periodicamente (per esempio, quotidianamente).
Supponiamo che il cablaggio interno dei rotori sia noto (come nel caso, per esempio, di una macchina catturata), anche se esistono dei modi per dedurre queste informazioni quando si ha a disposizione abbastanza testo cifrato. In effetti, questo è proprio ciò venne fatto in alcuni casi.

In quanti modi può essere inizializzata la macchina? Ci sono 26 posizioni iniziali per ognuno dei tre rotori, che danno $26^3 = 17576$ possibilità. Poi ci sono 6 ordinamenti possibili dei tre rotori, che in tutto danno $6 \cdot 17576 = 105456$ modi possibili per inizializzare i rotori. In versioni successive di Enigma, furono disponibili cinque rotori. Ogni giorno se ne sceglievano tre. In questo modo si avevano 60 ordinamenti possibili dei rotori e quindi 1054560 modi di inizializzare i rotori.
Sul pannello dei collegamenti, ci sono 100391791500 modi di scambiare sei coppie di lettere. Sembra proprio che ci siano troppe inizializzazioni possibili della macchina per avere una qualche speranza di violare il sistema. Tecniche come l'analisi delle frequenze falliscono, poiché le rotazioni dei rotori cambiano la sostituzione per ogni carattere del messaggio.
Ma allora come riuscirono ad attaccare Enigma? Non descriveremo l'intero attacco, ma ci limiteremo a mostrare come le posizioni iniziali dei rotori furono determinate intorno al 1937. Anche se questo attacco si basò su una debolezza nel protocollo usato a quei tempi, esso dà però l'idea generale di come gli attacchi procedettero in altre situazioni.
A ogni operatore Enigma veniva dato un libro di parole chiave [3] contenente le inizializzazioni giornaliere che dovevano essere usate nel mese successivo. Tuttavia, se queste inizializzazioni fossero state usate senza alcuna modifica, ogni messaggio spedito in un dato giorno avrebbe avuto la sua prima lettera cifrata dallo stesso cifrario a sostituzione. Il rotore avrebbe poi girato e la seconda lettera di ogni testo sarebbe corrisposta a un altro cifrario a sostituzione e questa sostituzione sarebbe stata la stessa per tutti i messaggi di quel giorno. Un'analisi delle frequenze della prima lettera di ogni messaggio intercettato durante un giorno avrebbe probabilmente permesso la decifrazione della prima lettera di ogni testo. Una seconda analisi delle frequenze avrebbe permesso di decifrare la seconda lettera di ogni testo. Procedendo in questo modo, si sarebbero decifrate le rimanenti lettere dei testi cifrati (ad eccezione delle parti finali dei testi cifrati più lunghi).
Per evitare questo problema, per ogni messaggio l'operatore sceglieva un messaggio chiave formato da una successione di tre lettere, per esempio r, f, u. Poi usava l'inizializzazione giornaliera per cifrare questo messaggio chiave. Poiché le comunicazioni radio erano soggette a errori, batteva *rfu* due volte, cifrando quindi *rfurfu* per ottenere una stringa di sei lettere. I rotori erano poi posti sulle posizioni r, f e u e quindi iniziava la cifratura del messaggio reale. Così le prime sei lettere del messaggio trasmesso erano il messaggio chiave cifrato e il resto era il testo cifrato. Poiché ogni messaggio usava una chiave differente, l'analisi delle frequenze era inutile.
Il ricevente usava semplicemente le inizializzazioni giornaliere per decifrare le prime sei lettere del messaggio. Poi metteva i rotori sulle posizioni indicate dal messaggio chiave decifrato e procedeva a decifrare il messaggio.
La duplicazione della chiave ha rappresentato un grande aiuto per i crittanalisti. Supponiamo che in un giorno vengano intercettati vari messaggi e che tra questi ve ne siano tre che hanno le seguenti sei lettere iniziali

[3] Nella crittografia classica, il termine "cifrario" indicava un elenco di parole chiave, mentre una trasformazione crittografica era chiamata codice. La crittografia moderna ha portato con sé il relativo linguaggio di origine anglosassone e il termine "cifrario" ha assunto il significato introdotto alla fine del Paragrafo 1.1.2 e usato nel resto del libro. (*N.d.Rev.*)

dmqvbn
vonpuy
pucfmq

Tutti sono stati cifrati con la stessa inizializzazione giornaliera. La prima cifratura corrisponde a una permutazione A delle 26 lettere. Prima di passare alla cifratura della seconda lettera, un rotore gira e quindi la seconda lettera usa un'altra permutazione B. Analogamente, le rimanenti quattro lettere corrisponderanno a delle permutazioni C, D, E, F. La strategia consiste nell'andare a considerare i prodotti AD, BE e CF. Prima di procedere abbiamo bisogno di ricordare alcune cose sulle permutazioni. Quando scriviamo AD per due permutazioni A e D, intendiamo che si applica prima la permutazione A e poi la permutazione D (in alcuni libri l'ordine è invertito). La permutazione che manda a in b, b in c e c in a sarà scritta come un ciclo $(a\,b\,c)$ di lunghezza 3. Un'analoga notazione verrà usata anche per cicli di lunghezza diversa. Per esempio, $(a\,b)$ è la permutazione che scambia a con b. Una permutazione può sempre essere scritta come un prodotto di cicli. Per esempio, la permutazione

$$(dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)$$

è la permutazione che manda d in v, v in p, t in e, r in w, ...e fissa a e s. Se i cicli sono disgiunti (ossia se non ci sono cicli che hanno lettere in comune), questa decomposizione in cicli è unica.
Torniamo ora ai testi intercettati. Non conosciamo le lettere di nessuno dei tre messaggi chiave. Se chiamiamo il primo messaggio chiave xyz, allora $xyzxyz$ viene cifrato in $dmqvbn$. Sappiamo che la permutazione A manda x in d. Inoltre, la quarta permutazione D manda x in v. Ma sappiamo di più. Per come è fatto il cablaggio interno della macchina, in realtà A scambia tra loro x e d e D scambia tra loro x e v. Quindi il prodotto AD delle due permutazioni manda d in v (più precisamente, A manda d in x e poi D manda x in v). L'incognita x è stata eliminata. Analogamente, il secondo testo intercettato dice che AD manda v in p e il terzo messaggio dice che AD manda p in f. Pertanto deve essere

$$AD = (dvpf\cdots)\cdots.$$

Nello stesso modo, la seconda e la quinta lettera dei tre messaggi portano ad avere

$$BE = (oumb\cdots)\cdots$$

e la terza e la sesta lettera portano ad avere

$$CF = (cqny\cdots)\cdots.$$

Con una quantità sufficiente di dati, si possono dedurre le decomposizioni di AD, BE e CF come prodotto di cicli. Per esempio, si potrebbe avere

$$\begin{aligned} AD &= (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)\\ BE &= (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k)\\ CF &= (abviktjgfcqny)(duzrehlxwpsmo). \end{aligned}$$

Queste informazioni dipendono solo dalle inizializzazioni giornaliere del pannello dei collegamenti e dei rotori, ma non dal messaggio chiave. Quindi sono relative ad ogni macchina usata in un dato giorno.
Diamo un'occhiata più da vicino al pannello dei collegamenti. Esso introduce una permutazione S all'inizio del processo e poi aggiunge la permutazione inversa S^{-1} alla fine. Abbiamo bisogno di un altro fatto sulle permutazioni. Si considerino una permutazione P e una seconda permutazione della forma SPS^{-1} (dove S è un'altra permutazione e dove S^{-1} è la permutazione inversa di S; nel nostro caso, $S = S^{-1}$). Le loro decomposizioni in cicli in genere non saranno formate dagli stessi cicli, ma di sicuro il numero dei cicli è il medesimo e le lunghezze dei cicli sono le stesse. Per esempio, AD ha cicli di lunghezza 10, 10, 2, 2, 1, 1. Se decomponiamo $SADS^{-1}$ in cicli disgiunti, comunque scelta la permutazione S, otterremo ancora cicli di lunghezza 10, 10, 2, 2, 1, 1. Quindi se si cambiano le inizializzazioni del pannello dei collegamenti senza cambiare le posizioni iniziali dei rotori, le lunghezze dei cicli restano invariate. Nella decomposizione di AD, BE e CF in cicli, le lunghezze dei cicli appaiono sempre un numero pari di volte. Questo è un fenomeno generale. Per una spiegazione di tale fenomeno, si veda l'Appendice E del libro di Kozaczuk precedentemente citato.
Rejewski e i suoi colleghi compilarono un catalogo di tutte le 105456 configurazioni iniziali dei rotori con l'insieme delle lunghezze dei cicli per le corrispondenti tre permutazioni AD, BE e CF. In questo modo, potevano prendere i testi cifrati di un dato giorno, dedurre le lunghezze dei cicli e trovare il piccolo numero di corrispondenti configurazioni iniziali per i rotori. Ognuna di queste sostituzioni poteva essere provata individualmente. L'effetto del pannello dei collegamenti (quando era usata la configurazione corretta) era allora semplicemente quello di un cifrario a sostituzione, facilmente violabile. Questo metodo funzionò fino al Settembre del 1938, quando venne adottato un nuovo metodo modificato per trasmettere i messaggi chiave. La precedente tecnica, opportunamente modificata, venne ancora usata per decifrare i messaggi. Il processo fu anche meccanizzato, usando macchine chiamate "bombe" per trovare le chiavi giornaliere, ognuna in circa due ore.
Queste tecniche furono estese dagli Inglesi a Bletchley Park durante la seconda guerra mondiale. Esse includevano la costruzione di "bombe" più sofisticate. Queste macchine, ideate da Alan Turing, sono spesso considerate come i primi calcolatori elettronici.

2.13 Esercizi

1. Cesare vuole organizzare un incontro segreto con Marco Antonio, presso il Tevere (river) o presso il Colosseo (arena). Invia il testo cifrato *EVIRE*. Antonio, non conoscendo la chiave, prova tutte le possibilità. Dove incontrerà Cesare? (*Suggerimento:* questa è una domanda a trabocchetto.)

2. Il testo cifrato UCR è stato messo in cifra usando la funzione affine $9x + 2 \pmod{26}$. Trovare il testo in chiaro.

3. Cifrare *howareyou* usando la funzione affine $5x + 7 \pmod{26}$. Qual è la funzione di decifrazione? Controllare che essa funzioni effettivamente.

4. Dato un cifrario affine (mod 26), si fa un attacco di testo in chiaro scelto usando *hahaha*. Il testo cifrato è *NONONO*. Determinare la funzione di cifratura.

5. Il testo cifrato *CRWWZ* è stato messo in cifra mediante un cifrario affine modulo 26. Il testo in chiaro inizia con *ha*. Decifrare il messaggio.

6. Si supponga di cifrare mediante un cifrario affine e poi di cifrare ulteriormente mediante un secondo cifrario affine (entrambi modulo 26). Questo porta a qualche vantaggio rispetto all'uso di un solo cifrario affine? Motivare la risposta, qualunque essa sia.

7. Se nei cifrari affini si lavora modulo 27 invece che modulo 26, quante sono le chiavi possibili? E se si lavora modulo 29?

8. Si supponga di voler cifrare un messaggio usando un cifrario affine. Si ponga $a = 0$, $b = 1$, ..., $z = 25$ e inoltre si includa ? $= 26$, ; $= 27$, " $= 28$, ! $= 29$. Quindi si usi come funzione di cifratura $x \mapsto \alpha x + \beta \pmod{30}$, dove α e β sono due interi fissati.

(a) Mostrare che esistono esattamente otto scelte possibili per l'intero α (cioé, esistono solo otto scelte di α (con $0 < \alpha < 30$) che permettono di decifrare).

(b) Per $\alpha = 10$ e $\beta = 0$, trovare due lettere in chiaro che vengono cifrate nella stessa lettera cifrata.

9. Si vuole effettuare una cifratura affine usando la funzione $\alpha x + \beta$, pur avendo $\text{MCD}(\alpha, 26) = d > 1$. Mostrare che se $x_1 = x_2 + (26/d)$, allora $\alpha x_1 + \beta \equiv \alpha x_2 + \beta \pmod{26}$. Pertanto in questo caso non è possibile decifrare univocamente.

10. Si consideri un linguaggio formato solo dalle lettere a e b. La frequenza di a è 0,1 e la frequenza di b è 0,9. Un messaggio è cifrato usando un cifrario di Vigenère (che lavora modulo 2 invece che modulo 26). Il testo cifrato è BABABAAABA.

(a) Mostrare che la lunghezza della chiave è probabilmente 2.

(b) Usando l'informazione sulle frequenze delle lettere, determinare la chiave e decifrare il messaggio.

11. Si consideri un linguaggio formato dalle tre lettere a, b, c, che compaiono rispettivamente con frequenza 0,7, 0,2, 0,1. Il seguente testo cifrato è stato cifrato mediante il metodo di Vigenère (dove, naturalmente, gli scorrimenti sono modulo 3 invece che modulo 26):

ABCBABBBAC.

Sapendo che la lunghezza della chiave è 1, 2, oppure 3, mostrare che la lunghezza della chiave è probabilmente 2 e determinare la chiave più probabile.

12. Il prodotto scalare di due vettori $\mathbf{v}$ e $\mathbf{w}$ dello spazio n-dimensionale è dato da $\mathbf{v} \cdot \mathbf{w} = |\mathbf{v}||\mathbf{w}| \cos\theta$, dove θ è l'angolo tra i due vettori (misurato nel piano da essi generato) e $|\mathbf{v}|$ è la lunghezza di $\mathbf{v}$. Usando questo fatto (e le notazioni del Paragrafo 2.3) mostrare che il prodotto scalare $\mathbf{A}_0 \cdot \mathbf{A}_i$ assume valore massimo per $i = 0$.

13. Il testo cifrato *YIFZMA* è stato messo in cifra mediante un cifrario di Hill che usa la matrice $\begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix}$. Trovare il testo in chiaro.

14. Il testo cifrato *GEZXDS* è stato messo in cifra mediante un cifrario di Hill che usa una matrice 2×2. Il testo in chiaro è *solved*. Trovare la matrice M di cifratura.

15. Eva cattura la macchina cifrario di Hill di Bob, che usa una matrice M modulo 26 di tipo 2×2. Prova un attacco di testo in chiaro scelto e trova che il testo in chiaro *ba* viene cifrato in *HC* e che il testo in chiaro *zz* viene cifrato in *GT*. Qual è la matrice M?

16. **(a)** Il testo cifrato *ELNI* è stato messo in cifra mediante un cifrario di Hill che usa una matrice 2×2. Il testo in chiaro è *dont*. Trovare la matrice di cifratura.

(b) Si supponga che il testo cifrato sia *ELNK* e che il testo in chiaro sia ancora *dont*. Trovare la matrice di cifratura. Si noti che la seconda colonna della matrice è cambiata. Questo mostra che nella generazione dell'ultimo carattere del testo cifrato (si veda la fine del Paragrafo 2.7) è coinvolta l'intera seconda colonna della matrice di cifratura.

17. In un cifrario di Hill si usa la matrice $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ come matrice di cifratura. Trovare due testi in chiaro cui corrisponde lo stesso testo cifrato.

18. Siano a, b, c, d, e, f interi modulo 26. Si consideri la seguente combinazione dei cifrari di Hill e affine. Rappresentato un blocco di testo in chiaro come una coppia (x,y) modulo 26, il corrispondente testo cifrato (u,v) è dato da

$$(x \quad y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e \quad f) \equiv (u \quad v) \pmod{26}.$$

Dire come si può attaccare questo sistema mediante un attacco di testo in chiaro scelto (con l'obiettivo di trovare la chiave a, b, c, d, e, f). Si dovrebbe dire esplicitamente quali testi in chiaro si scelgono e come recuperare la chiave.

19. Una successione generata da una ricorrenza di ordine 3 inizia con 001110. Trovare i quattro elementi successivi della successione.

20. Si consideri la successione che inizia con $k_1 = 1$, $k_2 = 0$, $k_3 = 1$ e che è definita dalla ricorrenza $k_{n+3} = k_n + k_{n+1} + k_{n+2}$ di ordine 3. Questa successione può anche essere generata mediante una ricorrenza di ordine 2. Determinare questa ricorrenza di ordine 2 risolvendo le appropriate equazioni matriciali.

21. Si supponga di avere una macchina LFSR che lavora modulo 3 invece che modulo 2. Essa usa una ricorrenza di ordine 2 della forma

$$x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} \pmod{3}$$

per generare la successione 1, 1, 0, 2, 2, 0, 1, 1. Scrivere e risolvere l'equazione matriciale che permette di trovare i coefficienti c_0 e c_1.

22. **Usare il metodo LFSR**, modificato in modo da lavorare modulo 5. Data la **ricorrenza** e le condizioni inziali seguenti

$$x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} + 2 \pmod 5,$$

$$x_1 = 0, \quad x_2 = 1, \quad x_3 = 1, \quad x_4 = 0,$$

determinare i coefficienti c_0 e c_1.

23. A metà degli anni ottanta del secolo scorso, un annuncio di lavoro dell'NSA riportava, nella parte superiore, un 1 seguito da cento 0. Il testo iniziava dicendo:

> "Stai guardando un 'googol'. Dieci elevato alla 100-esima potenza. Un 1 seguito da cento 0. Contando 24 ore al giorno, avresti bisogno di 120 anni per raggiungere un googol. Due vite. È un numero impossibile da afferrare. Un numero che va oltre l'immaginazione."

Quanti numeri si dovrebbero contare ogni secondo per raggiungere un googol in 120 anni? (Questo problema non ha nulla a che fare coi crittosistemi di questo capitolo. Serve solo per dare un'idea di quanto sia grande un numero con 100 cifre da un punto di vista computazionale. Per quanto riguarda l'annuncio di lavoro, un'ipotesi è che l'ente coinvolto ritenesse che il tempo richiesto allora per fattorizzare un numero di 100 cifre fosse uguale al tempo richiesto per contare un googol.)

24. Alice invia un messaggio a Bob usando uno dei seguenti crittosistemi.

(a) Cifrario a scorrimento.

(b) Cifrario affine.

(c) Cifrario di Hill (con una matrice 2×2).

Alice è annoiata e non sa come passare il tempo, quindi invia un testo in chiaro formato della sola lettera a ripetuta alcune centinaia di volte. Eva, che sa quale sistema è stato usato senza però conoscere la chiave, intercetta il testo cifrato. Per i sistemi (a), (b) e (c), dire in che modo Eva può riconoscere che il testo in chiaro è formato da una sola lettera ripetuta e dire se Eva può dedurre la lettera e la chiave. (*Nota:* per il sistema (c), la soluzione dipende in modo sostanziale dal fatto che la lettera ripetuta sia a e non b, c, ...)

25. L'operatore di una macchina di cifratura di Vigenère non ha niente di meglio da fare e cifra un testo in chiaro formato dalla stessa lettera dell'alfabeto ripetuta varie centinaia di volte. La chiave è una parola inglese di sei lettere. Eva sa che la chiave è una parola, ma non conosce la sua lunghezza.

(a) Quale proprietà del testo cifrato porterà Eva a sospettare che il testo in chiaro sia una lettera ripetuta e le permetterà di indovinare che la lunghezza della chiave è sei?

(b) Una volta che Eva ha riconosciuto che il testo in chiaro è una lettera ripetuta, come può determinare la chiave? (*Suggerimento:* usare il fatto che nessuna parola inglese di lunghezza sei è lo scorrimento di un'altra parola inglese.)

(c) Supponiamo che Eva non noti la proprietà richiesta nella parte (a) e che per trovare la lunghezza della chiave usi il metodo degli spostamenti per contare le corrispondenze. Qual è il numero delle corrispondenze per i vari spostamenti? In altre parole, perché la lunghezza della chiave diventa ovvia con questo metodo?

2.14 Problemi al calcolatore

1. Decifrare il seguente testo cifrato

```
ycvejqwvhqtdtwvwu
```

sapendo che è stato messo in cifra mediante un cifrario a scorrimento. (Il testo cifrato è contenuto nei file scaricabili, sotto il nome *ycve*. Si vedano le Appendici per informazioni su come scaricare i file.)

2. Il seguente testo cifrato è stato generato mediante un cifrario a scorrimento:

```
lcllewljazlnnzmvyiylhrmhza
```

Mediante un'analisi delle frequenze, ipotizzare la chiave usata nel cifrario. Usare il computer per verificare le varie ipotesi. Qual è il testo in chiaro che si ottiene dalla decifrazione? (Il testo cifrato è contenuto nei file scaricabili, sotto il nome *lcll.*)

3. Il seguente testo cifrato è stato ottenuto mediante un cifrario affine:

```
edsgickxhuklzveqzvkxwkzukcvuh
```

Le prime due lettere del testo in chiaro sono *se*. Decifrarlo. (Il testo cifrato è contenuto nei file scaricabili, sotto il nome *edsg.*)

4. Il seguente testo cifrato è stato ottenuto mediante un cifrario affine usando la funzione $3x + b$ per un opportuno b:

```
tcabtiqmfheqqmrmvmtmaq
```

Decifrarlo. (Il testo cifrato è contenuto nei file scaricabili, sotto il nome *tcab.*)

5. Sperimentare il cifrario affine $y \equiv mx + n \pmod{26}$ con $m > 26$. In particolare, dire se le cifrature che si ottengono sono uguali a quelle ottenute con $m < 26$.

6. In questo problema bisogna utilizzare un po' di programmazione. Sia $\{A,C,G,T\}$ un alfabeto su quattro lettere, che, per esempio, potrebbero rappresentare l'adenina, la citosina, la guanina e la timina, i quattro nucleotidi che formano i mattoni del DNA e dell'RNA. Si associno le lettere A, C, G, T rispettivamente ai numeri 0, 1, 2, 3.

(a) Usando il cifrario a scorrimento con uno scorrimento di 1, cifrare la seguente successione di nucleotidi presa dall'inizio del tredicesimo cromosoma umano:

GAATTCGCGGCCGCAATTAACCCTCACTAAAGGGATCTCT AGAACT.

(b) Scrivere un programma che esegua cifrature affini sull'alfabeto dei nucleotidi. Che restrizioni ci sono sul cifrario affine?

7. Il seguente messaggio è stato cifrato mediante il metodo di Vigenère con una chiave di lunghezza al più 6. Decifrarlo e dire cosa c'è di insolito nel testo in chiaro. In che modo altera i risultati?

```
hdsfgvmkoowafweetcmfthskucaqbilgjofmaqlgspvatvxqbiryscpcfr
mvswrvnqlszdmgaoqsakmlupsqforvtwvdfcjzvgsoaoqsacjkbrsevbel
vbksarlscdcaarmnvrysywxqgvellcyluwwveoafgclazowafojdlhssfi
ksepsoywxafowlbfcsocylngqsyzxgjbmlvgrggokgfgmhlmejabsjvgml
nrvqzcrggcrghgeupcyfgtydycjkhqluhgxgzovqswpdvbwsffsenbxapa
  sgazmyuhgsfhmftayjxmwznrsofrsoaopgauaaarmftqsmahvqecev
```

(Il testo cifrato è contenuto nei file scaricabili, sotto il nome *hdsf*. Il testo in chiaro viene da *Gadsby* di Ernest Vincent Wright.)

8. Il seguente messaggio è stato cifrato mediante il metodo di Vigenère. Trovare il testo in chiaro.

```
ocwyikooooniwugpmxwktzdwgtssayjzwyemdlbnqaaavsuwdvbrflauplo
oubfgqhgcscmgzlatoedcsdeidpbhtmuovpiekifpimfnoamvlpqfxejsm
xmpgkccaykwfzpyuavtelwhrhmwkbbvgtguvtefjlodfefkvpxsgrsorvg
tajbsauhzrzalkwuowhgedefnswmrciwcpaaavogpdnfpktdbalsisurln
psjyeatcuceesohhdarkhwotikbroqrdfmzghgucebvgwcdqxgpbgqwlpb
                  daylooqdmuhbdqgmyweuik
```

(Il testo cifrato è contenuto nei file scaricabili, sotto il nome *ocwy*. Il testo in chiaro proviene da *I pupazzi ballerini* di Sir Arthur Conan Doyle.)

9. Il seguente messaggio è stato cifrato mediante il metodo di Vigenère. Decifrarlo. (Il testo cifrato è contenuto nei file scaricabili, sotto il nome *xkju*.)

```
xkjurowmllpxwznpimbvbqjcnowxpcchhvvfvsllfvxhazityxohulxqoj
axelxzxmyjaqfstsrulhhucdskbxknjqidallpqslluhiaqfpbpcidsvci
hwhwewthbtxrljnrsncihuvffuxvoukjljswmaqfvjwjsdyljogjxdboxa
jultucpzmpliwmlubzxvoodybafdskxgqfadshxnxehsaruojaqfpfkndh
saafvulluwtaqfrupwjrszxgpfutjqiynrxnyntwmhcukjfbirzsmehhsj
          shyonddzzntzmplilrwnmwmlvuryonthuhabwnvw
```

10. Decifrare il seguente testo cifrato ottenuto mediante un cifrario di Hill


```
zirkzwopjjoptfapuhfhadrq
```

che usa la matrice

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 11 & 2 & 4 & 6 \\ 2 & 9 & 6 & 4 \end{pmatrix}.$$

11. Determinare la ricorrenza che genera la seguente successione LFSR:

```
1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0,
0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0,
0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1,
1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0,
1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1,
                    1, 1, 1, 1, 1
```

(Il testo cifrato è contenuto nei file scaricabili, sotto il nome *L101*.)

12. Trovare i coefficienti della ricorrenza che genera i seguenti cento termini iniziali dell'output di un LFSR:

```
1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0,
0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1,
1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0,
1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1,
0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0,
                    1, 0, 0, 0, 0
```

(Il testo cifrato è contenuto nei file scaricabili, sotto il nome *L100*.)

13. Il seguente testo cifrato è stato ottenuto facendo una somma XOR tra l'output di un LFSR e il testo in chiaro.

```
0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0,
1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0,
                  1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1
```

Se il testo in chiaro inizia con

```
1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0
```

trovare l'intero testo in chiaro. (Il testo cifrato è contenuto nei file scaricabili, sotto il nome *L011*.)