Alcune note introduttive sulla crittografia

Scuola Estiva di Geometrie Combinatorie
"Giuseppe Tallini"

Teoria dei Grafi, Criptologia e Geometrie Finite

Potenza, 5–9 settembre 2005

L. Giuzzi A. Sonnino

Introduzione

Un problema fondamentale in un numerosi sistemi di comunicazione è quello di come reagire in presenza di avversari. Un esempio classico è quello in cui si vuole trasmettere un messaggio, cercando di garantire che nessuno (a parte il destinatario) possa comprendere il contenuto di quanto detto. Questo, il problema della confidenzialità, è stato l'oggetto della crittografia (lett. scrittura nascosta) per la maggior parte della storia della civiltà umana.

Ad esempio, uno dei criptosistemi più antichi di cui si abbia notizia è il *cifrario di Atbash,* utilizzato nel Libro di Geremia del Vecchio Testamento. Il principio su cui si basava era estremamente semplice: si invertiva l'ordine delle lettere dell'alfabeto (ebraico) e per cifrare si usava la seguente sostituzione:

א	ב	ג	ד	⋯	ק	ר	ש	ת
↓	↓	↓	↓		↓	↓	↓	↓
ת	ש	ר	ק	⋯	ד	ג	ב	א

mentre per decifrare bastava compiere sul testo cifrato la stessa operazione. Ad esempio, utilizzando il cifrario di Atbash la parola אלהים viene mutata in תמצנך.

D'altro canto, sino a tempi relativamente recenti, l'utilizzo delle scritture segrete era appannaggio quasi esclusivo dei servizi segreti delle varie potenze e difficilmente riguardava il singolo individuo.

Con il diffondersi di mezzi di comunicazione digitali e di nuove modalità di interazione a distanza fra individui, sono sorte nuove necessità, quali, ad esempio, quella di stabilire un canale sicuro fra due individui che non abbiano mai comunicato fra loro in precedenza. Si sono dunque sviluppate nuove tecniche e prassi, quali, ad esempio, la *crittografia a chiave pubblica* o *crittografia asimmetrica*, presentata pubblicamente per la prima volta nel lavoro di W. Diffie & M. Hellman [DH76] del 1976.

In particolare, ci si è resi conto di come tecniche e metodi crittografici possano essere applicati anche a degli scenari più vasti rispetto quello della confidenzialità, quali ad esempio

1. nascondere l'esistenza di un messaggio (steganografia);

2. garantire l'integrità di un messaggio (hashing);

3. attestare l'identità di un soggetto (firma digitale, autenticazione).

In pratica, la crittografia oggi non serve solamente a trasmettere segreti, ma può, paradossalmente, essere impiegata per rendere maggiormente esplicito il contenuto di un messaggio.

Per tali motivi in queste note si userà una definizione in senso lato di crittografia come tutti i metodi e le tecniche che possono essere messi in atto per *comunicare in modo affidabile in presenza di avversari*.

È chiaro che una tale definizione è di natura puramente qualitativa e volutamente vaga. Concretamente, per poter parlare di criptosistema si devono formalizzare almeno tre fattori distinti:

1. la specifica della funzione e della modalità di utilizzo del sistema;

2. la descrizione di un meccanismo di trasformazione dei messaggi;

3. la validazione del meccanismo di trasformazione secondo dei modelli formali di attacco.

L'opera con cui lo studio della crittografia è stato formalizzato all'interno di una teoria matematica rigorosa è la fondamentale monografia di C. E. Shannon [Sha49] del 1949.

Proprio lo studio sitematico, con metodi matematici, dei criptosistemi ha mostrato come la nozione di *sicurezza* o *robustezza* non possa, in generale, essere espressa in termini assoluti.

Implementare un criptosistema è, in generale, un delicato gioco di equilibrio fra più fattori contrastanti, quali la velocità di cifratura richiesta, la lunghezza della chiave utilizzata, il modello di attacco previsto e, non trascurabile, il periodo di tempo per cui si prevede che i dati debbano restare segreti. Si può dire che ogni criptosistema possiede una data di scadenza; nel migliore dei casi, tale durata di vita utile si aggira probabilmente sui 10/15 anni.

In particolare, tutti i criptosistemi "storici", con l'eccezione dello *one time pad* che è dimostrabilmente sicuro, sono al giorno d'oggi forzabili.

Rappresentazione dei messaggi

Alfabeti

Un insieme finito di simboli $\mathfrak{A}$, contenente $q > 1$ elementi, è detto *a*lfabeto. Una qualsiasi n–pla ordinata di suoi elementi $\mathbf{w}$ è una *p*arola di lunghezza n su $\mathfrak{A}$ o n–*b*locco. In generale, se questo non dà luogo ad ambiguità, scriveremo la n–pla $\mathbf{w} = (w_1, w_2, \ldots, w_n)$ come

$$\mathbf{w} = w_1 w_2 \cdots w_n.$$

Esempio 1 Sia $\mathfrak{A}$ l'insieme formato dai 3 simboli $\{a, b, c\}$. Con tali simboli è possibile formare esattamente 3^n parole di lunghezza n. Ad esempio, le 27 parole su $\mathfrak{A}$ di lunghezza 3 sono

$$\begin{array}{ccccccccc} aaa & aab & aac & aba & abb & abc & aca & acb & acc \\ baa & bab & bac & bba & bbb & bbc & bca & bcb & bcc \\ caa & cab & cac & cba & cbb & cbc & cca & ccb & ccc \end{array}.$$

Siano ora $\mathbf{p} = p_1 p_2 \cdots p_n$ e $\mathbf{q} = q_1 q_2 \cdots q_m$ due parole su di un medesimo alfabeto $\mathfrak{A}$. La *s*omma o *c*oncatenazione di $\mathbf{p}$ e $\mathbf{q}$ è la parola su $\mathfrak{A}$

$$\mathbf{pq} = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m,$$

avente lunghezza $n + m$.

Il più piccolo alfabeto possibile è quello che contiene solamente 2 simboli, convenzionalmente indicati come 0 e 1. Tale alfabeto $\mathfrak{B} = \{0, 1\}$ è detto *binario* ed è particolarmente importante per i sistemi digitali. Un simbolo dell'alfabeto binario $\mathfrak{B}$ è detto *b*it. La rappresentazione interna dei dati nei moderni calcolatori elettronici[1] è binaria e tutte le operazioni sono implementate a livello di bit.

[1] I primi elaboratori elettronici, quali, ad esempio, l'ENIAC o l'IBM/650 utilizzavano una rappresentazione dei numeri in forma decimale, la cosidetta forma BCD (*b*inary coded decimal).

In generale, possiamo sempre supporre che ogni alfabeto $\mathfrak{A}$ sia in corrispondenza biunivoca con $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ oppure con gli elementi di qualche campo finito $\mathbb{F}_n$ con $n = p^h$ ove p è un primo.

Ad esempio, l'alfabeto latino `A-Z` può essere rappresentato mediante l'insieme $\mathbb{Z}_{26}$ degli interi modulo 26. Volendo invece considerare 2-blocchi possiamo etichettare le coppie ordinate di simboli (x, y) mediante la corrispondenza

$$\begin{array}{ccc} \mathbb{Z}_{26} \times \mathbb{Z}_{26} & \longrightarrow & \mathbb{Z}_{676} \\ (x, y) & \longmapsto & 26x + y. \end{array}$$

Così facendo, otteniamo un'espressione delle singole lettere che compongono ciascun blocco come cifre di un elemento di $\mathbb{Z}_{676}$ espresso in base 26, mentre i 2-blocchi sono rappresentati da numeri di due cifre nella stessa base. Similmente, volendo considerare 3-blocchi, si può usare la corrispondenza

$$\begin{array}{ccc} \mathbb{Z}_{26} \times \mathbb{Z}_{26} \times \mathbb{Z}_{26} & \longrightarrow & \mathbb{Z}_{17576} \\ (x, y, z) & \longmapsto & 676x + 26y + z. \end{array}$$

In generale, gli r-blocchi composti da simboli di un alfabeto di lunghezza N possono essere rappresentati da sequenze di interi compresi fra 0 e $N^r - 1$, facendo corrispondere ad ogni blocco un elemento di $\mathbb{Z}_{N^r}$ espresso in base N.

Un *testo* è un elemento o una sequenza concatenata di elementi dell'insieme

$$\mathcal{T} := \bigcup_{r \geq 0} \mathbb{Z}_n^r,$$

dove nel caso di un campo finito l'unione viene fatta su $\mathbb{F}_n^r$. Un *linguaggio* è un sottoinsieme di $\mathcal{T}$. Nel caso di un linguaggio formale, quale ad esempio un linguaggio di programmazione, il sottoinsieme è definito in modo molto preciso per mezzo di un certo numero di regole ricorsive, mentre per una lingua parlata tali regole sono perlopiù molto vaghe. In quest'ultimo caso è conveniente adottare un approccio probabilistico per descrivere le possibili occorrenze delle parole e delle singole lettere che le compongono.

Probabilità

Lo *spazio dei messaggi* è una sequenza di variabili casuali $\{X_0.X_1, \ldots, X_{r-1}\}$ con cui a ciascun evento $(m_0, m_1, \ldots, m_{r-1})$ è associata una probabilità

$$\Pr\left(X_j = m_0, X_{j+1} = m_1, \ldots X_{j+r} = m_{r-1}\right)$$

dove gli indici sono da intendersi ridotti modulo r. Ponendo $j = 0$ possiamo scrivere, più semplicemente, $\Pr(m_0, m_1, \ldots, m_{r-1})$. Dalla teoria della probabilità seguono le seguenti relazioni:

A	0,1119	H	0,0141	O	0,0954	V	0,0225
B	0,0073	I	0,0973	P	0,0255	W	0,0000
C	0,0483	J	0,0000	Q	0,0087	X	0,0002
D	0,0398	K	0,0000	R	0,0604	Y	0,0000
E	0,1269	L	0,0614	S	0,0565	Z	0,0044
F	0,0116	M	0,0288	T	0,0568		
G	0,0190	N	0,0706	U	0,0327		

Tabella 1: Distribuzione di probabilità delle lettere in Italiano

i) $\Pr(m_0, m_1, \ldots, m_{r-1}) \geq 0$ per ogni sequenza $(m_0, m_1, \ldots, m_{r-1})$;

ii) $$\sum_{(m_0,m_1,\ldots,m_{r-1})\in\mathcal{T}} \Pr(m_0, m_1, \ldots, m_{r-1}) = 1;$$

iii) $$\sum_{(m_r,m_{r+1},\ldots,m_{s-1})\in\mathcal{T}} \Pr(m_0, m_1, \ldots, m_{s-1}) = \Pr(m_0, m_1, \ldots, m_{r-1}), \text{ per } s > r.$$

Se nello studio di un linguaggio ci limitiamo a valutare blocchi a di lunghezza 1, osserviamo che la loro distribuzione $p(a)$ è indipendente dalla posizione che assumono all'interno di un blocco di lunghezza maggiore di 1, cosicché

$$\Pr(m_0, m_1, \ldots, m_{r-1}) = p(m_0)p(m_1)\ldots p(m_{r-1}).$$

Ad esempio, utilizzando i valori riportati nella tabella 2, possiamo calcolare la probabilità di occorrenza della parola "ten" nella lingua Inglese come segue

$$\Pr(\texttt{TEN}) = p(\texttt{T})p(\texttt{E})p(\texttt{N}) = \Pr(\texttt{NET}) \approx 8{,}2 \cdot 10^{-4}.$$

Osserviamo che in questo modello alle parole `TEN` e `NET` resta associata la stessa probabilità.

La probabilità che due caratteri scelti a caso in un messaggio coincidano dipende dalla distribuzione delle probabilità $(p_0, \ldots, p_{r-1})$ di occorrenza dei singoli caratteri e coincide col numero

$$\kappa_p = \sum_{i=0}^{r-1} p_i^2.$$

Il valore di κ_p è circa $0{,}0738$ per la lingua italiana e $0{,}0613$ per l'inglese. È interessante osservare come tale valore spesso sia sufficiente per caratterizzare in modo soddisfacente la lingua in cui un messaggio è scritto.

A	0,0804	H	0,0549	O	0,0760	V	0,0099
B	0,0154	I	0,0276	P	0,0200	W	0,0192
C	0,0306	J	0,0016	Q	0,0011	X	0,0019
D	0,0399	K	0,0067	R	0,0612	Y	0,0173
E	0,1251	L	0,0414	S	0,0654	Z	0,0009
F	0,0230	M	0,0253	T	0,0925		
G	0,0196	N	0,0709	U	0,0271		

Tabella 2: Distribuzione di probabilità delle lettere in Inglese

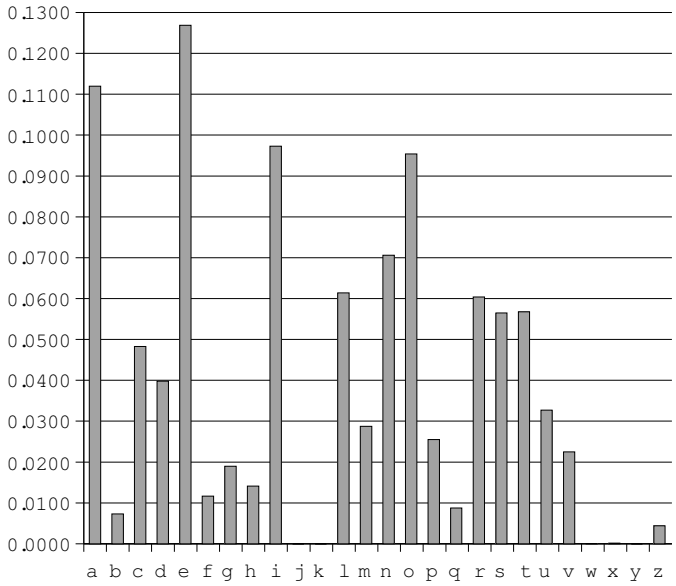

Figura 1: Grafico della distribuzione di probabilità delle lettere in Italiano

Un modello più accurato può essere realizzato considerando il modo in cui, in una certa lingua, una lettera segue un'altra all'interno di una parola. In tal caso lo spazio dei messaggi genera una catena di Markov finita, ossia, una sequenza di variabili casuali $\{X_0, X_1, \ldots, X_{r-1}\}$ tali che la distribuzione di probabilità condizionata X_{s+1}, con $0 \leq s < r$, dipende solo dalla distribuzione di probabilità X_s ed è indipendente dalle distribuzioni di probabilità precedenti. Le probabilità di transizione $\Pr(X_{s+1} = m_i | X_s = m_i) = p_{ij}$ definiscono una matrice di transizione P alla quale resta associato il vettore delle probabilità stazionarie

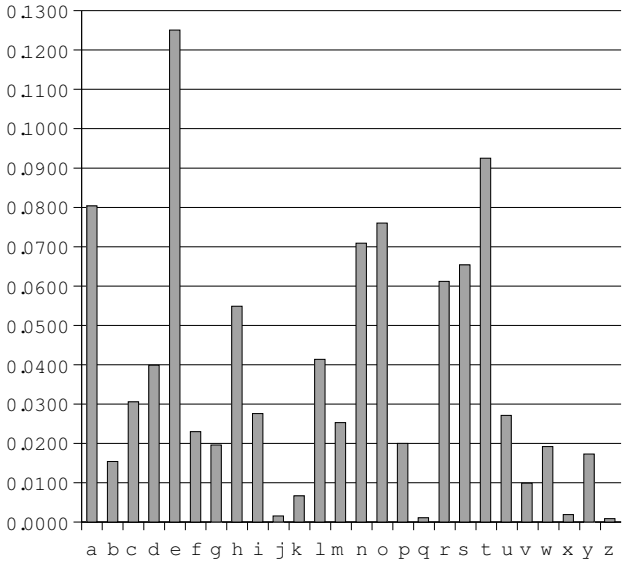

Figura 2: Grafico della distribuzione di probabilità delle lettere in Inglese

$\mathbf{p} = (p(0), p(1), \ldots, p(r-1))$ che si può calcolare risolvendo il sistema

$$\begin{cases} \mathbf{p}P = \mathbf{p} \\ p(i) \geq 0 \qquad \text{per ogni } 0 \leq i < r \\ \sum_{i=0}^{r-1} p(i) = 1 \quad \text{per ogni } 0 \leq i < r. \end{cases}$$

Quindi, per un evento $(m_0, m_1, \ldots, m_{r-1})$ si ha

$$\Pr(m_0, m_1, \ldots, m_{r-1}) = p(0)\Pr(X_1|X_0)\Pr(X_2|X_1)\cdots\Pr(X_{r-1}|X_{r-2}).$$

Una descrizione dettagliata delle catene di Markov esula dallo scopo di queste note; per un ulteriore approfondimento al riguardo si rimanda il lettore ad uno dei molti testi di teoria della probabilità che trattano l'argomento.

La matrice di transizione ed il vettore delle probabilità stazionarie per la lingua Inglese, come per altre lingue, sono stati calcolati e sono ben noti. Per l'Inglese si veda, ad esempio, [vT89, tabelle 1.2 e 1.3]. Utilizzando queste tabelle troviamo $\Pr(\texttt{T}|\texttt{E}) = 0{,}1417$, $\Pr(\texttt{E}|\texttt{T}) = 0{,}0404$, $\Pr(\texttt{E}|\texttt{N}) = 0{,}1381$, $\Pr(\texttt{N}|\texttt{T}) = 0{,}1641$, $\Pr(\texttt{N}|\texttt{E}) = 0{,}1212$, e le componenti del vettore delle probabilità stazionarie relative alle lettere `E`, `N` e `T` che sono, rispettivamente, 0,1566, 0,0814 e 0,0773. Per mezzo

di tali valori possiamo calcolare le seguenti probabilità:

$$\Pr(\texttt{TEN}) = 0{,}0773 \cdot 0{,}1417 \cdot 0{,}1381 \approx 1{,}51 \cdot 10^{-3},$$
$$\Pr(\texttt{NET}) = 0{,}0814 \cdot 0{,}1212 \cdot 0{,}0404 \approx 3{,}98 \cdot 10^{-4},$$
$$\Pr(\texttt{TNE}) = 0{,}1566 \cdot 0{,}0015 \cdot 0{,}1212 \approx 2{,}85 \cdot 10^{-5}.$$

Occorre comunque osservare che nel modello appena descritto la probabilità $\Pr(X_j = m_0, X_{j+1} = m_1, \ldots, X_{j+r-1} = m_{r-1})$ è indipendente da j, ossia dalla posizione di una certa parola all'interno di un testo. Questo in una lingua comune non sempre è vero. Ad esempio, è quasi certo che il testo di una lettera abbia inizio con la parola `CARO` o `CARA`, mentre è assai difficile che inizi con `MARE`, anche se "mare" è una parola molto comune nella lingua Italiana.

I criptosistemi classici

Come accennato nell'introduzione, per criptosistema classico si intende un meccanismo di trasformazione di messaggi finalizzato a rendere l'informazione fruibile solamente da parte di un destinatario prefissato con cui si sono condivisi *a priori* dei segreti. Un tale sistema è finalizzato a garantire la *confidenzialità* dei dati ma fornisce in modo quasi implicito anche una garanzia di *autenticità*: infatti un messaggio può essere cifrato solamente da chi è in possesso del sistema cifrante e questo, a priori, garantisce l'identità del mittente.

Una definizione formale di un tale tipo di criptosistema è la seguente. Consideriamo due insiemi di parole, $\mathcal{M}$ e C, a priori su alfabeti distinti. Essi sono detti rispettivamente *insieme dei messaggi* o dei *testi* e *insieme delle cifre*

Una *trasformazione crittografica* è semplicemente un'applicazione iniettiva

$$\varphi : \mathcal{M} \mapsto C.$$

Come visto in precedenza possiamo sempre supporre che si abbia $\mathcal{M} = \mathbb{Z}_n^k$ e $C = \mathbb{Z}_m^v$. In pratica, nella maggior parte dei casi concreti, $C = \mathcal{M}$.

Un criptosistema classico nella sua forma più generale è un insieme di

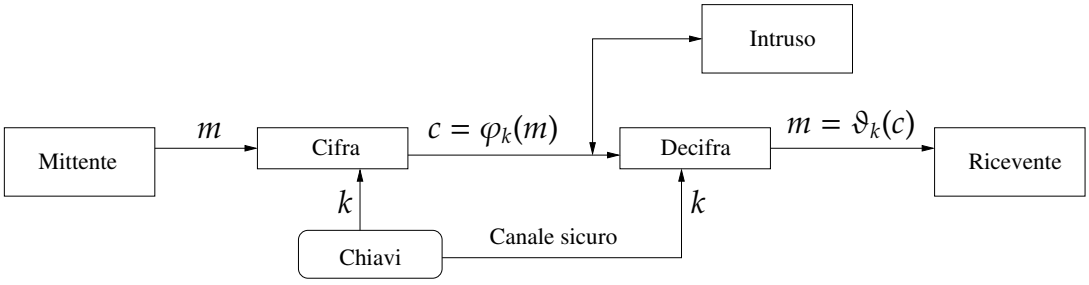

Figura 1: Un criptosistema convenzionale

trasformazioni crittografiche

$$\Phi := \{ \varphi_k \mid k \in \mathcal{K} \},$$

indicizzate dagli elementi in un insieme $\mathcal{K}$, detto *s*pazio delle chiavi.

Dato che per ogni $k \in \Phi$, la funzione φ_k è iniettiva, essa ammette almeno una inversa a sinistra ϑ_k, e dunque abbiamo

$$\vartheta_k(c) = \vartheta_k(\varphi_k(m)) = m$$

per ogni $c \in C$. Uno schema di criptosistema a chiave privata di tal tipo è rappresentato in figura 1.

Da un buon criptosistema ci si aspetta che caloclare $m = \vartheta_k(c)$ a partire dalla sola conoscenza di Φ e del testo cifrato c non sia praticamente fattibile. Tale affermazione euristico è nota sotto il nome di *principio di Kerckhoff*.

Il problema di esprimere in modo quantitativo il comportamento di un criptosistema è legato allo studio delle proprietà di tipo statistico dei messaggi. Seguendo Shannon [Sha49], a tal fine è stata introdotta la nozione di equivocità, una misura di quanto un avversario sia insicuro sul messaggio originale dopo aver intercettato un testo in cifra.

Modelli di attacco

Un metodo per valutare un criptosistema è quello di vedere come esso è in grado di resistere a dei tentativi di forzarlo, in cui si ipotizza che

1. l'avversario possegga delle informazioni parziali sul testo trasmesso;
2. le risorse di calcolo disponibili all'avversario siano quantificabili;
3. il criptosistema sia noto a tutte le persone coinvolte.

Essenzialmente, vengono considerati quattro tipi fondamentali di attacco, in cui si ipotizza ogni volta che l'avversario possegga maggiore controllo sulle apparecchiature di codifica e decodifica:

(1) **Testo cifrato noto**: in questo scenario l'avversario ha intercettato una copia di un messaggio cifrato trasmesso, ma non possiede alcuna altra informazione.

(2) **Testo in chiaro noto**: in questo caso l'avversario conosce la corrispondenza fra un testo in chiaro e un testo cifrato e vuole ricostruire la chiave utilizzata.

(3) **Testo in chiaro assegnato**: l'avversario può codificare uno (e un solo!) testo e vedere come il criptosistema si comporta.

(4) **Testo in chiaro modulato**: l'avversario può effettuare più operazioni di codifica, scegliendo ogni volta il testo in funzione dell'esito delle operazioni precedenti, cercando di scoprire il funzionamento dell'apparecchiatura cifrante.

È bene osservare che le tipologie di attacco (2) e (3) possono essere applicate anche quando solamente una piccola parte del testo in chiaro può essere nota o assegnata. In questi casi si parla di **Testo in chiaro parzialmente noto** e **Testo in chiaro parzialmente assegnato**.

In ogni caso, il modello di attacco adottato dipende strettamente dalle finalità del criptosistema impiegato e dalle intenzioni dell'avversario.

Mostriamo ora alcuni scenari in cui i 4 paradigmi di cui sopra possono essere concretamente applicati:

(1) un attacco in cui si conosce solamente il testo cifrato corrisponde al modello classico di criptosistema: un avversario intercetta una comunicazione apparentemente priva di significato e vuole scoprire che cosa essa significhi;

(2) un esempio di attacco in cui il testo in chiaro è noto è quello che può essere implementato contro sistemi di accesso condizionale ai dati (ad. es. Televisione Digitale). In questo caso, il segnale in ingresso ad un decodificatore è noto, come pure quello in uscita e si vuole scoprire quale chiave è utilizzata per decifrare il flusso di dati;

(3) l'attacco con testo in chiaro assegnato consiste nel verificare mediante una apparecchiatura come un flusso di informazioni venga codificato e cercare di dedurre il comportamento generale; ad esempio si può considerare il caso di un codificatore dotato di un sistema di allarme, per cui esso è in grado di fare solamente una codifica prima di autodistruggersi. Un esempio di sistema di questo genere è quello di protezione di accesso ai dati contenuti su di una smart card;

(4) il paradigma del testo in chiaro assegnato in modo modulato corrisponde alla situazione in cui si ha il massimo controllo sul meccanismo cifrante: è il caso in cui l'apparecchiatura di codifica può essere manipolata a piacere nei dati che vengono inseriti. Un esempio in cui questo è sempre possibile è quello dei criptosistemi implementati in software su di un generico calcolatore elettronico. Tale problema è simile a quello del *reverse engineering*.

Criptosistema di Giulio Cesare

Uno dei più antichi criptosistemi di cui abbiamo notizia è quello detto *di Giulio Cesare.* Si considerano blocchi di lunghezza 1 e si rappresentano le lettere dell'alfabeto latino, compreso lo spazio fra le parole, mediante gli elementi di $\mathbb{Z}_{26}$. Per ogni simbolo m si applica la trasformazione

$$\begin{array}{rccl} \varphi_k : & \mathbb{Z}_{26} & \longrightarrow & \mathbb{Z}_{26} \\ & m & \longmapsto & m + k \pmod{26} \end{array}$$

cosicché, con la chiave $k = 3$, il testo in chiaro `CAESAR` viene trasformato nel testo cifrato `FDHVDU`. In questo caso lo spazio delle chiavi è costituito dall'insieme $K = \{0, 1, 2, \ldots, 24, 25\}$, e si ha $\vartheta_k = \varphi_k^{-1} = \varphi_{26-k}$.

Per un criptanalista è abbastanza facile rompere il criptosistema di Giulio Cesare. Infatti, dato che lo spazio delle chiavi è molto piccolo, la chiave utilizzata può essere determinata per mezzo di una ricerca esaustiva in un tempo estremamente breve. Ad esempio nella tabella 1 è riportata la criptanalisi del testo cifrato `FDHVDU`.

0	FDHVDU	7	MKOCKB	14	TRVJRI	21	AYCQYP
1	GEIWEV	8	NLPDLC	15	USWKSJ	22	BZDRZQ
2	HFJXFW	9	OMQEMD	16	VTXLTK	23	CAESAR
3	IGKYGX	10	PNRFNE	17	WUYMUL	24	DBFTBS
4	JHLZHY	11	QOSGOF	18	XVZNVM	25	ECGUCT
5	KIMAIZ	12	RPTHPG	19	YWAOWN		
6	LJNBJA	13	SQUIQH	20	ZXBPXO		

Tabella 1: Criptanalisi di `FDHVDU` nel criptosistema di Giulio Cesare

Osserviamo che nel caso di un algoritmo di ricerca esaustiva automatizzato è necessario fornire una condizione che consenta di determinare quando si è

ottenuta una decodifica corretta del messaggio. Concretamente, per messaggi formulati in linguaggi naturali tale condizione può essere implementata semplicemente calcolando la frequenza delle singole lettere nel putativo messaggio in chiaro e verificando che tale frequenza coincida effettivamente con quella della lingua stessa. Un metodo ancora più veloce consiste nel calcolare il valore κ_p per i putativi testi decodificati e verificare se esso coincide con quello di una lingua nota.

In effetti, l'idea di utilizzare informazioni frequenziali per identificare le è utilizzata per la crittoanalisi dei sistemi per sostituzione semplice, come sarà visto nel seguente capitolo.

Si mostrerà, in particolare, come il criptosistema di Giulio Cesare non puossa essere reso più robusto semplicemente aumentando le dimensioni dello spazio delle chiavi, ma si rende necessario adottare costruzioni più sofisticate.

Sostituzione semplice

Nel *criptosistema a sostituzione semplice* o *criptosistema a sostituzione monoalfabetica* si considera come spazio delle chiavi l'insieme $K = \mathrm{Sym}(26)$ costituito da tutte le permutazioni su $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$. Si vede immediatamente che il criptosistema di Giulio Cesare è un caso particolare di questo sistema, in cui le chiavi sono limitate alle sole permutazioni della forma

$$(i, i+1, \ldots, i+25),$$

ove gli indici sono da intendersi modulo 26.

L'insieme delle sostituzioni crittografiche risulta dunque

$$\Phi = \{\, \varphi_\pi \mid \pi \in \mathrm{Sym}(26)\},$$

mentre per ogni chiave $\pi \in \mathrm{Sym}(_{26})$ la funzione per decifrare un testo cifrato con φ_π è data da $\vartheta_\pi = \varphi_{\pi^{-1}}$. Dato che $|K| = 26! = 403291461126605635584 \cdot 10^6$, in questo caso una ricerca esaustiva difficilmente può fornire una risposta in tempo utile.

D'altra parte, per forzare questo criptosistema si può tentare con un attacco probabilistico, confrontando la frequenza delle lettere in un testo cifrato con quelle di una tabella di distribuzione simile alle tabele 2,1; in tale modo, si riesce a ricostruire facilmente la chiave. Un diverso approccio è quello di partire dalla conoscenza di parte del messaggio in chiaro (mediante un attacco di tipo testo in chiaro parzialmente noto) e, da questo, ricavare informazioni sulla struttura della permutazione adottata come chiave. In realtà, la quantità di informazione necessaria per rompere un siffatto criptosistema è sorprendentemente poca. Nell'esempio che segue supponiamo di stare analizzando il testo cifrato, composto di 5-blocchi, della tabella 1, di cui sappiamo che riguarda la "teoria della comunicazione".

Possiamo assumere che la parola `COMUNICAZIONE` sia contenuta in un testo simile, cosicché dobbiamo semplicemente cercare una sequenza composta da

WSPBP	ZFKYL	BQXKW	SBQYU	BXSFP	FICFH	FIZIP
PKFZZ	FIFBS	MXIKY	UBXSF	LYWSH	WSZXY	LWSYE
ZIXBE	IBPQG	BXHIB	SQBHY	EFFQG	FBEKE	PPYAA
BXQGF	PBCWX	EFZIY	PKFZZ	FIFCF	SAYYL	YEZFI
YIPBS	FEEYQ	XKWSB	QYUBX	SFQBX	HWXLB	HFSLF
IFPBY	LYIYA	BXSBB	SZIBS	PFQGF	YEKFQ	QYSBP
KXLBZ	IYPKB	PPBXN	FWZBE	BUUYZ	XPBYL	YLBMF
ZZBSF	EPBPZ	FKYBE	BSAWY	AABSY	ZWIYE	BHIFI
FSZYS	XWSYI	FPBPZ	FSUYY	HBQQX	EBFII	XIBLB
ZIYPK	BPPBX	SFBSO	WYSZX	ZFSLX	SXYQX	LBMBQ
YIFOW	YSZXC	BFSFQ	XKWSB	QYZXB	SKXLX	IBLXS
LYSZF	...					

Tabella 1: Testo cifrato con una permutazione di Sym(26)

tredici lettere consecutive in cui la prima lettera è uguale alla settima, la seconda all'undicesima, la quinta alla dodicesima e la sesta alla decima. Scopriamo che una siffatta sequenza compare due volte nel testo ed è `QXKWSBQYUBXSF.` Così facendo ricaviamo la seguente informazione sulla chiave $\pi \in \mathrm{Sym}(26)$:

C	O	M	U	N	I	A	Z	E
↓	↓	↓	↓	↓	↓	↓	↓	↓
Q	X	K	W	S	B	Y	U	F.

Possiamo anche assumere che la parola `TRASMISSIONE` sia contenuta nel testo; quindi dobbiamo cercare sequenze della forma `**Y*KB**BXSF.` Nel testo compare due volte la sequenza `ZIYPKBPPBXSF` da cui ricaviamo:

T	R	S
↓	↓	↓
Z	I	P.

Ora sappiamo che all'inizio del testo deve esserci una frase del tipo `UN SISTEMA *I COMUNI...` da cui, ponendo `D` al posto di `*`, ricaviamo la corrispondenza `D` $\rightarrow$ `L`. procedendo in questo modo alla fine siamo in grado di ricostruire completamente la corrispondenza π:

A	B	C	D	E	F	G	H	I	J	K	L	M
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Y	T	Q	L	F	M	A	G	B	D	R	E	K

```
N  O  P  Q  R  S  T  U  V  W  X  Y  Z
↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓
S  X  H  O  I  P  Z  W  C  V  J  N  U
```

e quindi di decifrare il testo.

A conclusione di questo paragrafo, osserviamo che un criptosistema con poche chiavi possibili è sicuramente facile da rompere; d'altro canto l'avere uno spazio delle chiavi grande è solamente condizione necessaria (ma non sufficiente) per garantire sicurezza.

Criptosistema di Vigenère

Come precedentemente visto, il problema essenziale di un criptosistema a sostituzione monoalfabetica è che le frequenze dei simboli nel testo cifrato coincidono con quelle dei caratteri nel testo in chiaro; questo, nel caso in cui il messaggio in chiaro possegga una qualche struttura riconoscibile, consente di ricostruire facilmente la chiave. Notiamo che, essenzialmente, usare una sostituzione monoalfabetica corrisponde a scrivere i caratteri che formano una parola con simboli diversi da quelli usuali, ma i suoni rimangono sempre i medesimi.

Il criptosistema che tratteremo in questo paragrafo è stato introdotto nel 1586 da B. de Vigenère [dV86] ed è una importante generalizzazione di quello della sezione precedente. Esso viene detto *criptosistema di Vigenère* o *criptosistema per sostituzione polialfabetica* ed è, essenzialmente, realizzato mediante una sequenza di sostituzioni monoalfabetiche applicate periodicamente.

Più precisamente, l'insieme delle trasformazioni crittografiche del criptosistema di Vigenère è

$$\Phi = \{\, \varphi_{(k_0,k_1,\ldots,k_{s-1})} \mid (k_0, k_1, \ldots, k_{s-1}) \in \mathbb{Z}_n^s \,\},$$

ponendo

$$\varphi_{(k_0,k_1,\ldots,k_{s-1})}(m_0, m_1, m_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

con

$$c_t = m_t + k_u \pmod{n}$$

e gli indici u ridotti modulo s.

Ad esempio, usando la consueta rappresentazione dell'alfabeto latino $\mathfrak{A} = \{A, \ldots, Z\}$ per mezzo degli elementi di $\mathbb{Z}_{26}$, prendendo come parola chiave la sequenza `CHIAVE` e sommando lettera per lettera modulo 26, otteniamo la seguente trasformazione:

```
testo in chiaro:   UNCRI PTOSI STEMA COMEQ UESTO NONSE MBRAM OLTOS ...
chiave:            CHIAV ECHIA VECHI AVECH IAVEC HIAVE CHIAV ECHIA ...
testo cifrato:     WUKRD TVWSD NXGTI CJQGX CENXQ UWNNI OIZAH SNAWS ...
```

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tabella 1: Tavola di Vigenère

Un utile strumento per cifrare e decifrare manualmente il criptosistema di Vigenère è costituito dalla *tavola di Vigenère* riportata in tabella 1. Per cifrare, basta scrivere ripetutamente, sotto il testo in chiaro, la parola chiave tante volte quante è necessario ed eventualmente troncando alla fine. Quindi si cerca nella tavola di Vigenère la riga di ciascuna lettera del testo in chiaro e la colonna della relativa lettera della parola chiave. A questo punto la lettera corrispondente nel testo cifrato è quella che si trova nell'intersezione fra riga e colonna. Vice versa, per decifrare si cerca la colonna di ciascuna lettera della parola chiave e si scende fino a trovare la relativa lettera del testo cifrato. La lettera che etichetta la riga trovata è la lettera corrispondente nel testo in chiaro.

La sicurezza di questo tipo di sistema dipende essenzialmente da due fattori:

1. la lunghezza della chiave rispetto quella del testo da cifrare;
2. la mancanza di proprietà statistiche notevoli nella struttura della chiave stessa.

È possibile dimostrare che se la chiave è scelta in modo completamente casuale ed essa è tanto lunga quanto il messaggio che deve essere trasmesso, allora un criptosistema di Vigenère consente di avere *sicurezza perfetta*, nel senso che un qualsivoglia messaggio cifrato intercettato può corrispondere a un qualsiasi messaggio inviato di quella lunghezza. Tale criptosistema è detto *one time pad*.

Solitamente la chiave è più corta del testo da cifrare; essa può addirittura essere una qualche parola o sequenza di senso compiuto nella medesima lingua. In questi casi è possibile forzare il sistema di Vigenère mediante tecniche crittoanalitiche. L'idea base è che, dato un testo abbastanza lungo, la distribuzione di probabilità per ogni s–esimo carattere è la stessa che per la lingua in cui il testo è stato scritto.

La forzatura del sistema viene effettuata in due fasi:

1. determinazione della lunghezza s della chiave adottata;

2. risoluzione di s differenti criptosistemi a sostituzione monoalfabetica.

Per risolvere il secondo punto, si può utilizzare la tecnica vista nel paragrafo precedente. Per determinare la lunghezza della chiave, può essere impiegata la tecnicad etta dell'*incidenza delle coincidenze.* introdotta nel 1863 dall'ufficiale prussiano F. W. Kasiski.

Tale tecnica viene utilizzata per determinare la lunghezza s della chiave adottata, cosicché per rompere il criptosistema basta scomporre il testo cifrato in una sequenza concatenata di s frammenti di testo, ciascuno dei quali risulta essere cifrato, con una chiave distinta, mediante un criptosistema a sostituzione monoalfabetica.

Siano $\mathbf{X}_i = (X_{i,1}, X_{i,2}, \ldots, X_{i,r-1})$, con $i \in \{1, 2\}$, due sequenze di variabili casuali sopra $\mathbb{Z}_n$ indipendenti fra di loro ma identicamente distribuite, cioè:

$$\Pr(X_{i,j} = m) = p(m), \quad i \in \{1, 2\}, \quad 0 \leq j < r.$$

Supponiamo di voler calcolare il numero di coincidenze, definito come

$$\sigma[X_1, X_2] = |\{\, j \mid 0 \leq j < r,\ X_{1,j} = X_{2,j}\}|.$$

Dal calcolo delle probabilità si ha

$$\Pr(X_{1,j} = X_{2,j}) = \sum_{m \in \mathbb{Z}_n} \Pr(X_{1,j} = X_{2,j} = m) = \sum_{m \in \mathbb{Z}_n} p^2(m) = \kappa_p.$$

Sia G adesso un sottoinsieme di $\mathrm{Sym}(n)$ e si consideri una variabile casuale Π sopra G con distribuzione

$$\Pr(\Pi = \pi) = q(\pi).$$

Denotiamo con $Y_1 = (Y_{1,0}, Y_{1,1}, \ldots, Y_{1,r-1})$ e $Y_2 = (Y_{2,0}, Y_{2,1}, \ldots, Y_{2,r-1})$ le immagini di due dati due messaggi X_1, X_2, rispettivamente cifrati, con le sostituzioni semplici π_1 e π_2 in G.

Per $0 \leq j < n$ si ha

$$\Pr(Y_{1,j} = Y_{2,j} = c) = \sum_{\pi \in G} q(\pi) p(\pi^{-1}(c)).$$

A questo punto si devono considerare due casi distinti:

Δ_0 : X_1 ed X_2 sono stati cifrati mediante la stessa sostituzione semplice π con probabilità $q(\pi)$;

Δ_1 : X_1 ed X_2 sono stati cifrati, rispettivamente, mediante due sostituzioni semplici π_1 e π_2, scelte in modo indipendente e con rispettive probabilità $q(\pi_1)$ e $q(\pi_2)$.

Ne consegue

$$\Pr(Y_{1,j} = Y_{2,j} \mid \Delta_0) = \sum_{c \in \mathbb{Z}_n} \Pr(Y_{1j} = Y_{2,j} = c \mid \Delta_0) = \sum_{\pi \in G} \sum_{c \in \mathbb{Z}_n} q(\pi) p^2(\pi^{-1}(c)) = \sum_{\pi \in G} \sum_{m \in \mathbb{Z}_n} q(\pi) p^2(m) = \sum_{m \in \mathbb{Z}_n} p^2(m), \quad (7.1)$$

mentre

$$\Pr(Y_{1,j} = Y_{2,j} \mid \Delta_1) = \sum_{c \in \mathbb{Z}_n} \Pr(Y_{1j} = Y_{2,j} = c \mid \Delta_1) = \sum_{\pi_1, \pi_2 \in G} \sum_{c \in \mathbb{Z}_n} q(\pi_1) q(\pi_2) p(\pi_1^{-1}(c)) p(\pi_2^{-1}(c)) = \sum_{c \in \mathbb{Z}_n} \left(\sum_{\pi_1 \in G} q(\pi_1 p(\pi_1^{-1}(c))) \right) \left(\sum_{\pi_2 \in G} q(\pi_2 p(\pi_2^{-1}(c))) \right) = \sum_{c \in \mathbb{Z}_n} \left(\sum_{\pi \in G} q(\pi) p(\pi^{-1}(c))) \right)^2 = \sum_{c \in \mathbb{Z}_n} \Pr^2(Y = c). \quad (7.2)$$

Utilizzando la matrice di transizione di una certa lingua, la (7.1) fornisce un certo valore δ_0, mentre se prendiamo G come il gruppo composto dalle 26 chiavi del criptosistema di Giulio Cesare, e supponiamo che ciascuna di esse abbia la stessa probabilità di $1/26$, allora la (7.2) restituisce il valore $\delta_1 \approx 0{,}03846$. Ne consegue che il valore atteso per $\sigma[X_1, X_2]$ è $\delta_0 r$ sotto l'ipotesi Δ_0 e $\delta_1 r$ sotto l'ipotesi Δ_1.

Ora, per determinare la lunghezza della chiave usata per cifrare un testo con il criptosistema di Vigenère, poniamo

$$\begin{array}{lccccccc} \text{testo in chiaro:} & m_0 & m_1 & \dots & m_{s-1} & m_s & \dots & m_{r-1} \\ \text{chiave:} & k_0 & k_1 & \dots & k_{s-1} & k_0 & \dots & k_{r-1} \pmod s \\ \text{testo cifrato:} & c_0 & c_1 & \dots & c_{s-1} & c_s & \dots & c_{r-1} \end{array}$$

cosicché per ogni $0 \leq i < r$ si ha

$$c_i = m_i + k_i$$

con gli indici ridotti modulo s. Supponiamo che le componenti $m_i \in \mathbb{Z}_n$ siano valori indipendenti che la variabile casuale X possa assumere con probabilità $p(m_i)$, e che le componenti k_i siano valori indipendenti scelti in G con probabilità $q(k_i)$. Definiamo, inoltre,

$$\begin{aligned} \mathbf{c}^{(v)} &= (c_0, c_1 \dots, c_{r-v-1}), \\ {}^{(v)}\mathbf{c} &= (c_v, c_{v+1}, \dots, c_{r-1}). \end{aligned}$$

Il valore atteso per $\sigma[{}^{(v)}\mathbf{c}, \mathbf{c}^{(v)}]$ fornisce ora un'indicazione per determinare la lunghezza della chiave. Invero, se s è un divisore di v e $0 \leq i < r - v$, allora

$$\Pr({}^{(v)}\mathbf{c} = \mathbf{c}^{(v)}) = \sum_{c \in \mathbb{Z}_n} \Pr(c_i = c_{i+v} = c) = \sum_{\pi \in G} \sum_{c \in \mathbf{Z}_n} q(\pi) p^2(\pi^{-1}(c)) = \sum_{\pi \in G} \sum_{m \in \mathbf{Z}_n} q(\pi) p^2(m) = \sum_{m \in \mathbb{Z}_n} p^2(m),$$

Il seguente teorema è conseguenza di quanto sopra introdotto.

Teorema 1 Il valore più probabile di $\sigma[{}^{(v)}\mathbf{c}, \mathbf{c}^{(v)}]$ è dato da

$$\sigma[{}^{(v)}\mathbf{c}, \mathbf{c}^{(v)}] = \begin{cases} (r-v) \sum_{m \in \mathbb{Z}_n} p^2(m) & \text{se } s \text{ divide } v \\ (r-v) \sum_{c \in \mathbb{Z}_n} \Pr^2(Y = c) & \text{se } s \text{ non divide } v. \end{cases}$$

Utilizzando il teorema 1 si riesce dunque a determinare la lunghezza della parola chiave utilizzata per cifrare un testo, purché esso sia abbastanza lungo e strutturato da rendere attendibile un'analisi probabilistica. Fissato un certo valore τ, ad esempio $\tau = 26$ potrebbe essere una scelta ragionevole, si elencano tutti i valori $\sigma[{}^{(v)}\mathbf{c}, \mathbf{c}^{(v)}]/(r-v)$ che si ottengono per $0 < v < \tau$ e si determina il periodo s con cui i valori più vicini a quello di δ_0 calcolato con la (7.1) compaiono nell'elenco. A questo punto sappiamo che s è la lunghezza più probabile per la chiave.

L'esempio che segue, ancorché breve, fornisce una semplice schematizzazione dell'idea che è alla base della tecnica di Kasiski. Supponiamo di avere intercettato il seguente frammento di testo cifrato, che sappiamo essere stato cifrato con il criptosistema di Vigenère e con una chiave la cui lunghezza s ci accingiamo a determinare.

```
ECQTC GJWDZ GDBOH TCWGA STKGK HDTCW EWHVB ...
```

Cerchiamo tutti i gruppi di due lettere che compaiono più volte nel testo. In questo caso abbiamo tre occorrenze di `TC` alle posizioni 4–5, 16–17, 28–29 e due occorrenze di `CW` alle posizioni 17–18, 29–30. Osserviamo che le coppie `TC` distano fra di loro 12 posizioni, come anche le coppie `CW`. Ne deduciamo che la lunghezza della chiave deve essere 2, 3, 4, 6 oppure 12, cosicché otteniamo una notevole limitazione della scelta.

Ovvialmente il testo analizzato è troppo breve per affermare con certezza che il calcolo è accurato. Infatti, non è detto che tutte le coppie di caratteri che si incontrano vengano dalla stessa duplice sostituzione; potrebbero esserci, casualmente, coppie uguali che vengono da una cifratura diversa. Comunque, in un testo abbastanza lungo, molte coppie coincidenti vengono dalla stessa cifratura e quindi forniscono un'indicazione sufficientemente precisa per dererminare la lunghezza della chiave. In particolare, è molto probabile che questa lunghezza sia il prodotto dei primi che compaiono più frequentemente nelle fattorizzazioni delle distanze fra coppie coincidenti. A questo punto, determinata la lunghezza s della chiave, il criptanalista deve solo scomporre il testo ciclicamente in s sequenze distinte, una lettera ogni s in ciascuna sequenza, e quindi effettuare un'analisi del criptosistema di Giulio Cesare su ognuna di esse. Nel nostro caso la chiave, di lunghezza 6, è `CODICE`; pertanto sono sei le sequenze da analizzare per forzare il criptosistema.

Per concludere questa sezione, osserviamo che tutte le tecniche di crittoanalisi probabilistica mostrate sino ad ora si basano sull'osservazione che per un linguaggio con un alfabeto $\mathfrak{A}$ di n caratteri, il valore κ_p è nettamente superiore a $\frac{1}{n}$. Un metodo per evitare attacchi di tipo probabilistico/frequenziale di tale tipo è quello di uniformare preventivamente le probabilità di occorrenza di ogni singolo simbolo, ad esempio, comprimendo il testo.

Il disco cifrante di Leon Battista Alberti

Il *disco cifrante* fu introdotto nel 1470 da Leon Battista Alberti, filosofo, architetto, musicista, pittore e scultore, nel suo "Modus scribendi in ziferas". In effetti, l'Alberti può essere considerato più un crittonalista ante litteram che un crittografo, dato che a lui sono dovuti i primi studi noti sulla distribuzione delle lettere in un testo in lingua latina.

Il criptosistema ideato da Alberti è basato su di un marchingegno come quello illustrato in figura 1, composto da due dischi di rame in grado di ruotare indipendentemente intorno allo stesso asse. Il disco esterno, detto stabile, è per il testo in chiaro. Esso ha 24 caselle contenenti 20 lettere latine maiuscole, con

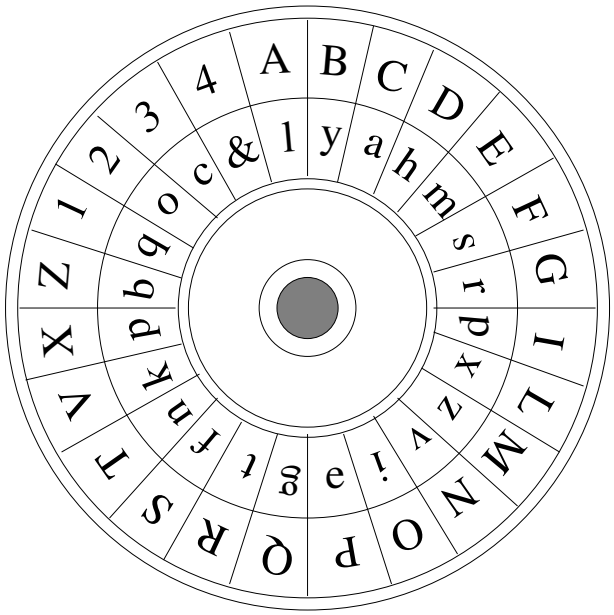

Figura 1: Il disco cifrante di Leon Battista Alberti

l'esclusione di H, K, W, Y, e con U=V ed I=J. Le rimanenti quattro posizioni sono occupate dai numeri 1, 2, 3 e 4. Il disco interno, detto mobile, contiene le 24 lettere latine minuscole per il testo cifrato. Inoltre, mentre le 20 lettere maiuscole sono disposte in ordine alfabetico, le 24 minuscole sono in ordine casuale.

Un tipico utilizzo del disco cifrante di Alberti può essere schenatizzato come segue. Mittente e destinatario sono entrambi dotati dello stesso disco, con le lettere disposte allo stesso modo, e concordano una lettera iniziale come chiave comune. Per crittare un messaggio, il mittente inizia ruotando il disco interno in modo arbitrario; quindi scrive il testo cifrato riportando per prima la lettera sul disco piccolo corrispondente alla chiave concordata che si trova sul disco grande. Quindi esegue la sostituzione del testo prelevando i caratteri sul disco piccolo in corrispondenza dei caratteri da cifrare sul disco più grande. Dopo aver cifrato la prima parola, il mittente ruota di nuovo, in maniera casuale, il disco interno ed inizia a scrivere un'altra parola facendola precedere dalla nuova lettera che corrisponde, sul disco piccolo, alla chiave concordata sul disco grande. Ad esempio, supponiamo di voler cifrare il testo `NEL MEZZO DEL CAMMIN...`, avendo concordato con il destinatario la lettera `Q` come chiave di partenza, e con il disco nella posizione iniziale illustrata in figura 1. All'inizio riportiamo la lettera `g` corrispondente alla chiave iniziale, quindi scriviamo, per la prima parola, `GVMX`. Poi ruotiamo a caso il disco e supponiamo che ora la lettera del disco piccolo corrispondente con la chiave sia la `h`. Ora possiamo scrivere, per la seconda parola del testo cifrato, `H&PZZY`. Ruotiamo di nuovo e, se ora la lettera corrispondente alla chiave è la `r`, scriviamo `RQOY`. Qunidi, se dopo un'altra rotazione abbiamo la lettera `f` in corrispondenza con la chiave, scriviamo `FMAIIZE` cosicché, alla fine, il testo cifrato è `GVMX H&PZZY RQOY FMAIIZE...`

Oltre a quanto visto, Leon Battista Alberti aveva ideato un codice formato da 336 valori, combinando 1, 2, 3 e 4 in gruppi di 2, 3 e 4 cifre. Grazie ai quattro numeri riportati nel disco più grande, era possibile cifrare tale codice rendendolo ancora più sicuro anche se, per l'epoca, garantisse già di per sé una certa sicurezza. Per cifrare questi numeri si utilizzava il disco cifrante con la stessa tecnica già descritta.

Un aspetto particolarmente interessante è che, contrariamente al criptosistema di Vigenère, il criptosistema di Alberti è resistente ad un attacco portato per mezzo di un'analisi probabilistica sulla frequenza delle lettere, che l'Alberti stesso aveva precedentemente studiato. È interessante inoltre notare che il criptosistema basato sul disco cifrante di Alberti non un ebbe successo immediato, per la decisione dell'Alberti stesso di tenerlo segreto. In effetti, il suo trattato di crittografia fu pubblicato a Venezia solo un secolo più tardi.

Il criptosistema di Playfair

Il *criptosistema di Playfair* fu introdotto dal fisico C. Wheatstone, ma prende il nome da L. Playfair che lo divulgò nel 1854. Esso fu utilizzato dagli Inglesi nel corso della prima guerra mondiale. Nel criptosistema di Playfair il testo viene diviso in 2-blocchi, e non si fa distinzione fra le lettere `I` e `J`, cosicché l'alfabeto utilizzato consta solamente di 25 lettere. Queste lettere vengono poi disposte riga per riga in una tabella 5×5, i cui primi elementi sono occupati dalle lettere di una parola chiave, in modo tale che una lettera che vi compare più di una volta viene inserita una volta sola; le rimanenti lettere, invece, sono disposte secondo l'ordine alfabetico naturale. Ad esempio, la parola chiave `LUIGI` dà origine alla seguente tabella per cifrare:

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

Sia $(x, y) = (a_{ij}, a_{mn})$ il 2-blocco composto da a_{ij}, cioè la lettera all'intersezione fra la i-esima riga e la j-esima colonna della tabella per cifrare, ed a_{hl}, la lettera all'intersezione fra l'm-esima riga e l'm-esima colonna. Tale 2 blocco si cifra come segue:

$$\begin{aligned}
(a_{ij}, a_{mn}) &\longmapsto (a_{in}, a_{mj}) && \text{se } i \neq m \text{ e } j \neq n,\\
(a_{ij}, a_{mn}) &\longmapsto (a_{i,j+1}, a_{i,n+1}) && \text{se } i = m \text{ e } j \neq n,\\
(a_{ij}, a_{mn}) &\longmapsto (a_{i+1,j}, a_{m+1,j}) && \text{se } i \neq m \text{ e } j = n,
\end{aligned}$$

in cui gli indici sono ridotti modulo 5. Inoltre, se $x = y$, si inserisce la lettera `Q` fra x ed y e quindi si cifra il nuovo testo contenente $\ldots x\mathtt{Q}y \ldots$ Inoltre, se alla fine si rimane con un numero dispari di lettere nel testo da cifrare, si può aggiungere una qualsiasi lettera diversa dall'ultima in fondo alla sequenza per completare l'ultimo 2-blocco. Ad esempio, con la parola chiave `LUIGI` il testo in chiaro

```
CO MP RE SS O ...
```

viene dapprima trasformato in

```
CO MP RE SQ SO ...
```

e quindi cifrato come

```
FK HR SR TR TN ...
```

Conoscendo la parola chiave, il testo in chiaro si può ricavare immediatamente invertendo il procedimento sugli indici.

Trasposizioni

Un approccio completamente differente è rappresentato dall'uso della cifratura mediante *trasposizione*. In un siffatto criptosistema il testo viene spezzato in k-blocchi e quindi cifrato, blocco per blocco, con una permutazione di Sym(k). Ad esempio, ponendo $k = 7$ e scegliendo la permutazione $(1\,3\,5)(2\,4\,7) \in \mathrm{Sym}(7)$, il testo in chiaro

```
LACRITT OGRAFIA EUNASCI ENZAPOC OESATTA ...
```

viene mutato nel testo cifrato

```
ITLACTR FAOGRIA SIEUNCA PCENZOA TAOESTA ...
```

Si può anche usare una permutazione scelta in un modo particolare. Un esempio è fornito dalla cosiddetta *trasposizione per colonne*, la quale è di natura essenzialmente geometrica. In questo caso il testo viene scritto riga per riga in una matrice $k \times k$, ma poi viene letto colonna per colonna secondo un ordine dipendente da una certa parola chiave. Ad esempio, scegliendo di cifrare mediante una matrice 6×6 con parola chiave `CHIAVE` intendiamo che la prima colonna da trasmettere è la quarta perché la prima lettera in ordine alfabetico che compare in `CHIAVE` è la `A` che si trova in quarta posizione. In questo caso, il testo "la crittografia è una scienza poco esatta perché ci sono molti modi di interpretarla ..." viene ordinato come segue:

416235	416235	416235
LACRIT	ERCHEC	ETARLA
TOGRAF	ISONOM	...
IAEUNA	OLTIMO	
SCIENZ	DIDIVE	
APOCOE	RSIDII	
SATTAP	NTERPR	

e quindi trasmesso come

```
AOACPA  RRUECT  IANNOA  LTISAS  TFAZEP  CGEIOT
RSLIST  HNIIDR  EOMVIP  EIODRN  CMOEIR  COTDIE
  ...     ...     ...     ...     ...     ...
```

Osserviamo che la trasposizione non cambia la frequenza delle lettere in un testo. D'altra parte, contrariamente al criptosistema di Vigenère, in questo caso viene distrutta la logica con cui una certa lettera segue un'altra all'interno di una parola. Per questo motivo la trasposizione è stata utilizzata quasi sempre in associazione con qualche altro criptosistema (ad esempio, quello di Vigenère).

Macchine a rotore

Molti ricorderanno che nei film di spionaggio degli anni '60 uno degli obiettivi tipici degli agenti segreti era quello di impossessarsi di una certa "valigetta nera". Quella valigetta non conteneva altro che la chiave di un criptosistema usato per proteggere dati strategici da cui dipendeva la sicurezza (o l'insicurezza, a seconda dei punti di vista...) del mondo civile. Più precisamente, nella valigetta poteva esserci un rotore simile a quello schematizzato in figura 2. Esistono diverse varianti di criptosistemi basati su rotori. La più famosa era probabilmente quella basata sulla macchina enigma, inventata originariamente nel 1918 a Berlino da Arthur Scherbius ed utilizzata, dopo notevoli perfezionamenti, dai

http://www.impan.gov.pl/Great/Rejewski/article.html

Figura 1: La macchina enigma

Tedeschi durante la seconda guerra mondiale.

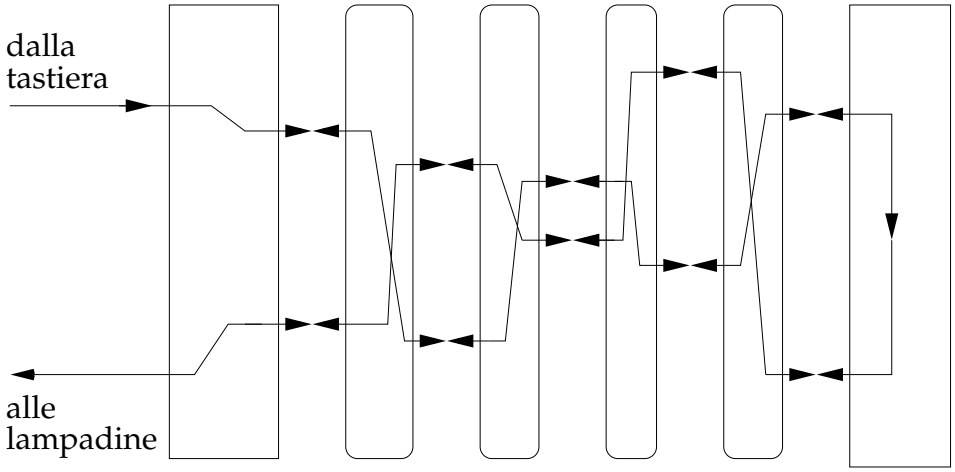

Figura 2: Schema di funzionamento di una macchina enigma

Una macchina enigma è composta essenzialmente da una valigetta contenente una tastiera, due ruote fisse (gli statori), tre ruote mobili (i rotori) comprese fra i due statori, ed una serie di 26 lampadine corrispondenti alle lettere dell'alfabeto latino. I rotori e gli statori hanno vari punti di ingresso e di uscita della corrente, ed in corrispondenza di questi hanno dei contatti elettrici sistemati in modo tale che in ogni momento ciascuno dei contatti di una ruota sia collegato con uno ed un solo contatto di ogni ruota contigua. Inoltre le ruote sono cablate internamente in modo irregolare, cosicché una corrente che entra in una di esse ne esce "altrove" in modo pressoché casuale, vedi figura 2. Oltre ai rotori, per estendere quanto più possibile la scelta delle chiavi di cifatura, la valigetta contiene un circuito elettrico il quale, mediante un sistema di cavetti mobili, permette di scambiare un certo numero di lettere prima di avviarle ai rotori.

Ora, premendo un tasto sulla tastiera, una corrente passa verso lo statore di sinistra. Da questo statore la corrente passa al primo rotore, al secondo, al terzo, quindi arriva allo statore di destra, detto anche ruota di riflessione. Da qui la corrente torna indietro, percorrendo di nuovo i tre rotori, verso il primo statore e quindi verso il pannello con le lampadine. L'effetto della pressione di un tasto sulla tastiera consiste nell'accensione di una lampadina corrispondente ad una lettera dell'alfabeto: questa è la lettera del testo cifrato corrispondente alla lettera del testo in chiaro.

Il movimento dei rotori all'interno della macchina è fondamentale: ad ogni pressione di tasto, il primo rotore scatta di una posizione. Questo significa che premendo di nuovo la stessa lettera, la cifratura non è più la stessa. Il primo rotore funge quindi da chiave di cifratura con lunghezza 26 caratteri, che si ripete

ciclicamente per tutto il messaggio. Al completamento di un giro del primo rotore, il secondo rotore scatta di una posizione e dopo un giro completo del secondo rotore, segue uno scatto del terzo, dando così luogo ad una chiave di crittazione lunga 17576 caratteri, sufficienti per rendere la cifratura simile all'utilizzo della chiave monouso con tutti i testi non più lunghi di questo valore. In realtà, la scelta delle chiavi è molto più estesa. Il pannello elettrico, ad esempio, permette di scambiare fra loro sei, otto o anche dieci coppie di lettere e, tenuto conto del numero di possibili accoppiamenti di ventisei lettere, estende notevolmente il numero di scelte per la chiave. In pratica, una chiave di enigma viene definita per mezzo dei seguenti parametri:

- la scelta e la disposizione dei tre rotori fra i due statori;
- la posizione iniziale dei rotori;
- una certa permutazione iniziale dell'alfabeto ottenuta per mezzo del circuito con i cavetti mobili.

Considerando che i rotori, ciascuno con una propria circuiteria interna, venivano generalmente scelti in un gruppo di sei, e che il circuito a cavetti mobili poteva essere utilizzato per effettuare fino a dieci sostituzioni alfabetiche preliminari, si ottengono, per la scelta della chiave, un numero di combinazioni di ordine superiore a 10^{20},

L'elemento strutturale che forniva grande flessibilità d'uso a Enigma, ma che allo stesso tempo costituiva un elemento di debolezza, era costituito dal fatto che i due testi, quello in chiaro e quello cifrato, erano ottenibili l'uno dall'altro allo stesso modo; cioè, con due applicazioni la macchina enigma forniva l'identità. L'utilità di un siffatto sistema nell'uso pratico è evidente: per leggere il messaggio, il legittimo destinatario, che aveva predisposto una macchina uguale a quella cifrante e nelle stesse condizioni iniziali, non doveva far altro che digitare il testo cifrato per ricostruire il testo in chiaro sul visore.

Nonostante l'apparente inviolabilità, alla fine il criptosistema enigma fu rotto. Varie furono le ragioni che condussero gli Alleati a questo risultato. Innanzitutto, i Tedeschi si abbandonarono incautamente ad un certo senso di sicurezza, probabilmente utilizzando molte volte le stesse combinazioni, e quindi fornendo informazioni preziose ai criptanalisti. Ad esempio, la posizione iniziale dei rotori veniva cambiata ogni ventiquattro ore secondo una regola prefissata, cosicché questa regola finiva per essere la vera chiave; questo introduceva già di per sé un notevole elemento di debolezza. Un altro elemento di debolezza strutturale di enigma era, come già detto, insito nella sua struttura simmetrica: dal punto di vista della teoria dei gruppi, ad esempio, ciò significa che la sostituzione complessiva ottenuta è semplicemente un prodotto di scambi.

Il primi a rompere il criptosistema enigma nella sua versione più semplice furono, negli anni '30, i Polacchi grazie al lavoro di un gruppo di matematici guidato da Marian Rejewski [Rej80]. Successivamente, anche gli Inglesi riuscirono nell'intento di rompere il criptosistema enigma basato sulla macchina più avanzata allora disponibile. Tale risultato fu raggiunto, oltre che con le informazioni passate dai Polacchi, grazie al matematico Alan Touring ed all'uso dei Colossi, i precursori dei moderni computer. Molti dettagli sulle tecniche di decifrazione utilizzate all'epoca sono ancora tenuti segreti. Per aver un'idea un po' più precisa su come il criptosistema enigma fu rotto si può consultare [Kon81, cap. 5].

Una variante un po' più sofisticata di enigma è la macchina ideata dallo svedese Boris Caesar Wilhelm Hagelin alla fine degli anni '30, detta CSP-1500, ed adottata dall'U.S. Army con la denominazione M-209 durante gli anni '40.

Nella macchina di Hagelin sono presenti 6 rotori aventi, rispettivamente, 26, 25, 23, 21, 19 e 17 contatti. Una volta che una lettera è stata cifrata—a seconda della mutua posizione dei contatti dei rotori—i sei rotori si muovono di una posizione. Ne consegue che il primo rotore torna alla posizione iniziale dopo 26 lettere cifrate. Ora, dato che ciascuno dei rotori ha un numero di contatti primo con gli altri, in pratica il criptosistema basato sulla macchina di Hagelin può venire riguardato come un criptosistema di Vigenère di periodo $26 \cdot 25 \cdot 23 \cdot 21 \cdot 17 = 101405850$. Anche il criptosistema basato sulla macchina di Hagelin è stato rotto. Il lettore interessato può consultare [BP82, §23] al riguardo.

Sostituzioni e trasposizioni

In questo paragrafo conclusivo si riassumono in modo formale le metodologie per costruire un sistema di trasformazioni crittografiche che agisca su blocchi di testo.

Trasposizioni

Sia dato un blocco di lunghezza n sull'alfabeto $\mathfrak{A}$, e consideriamo come insieme dei messaggi $\mathcal{M} \subseteq \mathfrak{A}^n$.

Una trasposizione è semplicemente un elemento del gruppo simmetrico S_n, che agisce sugli indici corrispondenti ai singoli simboli in una parola. Le seguenti due definizioni formalizzano tale nozione.

Definizione 1 Sia $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ una parola di lunghezza n. Una parola $\mathbf{c}' = (c'_1, c'_2, \ldots, c'_n)$ è *ottenuta per trasposizione* da $\mathbf{c}$ se esiste $\sigma \in S_n$ tale che per ogni i con $1 \leq i \leq n$,

$$c'_i = c_{\sigma(i)}.$$

In tale caso, scriveremo $\mathbf{c}' = \mathbf{c}^\sigma$.

Definizione 2 Sia $\mathcal{M}$ un insieme di parole di lunghezza n e $\sigma \in S_n$ una permutazione sull'insieme degli indici $I = \{1, 2, \ldots, n\}$. L'*insieme trasposto* $\mathcal{M}^\sigma$ è

$$\mathcal{M}^\sigma = \{\, \mathbf{c}^\sigma : \mathbf{c} \in \mathcal{M} \,\}.$$

L'insieme di tutte le trasposizioni su $\mathfrak{A}^n$ è chiaramente il gruppo simmetrico S_n.

Sostituzioni

La nozione di sostituzione è leggermente più difficile da scrivere formalmente. Infatti, una sostituzione corrisponde ad assegnare una biiezione $\mathfrak{A} \mapsto \mathfrak{A}$ (possibilmente diversa) per ogni posizione in una parola.

Definizione 3 Sia $\mathfrak{A}$ un alfabeto e n un intero. Una qualsiasi funzione da $\alpha : \{1, 2, \ldots, n\} \mapsto \mathrm{Sym}(\mathfrak{A})$ è detta *sostituzione (monoalfabetica)* di $\mathfrak{A}$ per parole di lunghezza n.

Il prodotto di due sostituzioni α, β per parole di lunghezza n è definito come la sostituzione γ tale che

$$\gamma(x) = \alpha(x)\beta(x),$$

per ogni $x \in \{1, 2, \ldots, n\}$. È immediato vedere che l'insieme $\Gamma_n(\mathfrak{A})$ di tutte le sostituzioni per parole di lunghezza n, dotato di questa operazione di prodotto, è un gruppo. Per semplificare la notazione, indicheremo con α_i la permutazione $\alpha(i)$. Al fine di caratterizzare la struttura del gruppo $\Gamma_n(\mathfrak{A})$, consideriamo l'azione di una sostituzione sulle singole posizioni di una parola.

Definizione 4 Per ogni $\vartheta \in \mathrm{Sym}(\mathfrak{A})$ sia

$$(\vartheta, i)(j) = \begin{cases} \vartheta & \text{se } i = j \\ 1 & \text{se } i \neq j. \end{cases}$$

La sostituzione (ϑ, i) è detta *sostituzione indotta da ϑ nella i–esima componente*.

Notiamo che l'insieme

$$\Gamma_n^i(\mathfrak{A}) := \{ (\vartheta, i) : \vartheta \in \mathrm{Sym}(\mathfrak{A}) \}$$

è un gruppo isomorfo a $\mathrm{Sym}(\mathfrak{A})$. Indicata con 1 l'identità di $\Gamma_n(\mathfrak{A})$, è immediato verificare che $\Gamma_n^i(\mathfrak{A}) \cap \Gamma_n^j(\mathfrak{A}) = \{1\}$ ogni qual volta $i \neq j$. D'altro canto, per ogni $\alpha \in \Gamma_n(\mathfrak{A})$,

$$\alpha = \prod_{i=1}^{n} (\alpha_i, i), \qquad (\alpha_i, i) \in \Gamma_n^i(\mathfrak{A})$$

e dati $(\alpha_i, i) \in \Gamma_n^i$, $(\alpha_j, j) \in \Gamma_n^j$ con $i \neq j$ si ha

$$(\alpha_i, i)(\alpha_j, j) = (\alpha_j, j)(\alpha_i, i).$$

Ne segue che

$$\Gamma_n(\mathfrak{A}) = \prod_{i=1}^{n} \Gamma_n^i(\mathfrak{A})$$

è isomorfo al prodotto diretto di n copie di $\mathrm{Sym}(\mathfrak{A})$.

Introdotta la nozione di sostituzione, è possibile mostrare come essa agisce sulle parole di $\mathcal{M}$.

Definizione 5 Sia $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ una parola di lunghezza n sull'alfabeto $\mathfrak{A}$ e sia $\alpha \in \Gamma_n(\mathfrak{A})$. La parola

$$\mathbf{c}_\alpha = (\alpha_1(c_1), \alpha_2(c_2), \ldots, \alpha_n(c_n))$$

è *ottenuta mediante la sostituzione* α da $\mathbf{c}$. Dato un insieme di messaggi $\mathcal{M}$ di lunghezza n e una sostituzione $\alpha \in \Gamma_n(\mathfrak{A})$, l'*insieme ottenuto per la sostituzione* α è

$$\mathcal{M}_\alpha = \{\, \mathbf{c}_\alpha : \mathbf{c} \in \mathcal{M} \,\}.$$

Una fondamentale proprietà del gruppo delle sostituzioni su $\mathfrak{A}^n$ è espressa nel seguente teorema.

Teorema 2 Il gruppo $\Gamma_n(\mathfrak{A})$ è transitivo sull'insieme $\mathfrak{A}^n$.

In particolare, date due qualsiasi parole di lunghezza n esiste sempre una sostituzione che trasforma l'una nell'altra.

Bibliografia

[ARS78] L. M. Adleman, R. L. Rivest, and A. Shamir. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[BB96] L. Berardi and A. Beutelspacher. *Crittologia*. Collana Quaderni di Informatica. Angeli, 1996.

[Beu94] A. Beutelspacher. *Cryptology*. The Mathematical Association of America, 1994.

[BL96] D. Boneh and R. J. Lipton. Algorithms for black-box fields and their application to cryptography. In *Advances in cryptology—CRYPTO '96 (Santa Barbara, CA)*, volume 1109 of *Lecture Notes in Comput. Sci.*, pages 283–297. Springer, Berlin, 1996.

[BLS+83] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckermann, and S. S. Wagstaff Jr. *Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*. AMS, Providence RI, 1983.

[BN58] J. Bretagnolle Nathan. Cubiques définies sur un corps de caractéristique quelconque. *Ann. Fac. Sci. Toulouse*, 22:175–234, 1958.

[BP82] H. Beker and F. Piper. *Cypher Systems, The Protection of Communications*. Northwood Books, London, 1982.

[BS66] Z. I. Borevich and I. R. Shafarevich. *Number Theory*, volume 20 of *Pure and Applied Mathematics*. Academic Press, New York, London, 1966.

[Can87] D. Cantor. Computing in the jacobian of a hyperelliptic curve. *Math. Comp.*, 48:95–101, 1987.

[Del74] P. Deligne. La conjecture de Weil. *Inst. Hautes Etudes Sci. Publ. Math.*, 43:273–307, 1974.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, 22:644–654, 1976.

[dV86] B. de Vigenère. *Traicté des Chiffres, ou Secrètes Manières d'Escrire*. A. L'Angelier, Paris, 1586.

[ElG85] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, pages 469–472, 1985.

[Ful69] W. Fulton. *Algebraic Curves*. Benjamin, New York, 1969.

[GM86] R. Gupta and M. R. P. Murty. Primitive points on elliptic curves. *Compositio Math.*, 58:13–44, 1986.

[Her82] I. N. Herstein. *Algebra*. Editori Riuniti, 1982.

[Hir80] J. W. P. Hirschfeld. Sulle varietà algebriche negli spazi proiettivi finiti, 1980. Quaderni Seminario di Geometrie Combinatorie N. 27, Dip. Mat. Univ. di Roma "La Sapienza".

[Hir83] J. W. P. Hirschfeld. The Weil conjecture in finite geometry. In *Proc. of Australian Combinatorial Conference, Adelaide*, volume 1036 of *Lecture Notes in Mathematics*. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1983.

[Hir98] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields, 2nd edition*. Oxford University Press, Oxford, 1998.

[Hus87] D. Husemöller. *Elliptic Curves*. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1987.

[HW60] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Clarendon, Oxford, 1960.

[Kob84] N. Koblitz. *An Introduction to Elliptic Curves and Modular Forms*. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1984.

[Kob87a] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1987.

[Kob87b] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.

[Kob88] N. Koblitz. Primality of the number of points on an elliptic curve. *Pacific J. Math.*, 131:157–165, 1988.

[Kob89] N. Koblitz. Hyperelliptic cryptosystems. *J. of Cryptology*, 1:139–150, 1989.

[Kob98] N. Koblitz. *Algebraic Aspects of Cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1998.

[Kon81] A. G. Konheim. *Cryptography, a primer*. John Wiley & Sons, New York, Chichester, Brisbane, 1981.

[Lan58] S. Lang. *Introduction to Algebraic Geometry*. Interscience, New York, 1958.

[Lan78] S. Lang. *Elliptic Curves: Diophantine Analysis*. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1978.

[Le65] S. Lang and J. T. Tate (eds.). *The Collected Papers of Emil Artin*. Addison Wesley, Reading MA, 1965.

[Len86] H. W. Lenstra Jr. Elliptic curves and number-theoretic algorithms. Report 86-19 Math. Inst. Universiteit Amsterdam, 1986.

[Len87] H. W. Lenstra Jr. Factoring integers with elliptic curves. *Ann. Math.*, 126:649–673, 1987.

[LN83] R. Lidl and H. Niederreiter. *Finite Fields*. Addison Wesley, Reading MA, 1983.

[LN86] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, 1986.

[LT87] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Amer. Math. Soc.*, 83:289–292, 1987.

[Mas83] J. L. Massey. Logarithms in finite cyclic groups—cryptographic issues. In *Proc. 4th Benelux Symposium on Information Theory*, pages 17–25, 1983.

[Mil85] V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology—Crypto '85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1985.

[MLB78] S. Mac Lane and G. Birkhoff. *Algebra*. Mursia, 1978.

[Mur83] M. R. P. Murty. On Artin's conjecture. *J. Number Theory*, 16:147–168, 1983.

[MV90a] A. Menezes and S. Vanstone. The implementation of elliptic curve cryptosystems. In *Advances in cryptology—AUSCRYPT '90 (Sydney, 1990)*, volume 453. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1990.

[MV90b] A. Menezes and S. Vanstone. Isomorphism classes of elliptic curves over finite fields of characteristic 2. *Utilitas Math.*, 38:135–153, 1990.

[MV90c] A. Menezes and S. Vanstone. Isomorphism classes of elliptic curves over finite fields. Research Report CORR 90–1, Department of Combinatorics and Optimization, University of Waterloo, January 1990.

[MV93] A. Menezes and S. Vanstone. Elliptic curve cryptosystems and their implementation. *J. Cryptology*, 6:209–224, 1993.

[MVZ93] A. Menezes, S. Vanstone, and R. Zuccherato. Counting points on elliptic curves over $\mathbf{f}_{2^m}$. *Math. Comp.*, 60:407–420, 1993.

[NZ80] I. Niven and H. S. Zuckerman. *An introduction to the theory of numbers, fourth edition*. John Wiley & Sons, New York, Chichester, Brisbane, 1980.

[Odl85] A. M. Odlyzko. Discrete logarithms and their cryptographic significance. In *Advances in Cryptography: Proc. of Eurocrypt '84*, volume 209 of *Lecture Notes in Computer Science*, pages 224–314. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1985.

[Pol74] J. M. Pollard. Theorems on factorization and primality testing. *Proc. Cambridge Phil. Soc.*, 76:521–528, 1974.

[Rej80] M. Rejewski. An application of the theory of permutations in breaking the enigma cipher. *Applicationes Mathematicae*, 16(4), 1980.

[Riv85] R. L. Rivest. Advances in cryptology. In *Advances in Cryptography: Proc. of Eurocrypt '84*, volume 209 of *Lecture Notes in Computer Science*, pages 159–165. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1985.

[Sch85] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod. p. *Math. Comp.*, 44:483–494, 1985.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949.

[Sil86] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer Verlag, Berlin, Heidelberg, New York, Tokio, 1986.

[SW79] E. Seah and H. C. Williams. Some primes of the form $(a^n - 1)/(a - 1)$. *Math Comp.*, 33:1337–1342, 1979.

[vT89] H. C. A. van Tilborg. *An Introduction to Cryptology*. Kluwer Academic Publishers, Boston, 1989.

[WW84] P. K. S. Wah and M. Z. Wang. Realization and application of the massey-omura lock. In *Proc. International Zürich Seminar*, pages 175–182, 1984.