1 Crittosistemi Classici

1.1 Cifrari a blocchi

L'obiettivo della **Crittografia** è permettere a due utenti A e B di comunicare attraverso un canale insicuro, senza che un terzo utente non autorizzato riesca a capire l'oggetto della loro comunicazione.

Per fare ciò, A cifra il messaggio in modo tale che solo il destinatario prestabilito B possa invertire la procedura di cifratura e ricavare il messaggio originario.

Queste idee sono descritte in modo funzionale nella seguente definizione.

Definizione 1.1. (Crittosistema).
Una quintupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ di insiemi finiti e non vuoti tali che per ogni $K \in \mathcal{K}$ esistono $e_K \in \mathcal{E}$ e $d_K \in \mathcal{D}$ dove $e_K : \mathcal{P} \to \mathcal{C}$ e $d_K : \mathcal{C} \to \mathcal{P}$ e $d_K \circ e_K = Id_{\mathcal{P}}$, si dice **cifrario a blocchi**.

- $\mathcal{P}$ è l'insieme delle **unità dei messaggi in chiaro**;
- $\mathcal{C}$ è l'insieme delle **unità dei messaggi cifrati**;
- $\mathcal{K}$ è l'insieme delle **chiavi**.

Definizione 1.2. Un crittosistema si dice **endomorfico** se $\mathcal{P} = \mathcal{C}$.

La proprietà principale è $d_K \circ e_K = Id_{\mathcal{P}}$, ovvero l'**iniettività** della funzione e_K. Essa è importante al fine di evitare ambiguità nella decifratura di un messaggio. In particolare, se il sistema è endomorfico, allora e_K è una permutazione di $\mathcal{P}$.

Il mittente A del messaggio, e B, il destinatario, impiegano il seguente protocollo per usare uno specifico crittosistema:

- A e B scelgono una chiave $K \in \mathcal{K}$. Lo scambio della chiave deve avvenire attraverso un canale sicuro;
- Si supponga che A voglia mandare il messaggio in chiaro $X = x_1 x_2 ... x_n$, dove $x_i \in \mathcal{P}$, $i = 1, 2, ...n$, attraverso un canale di comunicazione insicuro; quindi A opera come segue: per $i = 1, ..., n$ calcola $y_i = e_K(x_i) \in \mathcal{C}$, con e_K algoritmo di cifratura, e trasmette $Y = y_1 ... y_n$. Un terzo individuo (l'attaccante) legge il messaggio cifrato e tenta di trovare il presunto messaggio in chiaro X' e la presunta chiave K';
- B riceve Y e per $i = 1, ...n$ calcola $x_i = d_K(y_i)$, con d_K algoritmo di decifratura, e quindi ottiene il messaggio in chiaro X.

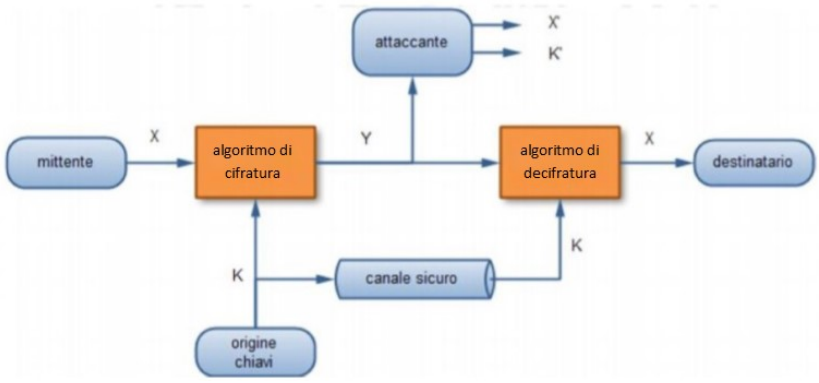

Figura 1.1: Funzionamento del protocollo di un crittosistema.

All'interno dei cifrari a blocchi distinguiamo quelli la cui chiave consta di un solo carattere, detti **monoalfabetici**, e quelli che hanno chiave composta da almeno 2 caratteri, detti **polialfabetici**.

Di seguito sono riportati alcuni cifrari classici e le loro proprietà.

1.2 Cifrario mediante sostituzione

Definizione 1.3. **(Cifrario mediante sostituzione).**
Siano $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$ e siano

$$e_K(x) = (x + K) \ mod \ 26$$
$$d_K(y) = (y - K) \ mod \ 26$$

con $x, y \in \mathbb{Z}_{26}$.

Un esempio di cifrario mediante sostituzione è il **cifrario di Cesare**. Esso prende il nome da Gaio Giulio Cesare, che lo utilizzava per proteggere i suoi messaggi segreti.
Grazie allo storico Svetonio sappiamo che Cesare utilizzava in genere una chiave di 3 per il cifrario, cioè ogni lettera viene sostituita con quella posizionata nell'alfabeto tre posti in avanti.
L'imperatore romano, in realtà, utilizzò l'alfabeto latino, ovvero $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{21}$ con $e_3(x) = (x + 3) \ mod \ 21$ e $d_3(y) = (y - 3) \ mod \ 21$.

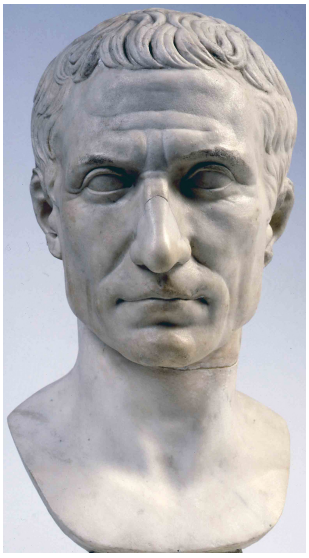

Figura 1.2: Gaio Giulio Cesare (101 a.C. – 44 a.C.)

$\mathcal{P}$	A	B	C	D	E	F	G	H	I	J	K	L	M
$\mathcal{C}$	D	E	F	G	H	I	J	K	L	M	N	O	P

$\mathcal{P}$	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\mathcal{C}$	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Si veda come esempio la cifratura del testo **venividivici**. Si assegna ad ogni lettera un valore numerico: ad A viene associato 0 fino a Z a cui viene associato 25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Sostituire una lettera con quella che si trova tre posti più avanti significa sommare il valore numerico associato alla lettera a 3 e poi ridurre modulo 26.
Pertanto il messaggio **venividivici** corrisponde a 21 4 13 8 21 8 3 8 21 8 2 8 che cifrato risulta 24 7 16 11 24 11 6 11 24 11 5 11, ovvero convertendo i numeri nuovamente in lettere si ha **YHQLYLQGYLFL**.

1.3 Cifrario Affine

Il cifrario mediante sostituzione è un particolare caso di cifrario affine, dove le chiavi possibili sono 26. In generale, il cifrario affine è definito come segue:

Definizione 1.4. **(Cifrario affine).**
Siano $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ e $\mathcal{K} = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : mcd(a,26) = 1\}$. Se $K = (a,b) \in \mathcal{K}$, siccome $mcd(a,26) = 1$ quindi a è invertibile in $\mathbb{Z}_{26}$, allora

$$e_K(x) = (ax + b) \ mod \ 26$$
$$d_K(y) = a^{-1}(y - b) \ mod \ 26$$

con $x, y \in \mathbb{Z}_{26}$.

Si noti che

$$| \mathcal{K} | = 26 \cdot \varphi(26) = 26 \cdot 12 = 312,$$

dove φ denota la phi di Eulero.

Di seguito viene fornito un esempio di cifrario affine. Se $K = (7,3)$, sapendo che $(7^{-1}) \ mod \ 26 = 15$, allora

$$e_K(x) = (7x + 3) \quad mod \ 26$$
$$d_K(x) = (15y - 19) \quad mod \ 26$$

Si consideri come testo da cifrare **ciao**, che corrisponde a 2 8 0 14.
Cifrando si ha:

$$(7 \cdot 2 + 3) \ mod \ 26 = 17 \ mod \ 26 = 17$$
$$(7 \cdot 8 + 3) \ mod \ 26 = 59 \ mod \ 26 = 7$$
$$(7 \cdot 0 + 3) \ mod \ 26 = 3 \ mod \ 26 = 3$$
$$(7 \cdot 14 + 3) \ mod \ 26 = 101 \ mod \ 26 = 23.$$

Quindi il messaggio cifrato è **MHDX**. Applicando la funzione di decifratura si ottiene:

$$(15 \cdot 17 - 19) \ mod \ 26 = 236 \ mod \ 26 = 2$$
$$(15 \cdot 7 - 19) \ mod \ 26 = 86 \ mod \ 26 = 8$$
$$(15 \cdot 3 - 19) \ mod \ 26 = 26 \ mod \ 26 = 0$$
$$(15 \cdot 23 - 19) \ mod \ 26 = 326 \ mod \ 26 = 14,$$

che risulta essere proprio il messaggio in chiaro di partenza.

1.4 Cifrario mediante permutazione

Il cifrario mediante permutazione permette di aumentare la cardinalità dell'insieme delle chiavi, quindi la sicurezza, poiché la funzione di cifratura non è necessariamente un'applicazione affine, ma bensì una permutazione.

Definizione 1.5. (Cifrario mediante permutazione).
Sia $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ e $\mathcal{K} = Sym(26)$. Per ogni permutazione $\pi \in K$ siano

$$e_K(x) = \pi(x)$$
$$d_K(x) = \pi^{-1}(x)$$

con π^{-1} l'inversa di π.

Nel cifrario mediante permutazione è più comodo utilizzare direttamente le lettere piuttosto che convertirle nel loro valore numerico.
La chiave di un cifrario di permutazione consiste in una permutazione dei 26 caratteri. Pertanto

$$|\mathcal{K}| = |Sym(26)| = 26! = 4.0329146 \cdot 10^{26},$$

un numero molto elevato anche per un computer.

Si consideri il seguente esempio: sia

$$\pi = (0\ 15)(1\ 3\ 11\ 25\ 14\ 23\ 9\ 10\ 4\ 5\ 6\ 20\ 7\ 17\ 19\ 2\ 16\ 8\ 13\ 18\ 12\ 21\ 24\ 22)$$

la chiave del cifrario e sia **Ho bisogno di aiuto**, cioè **hobisognodiaiuto**, il testo in chiaro. Ciò numericamente è descritto come

$$7\ 14\ 1\ 8\ 18\ 14\ 6\ 13\ 14\ 3\ 8\ 0\ 8\ 20\ 19\ 14$$

che, attraverso la permutazione π, è cifrato in

$$17\ 23\ 3\ 13\ 12\ 23\ 20\ 18\ 23\ 11\ 13\ 15\ 13\ 7\ 2\ 23$$

cioè in **RXDNMXUSXLNPNHCX**.

1.5 Cifrario di Vigenère

Nel 1586 un diplomatico, traduttore e alchimista francese di nome Blaise de Vigenère rese pubblico un primo esempio di cifrario polialfabetico.

Figura 1.3: Blaise de Vigenère (1523 – 1596)

Il principale punto di forza di questo metodo è l'utilizzo non di uno ma di ben 26 alfabeti (pari al numero delle lettere dell'alfabeto inglese) per cifrare un solo messaggio. Il metodo si può quindi considerare una generalizzazione del cifrario di Cesare.
L'idea è piuttosto semplice: invece di spostare sempre dello stesso numero di posti la lettera da cifrare, come accade nel cifrario di Cesare, questa viene spostata di un numero di posti variabile, determinato in base a una parola chiave da concordarsi tra mittente e destinatario.
Per rendere più semplice il processo di cifratura, Vigenére propose l'utilizzo della **Tabella 1** composta da alfabeti ordinati e traslati.

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

Tabella 1: Tavola di Vigenère.

Il seguente esempio e la **Tabella 1** permettono di capire il funzionamento del cifrario di Vigènere.

Si consideri un messaggio del tipo **Tu non puoi passare**, quindi si ha **tunonpuoipassare**, con la parola chiave **ISUFI**. Per cifrare la prima lettera **T** con la corrispondente lettera della chiave (in questo caso **I**) si individua l'elemento posizionato nella colonna **T** e riga **I**, che è proprio **B**.

Numericamente il messaggio precedente corrisponde a

19 20 13 14 13 15 20 14 8 15 0 18 18 0 17 4

e la parola chiave corrisponde a 8 18 20 5 8. Si ripeta la chiave più volte e si sommi modulo 26 il suo valore a quello da sostituire.

t	u	n	o	n	p	u	o	i	p	a	s	s	a	r	e	+
i	s	u	f	i	i	s	u	f	i	i	s	u	f	i	i	=

Ciò corrisponde numericamente a

19	20	13	14	13	15	20	14	8	15	0	18	18	0	17	4	+
8	18	20	5	8	8	18	20	5	8	8	18	20	5	8	8	=
1	12	7	19	21	23	12	8	13	23	8	10	12	5	25	12	

con somma in $\mathbb{Z}_{26}$. Convertendo i numeri in lettere si ha

BMHTVXMINXIKMFZM.

È evidente dall'esempio che la stessa lettera di un testo nel cifrario di Vigenère può essere cifrata con lettere diverse, inoltre lettere diverse sono cifrate con la stessa lettera.

Definizione 1.6. Sia m un intero positivo e siano $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. In corrispondenza della chiave $K = (k_1, k_2, k_3, \cdots, k_m)$ siano

$$e_K(x_1, x_2, \cdots, x_m) = (x_1 + k_1, x_2 + k_2, \cdots, x_m + k_m)$$
$$d_K(y_1, y_2, \cdots, y_m) = (y_1 - k_1, y_2 - k_2, \cdots, y_m - k_m)$$

dove la somma è da intendersi in $\mathbb{Z}_{26}$.

Il numero di possibili chiavi di lunghezza m nel cifrario di Vigenère è 26^m, abbastanza elevato per un valore relativamente piccolo di m, e quindi la ricerca esaustiva della chiave può richiedere molto tempo.

K viene detta anche **verme** per il motivo che, se è molto più corta del messaggio, deve essere ripetuta, eventualmente troncandola, un numero di volte pari alla lunghezza del testo in chiaro.

1.6 Cifrario di Hill

Un altro esempio di cifrario polialfabetico è il cifrario di Hill, inventato dall'omonimo matematico statunitense nel 1929.

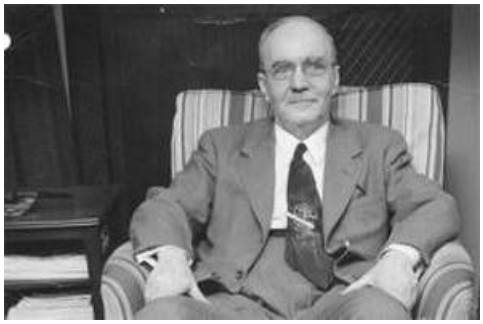

Figura 1.4: Lester S. Hill (1891 – 1961)

Definizione 1.7. **(Cifrario di Hill)**
Sia $m \geq 2$ un intero, siano $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ e sia $\mathcal{K}$ l'insieme delle matrici quadrate invertibili di ordine m a coefficienti in $\mathbb{Z}_{26}$. Se K è una chiave, allora

$$e_K(x) = xK$$
$$d_K(y) = yK^{-1}$$

dove il prodotto righe per colonne tra matrici è in $\mathbb{Z}_{26}$.

Per esempio, sia **Il tesoro luccicante** il testo in chiaro e siano $m = 6$ e la chiave definita da

$$K = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Si convertano le varie lettere nei rispettivi numeri

i	l	t	e	s	o	r	o	l	u	c	c	i	c	a	n	t	e
8	11	19	4	18	14	17	14	11	20	2	2	8	2	0	13	19	4

e si dividano i numeri così trovati in gruppi di lunghezza 6 applicando poi la funzione e_K.

$$\begin{pmatrix}8 & 11 & 19 & 4 & 18 & 14\end{pmatrix}\begin{pmatrix}0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0\end{pmatrix} = \begin{pmatrix}19 & 18 & 8 & 14 & 4 & 11\end{pmatrix}$$

e cosí via per tutti i gruppi, fino ad arrivare ad avere numericamente

$$19\ 18\ 8\ 14\ 4\ 11\ 11\ 2\ 17\ 2\ 20\ 14\ 0\ 19\ 8\ 4\ 13\ 2$$

cioè **TSIOELLCRCUOATIENC**.
Utilizzando la matrice inversa

$$K^{-1} = \begin{pmatrix}0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0\\ 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\end{pmatrix}$$

è facile vedere che si ottiene il messaggio di partenza.

1.7 Cifrario mediante trasposizione

L'idea su cui si basa il cifrario mediante trasposizione è quella di non modificare le lettere, ma solo la loro posizione attraverso l'utilizzo di permutazioni.

Definizione 1.8. **(Cifrario mediante trasposizione)**
Siano $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ e $\mathcal{K} = Sym(m)$, dove $m \in \mathbb{N}$. Se $\pi \in \mathcal{K}$, allora

$$e_\pi(x_1, ..., x_m) = (x_{\pi(1)}, ..., x_{\pi(m)})$$
$$d_\pi(y_1, ..., y_m) = (y_{\pi^{-1}(1)}, ..., y_{\pi^{-1}(m)}),$$

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

Osserviamo che il cifrario di trasposizione è un caso particolare del cifrario di Hill. Infatti, a una permutazione π dell'insieme $\{1, \cdots, m\}$ possiamo associare **una matrice di permutazione** K_π in cui il termine di posto $a_{ij} = 1$ se, e solo se, $\pi(i) = j$, e 0 altrimenti.

Riprendendo l'esempio precedente, la chiave

$$K_\pi = \begin{pmatrix} 0&0&1&0&0&0 \\ 0&0&0&0&0&1 \\ 1&0&0&0&0&0 \\ 0&0&0&0&1&0 \\ 0&1&0&0&0&0 \\ 0&0&0&1&0&0 \end{pmatrix}$$

è la matrice della permutazione $\pi = (1\ 3)(2\ 6\ 4\ 5)$. Inoltre, $K_\pi^{-1} = K_{\pi^{-1}}$.

1.8 Cifrari a flusso

Nei cifrari a blocchi la chiave è costante, cioè $y = y_1 \cdots y_n = e_K(x_1), \cdots e_K(x_n)$. Un'idea differente è quella alla base dei **cifrari a flusso** in cui è possibile generare un flusso di chiavi $z = z_1 z_2 ... z_n$ e utilizzare queste per cifrare il messaggio attraverso la regola

$$y = y_1 y_2 \cdots = e_{z_1}(x_1) e_{z_2}(x_2) \cdots$$

Esistono diversi tipi di cifrari a flusso. Il più semplice è quello in cui il flusso di chiavi viene costruito a partire da una chiave indipendente dal testo da decifrare.

Definizione 1.9. **(Cifrario a flusso sincrono)**
Un **cifrario a flusso sincrono** è una sestupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{E}, \mathcal{D})$ di insiemi finiti non vuoti e una funzione $g : \mathcal{K} \to \mathcal{L}^{\mathbb{N}}$ tali che

- $\mathcal{P}$ è l'insieme delle **unità di messaggio in chiaro**;
- $\mathcal{C}$ è l'insieme delle **unità di messaggio cifrato**;
- $\mathcal{K}$ è l'insieme delle **chiavi**;
- $\mathcal{L}$ è l'insieme detto **alfabeto delle chiavi**;
- g è il **generatore di chiavi**: una funzione che ad ogni chiave $k \in K$ associa una stringa infinita $z_1 z_2 \cdots$ detta **flusso delle chiavi**, $z_i \in \mathcal{L}$ per ogni $i \geq 1$;
- per ogni $z \in \mathcal{L}$ c'è una **funzione di cifratura** $e_z \in \mathcal{E}$, $e_z : \mathcal{P} \to \mathcal{C}$ e una **funzione di decifratura** $d_z \in \mathcal{D}$, $d_z : \mathcal{C} \to \mathcal{P}$ t.c. $d_z \circ e_z = Id_{\mathcal{P}}$.

Esempi di cifrari a flusso sincrono sono:

- I **cifrari a blocchi**, per cui vale che $\mathcal{L} = \mathcal{K}$ e $g : \mathcal{K} \to \mathcal{K}^{\mathbb{N}}$, $g(K) = (K, K, \cdots)$ è la successione costante di costante valore K;
- Il **cifrario di Vigenère** con $\mathcal{K} = (\mathbb{Z}_{26})^m$, $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathbb{Z}_{26}$ e il flusso $g : (\mathbb{Z}_{26})^m \to (\mathbb{Z}_{26})^{\mathbb{N}}$ di chiavi definito come segue:

$$z_i = \begin{cases} k_i \text{ se } 1 \leq i \leq m \\ z_{i-m} \text{ se } i \geq m+1 \end{cases}$$

dove $K = (k_1 \cdots k_m)$. Quindi, si ha

$$e_z(x) = (x + z) \mod 26$$

$$d_z(y) = (y - z) \mod 26.$$

Un cifrario a flusso è detto **periodico** con periodo d se $z_{i+d} = z_i$ per tutti gli interi $i \geq 1$. Un cifrario a flusso è spesso descritto in termini di alfabeto binario, cioè $\mathcal{P} = \mathcal{C} = \mathbb{Z}_2$. Cifratura e decifratura sono operazioni in $\mathbb{Z}_2$:

$$e_z(x) = (x + z) \mod 2$$
$$d_z(y) = (y + z) \mod 2$$

Questo tipo di operazioni sono molto efficienti nell'hardware ed è per questo che questo cifrario viene implementato spesso.

Sia $K = (k_1, ..., k_m, c_0, ..., c_{m-1}) \in \mathbb{Z}_2^{2m}$ con $c_0, c_1, ..., c_{m-1}$ opportune costanti e sia $z_i = k_i$ con $1 \leq i \leq m$. Usando una ricorrenza lineare di grado m il flusso di chiavi è

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \mod 2$$

per tutti gli $i \geq 1$.

A partire dalle $2m$-uple $(k_1 \cdots k_m, c_0 \cdots c_{m-1})$ in cui $c_0, ..., c_{m-1}$ sono scelte in maniera opportuna viene creato un flusso di chiavi di periodo $2^m - 1$.
Sia per esempio $m = 4$ e il flusso di chiavi sia generato usando la ricorrenza lineare

$$z_{i+4} = (z_i + z_{i+1}) \mod 2$$

con $i \geq 1$. Se il flusso è inizializzato con un vettore diverso da $(0, 0, 0, 0)$, allora otteniamo un flusso di periodo $2^4 - 1 = 15$. Per esempio, iniziando con $(1, 0, 0, 0)$ si avrà

$$1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1 \cdots$$

Un qualsiasi altro vettore darà un permutazione ciclica dello stesso flusso di chiavi.

Un altro metodo di generazione di flusso di chiavi è **linear feedback shift register (LFSR)**.

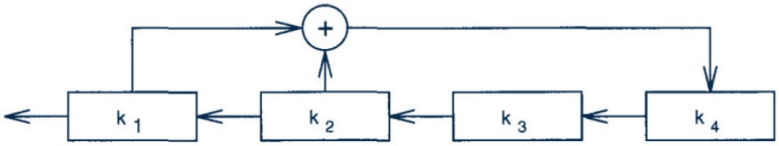

Figura 1.5: Esempio di LFSR

Come evidenziato in **Figura 1.5**, il vettore binario $(k_1, \cdots, k_m)$ è utilizzato per inizializzare il flusso e ad ogni passo vengono applicate le seguenti operazioni:

- k_1 viene messo in cima come successivo bit del flusso di chiavi;
- ognuno dei $k_2 \cdots k_m$ viene spostato a sinistra di un posto;
- il "nuovo" valore di k_m inserito è

$$\sum_{j=0}^{m-1} c_j k_{j+1}.$$

LSFR è eseguito per un certo numero di passi e utilizza una somma in $\mathbb{Z}_2$.

Un **cifrario a flusso non sincrono** è un cifrario in cui il flusso di chiavi z_i dipende dalle precedenti unità di messaggi in chiaro così come dalla chiave K.

Definizione 1.10. **(Cifrario autokey)**
Siano $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}_{26}$. Sia $g : \mathbb{Z}_{26} \to (\mathbb{Z}_{26})^{\mathbb{N}}$ definito da $z_1 = K$ e $z_i = x_{i-1}$ per tutti gli $i \geq 2$. Per $0 \leq z \leq 25$ siano

$$e_z(x) = (x + z) \ mod \ 26$$
$$d_z(y) = (y - z) \ mod \ 26$$

con $x, y \in \mathbb{Z}_{26}$.

Si osservi che, dal punto di vista formale, il cifrario autokey sembra molto vicino a quello di Vigenère. La ragione per cui viene denominato in questo modo è dovuto all'autogenesi della chiave durante la cifratura del messaggio. Il cifrario autokey è pertanto insicuro perché vi sono solo 26 possibili chiavi.

Sia $K = 8$ la chiave e il testo da cifrare **buona giornata**. Convertito in interi:

1 20 14 13 0 6 8 14 17 13 0 20 0

il flusso di chiavi sarà il seguente:

8 1 20 14 13 0 6 8 14 17 13 0 20

sommandole modulo 26 si ha:

9 21 8 1 13 6 14 22 5 4 13 20 20

che convertito in lettere è **JVIBNGOWFENUU**.

1.9 La macchina Enigma

Enigma era una macchina per cifrare utilizzata dal Terzo Reich negli anni precedenti e durante la Seconda Guerra Mondiale.

La macchina era costituita da:

- una **tastiera** per immettere il testo da cifrare;
- lo **scambiatore** che cifra la lettera del testo in chiaro nella corrispondente lettera del testo cifrato;
- un **visore** con varie lampadine che illuminandosi indicano la lettera del testo cifrato da trasmettere.

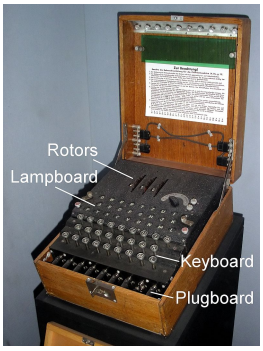

Figura 1.6: Macchina Enigma

Lo scambiatore (o rotore) rappresenta la parte più importante della macchina. Consiste in uno spesso disco di gomma attraversato da una fitta rete di fili proveniente dalla tastiera, che entrano nello scambiatore ed escono dalla parte opposta, determinando una cifratura a sostituzione monoalfabetica.

L'idea fondamentale di Scherbius, uno dei due creatori di Enigma, fu quella di far ruotare il disco di un ventiseiesimo di giro, in modo tale da cambiare cifratura ad ogni lettera pigiata sulla tastiera trasformando così la cifratura in una sostituzione polialfabetica.

Figura 1.7: Arthur Scherbius (1878 – 1929)

Per aumentare la sicurezza di Enigma vennero poi inseriti un secondo e un terzo scambiatore: il secondo compiva una rotazione parziale soltanto dopo che il primo avesse compiuto un intero giro e il terzo compiva la stessa cosa basandosi sul secondo. Il numero totale di chiavi è circa 10 milioni di miliardi, un numero enorme anche per un computer!

Di seguito è presentata una versione semplificata del cifrario che sta alla base di Enigma.

Siano $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}_{26}$ e π una fissata permutazione di $\mathbb{Z}_{26}$.
Sia $g : \mathcal{K} \to \mathcal{L}^{\mathbb{N}}$ definita da $z_i = (K + i - 1) \ mod\ 26$ per $i \geq 1$.

La cifratura e decifratura utilizzano π e π^{-1} come segue

$$e_z(x) = \pi(x) + z \ mod\ 26$$
$$d_z(x) = \pi^{-1}(y) - z \ mod\ 26,$$

dove $z \in \mathbb{Z}_{26}$.

Si consideri la seguente permutazione di $\mathbb{Z}_{26}$:

$$\pi = (0\ 23\ 9\ 16\ 17\ 2\ 24\ 3)(1\ 13\ 18\ 21\ 4\ 7\ 6\ 14\ 5\ 15\ 11)(8\ 25)(10\ 22)(12\ 19)$$

Si consideri il messaggio in chiaro **Spruchnummer** ("messaggio numero" in tedesco, una delle frasi che permise al gruppo di Bletchley Park [1] guidato da Alan Turing di decifrare il funzionamento di Enigma durante la II guerra mondiale) e si cifri seguendo il crittosistema appena definito.

[1] Bletchley Park fu il sito dell'unità principale di crittoanalisi del Regno Unito, nonchè sede della Scuola governativa di codici e cifratura durante la Seconda Guerra Mondiale. Le informazioni ottenute con le attività svolte a Bletchley Park hanno aiutato lo sforzo alleato e accorciato la durata della guerra.

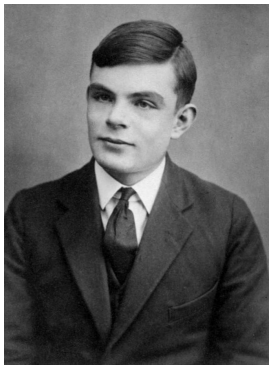
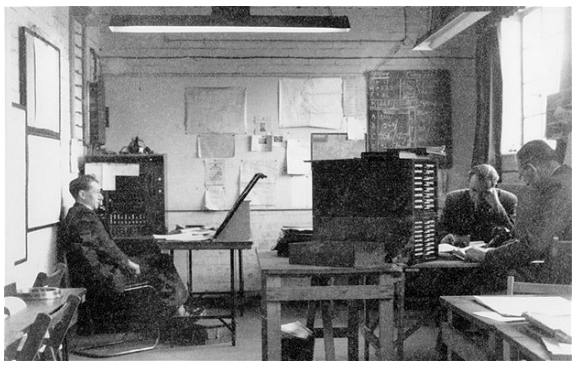

Figura 1.8: Alan Mathison Turing (1912 – 1954) e la stanza di controllo nella Baracca 6 (crittoanalisi dei codici Enigma per l'Army and Air Force) nel Bletchley Park

Quindi,

s	**p**	**r**	**u**	**c**	**h**	**n**	**u**	**m**	**m**	**e**	**r**
18	**15**	**17**	**20**	**2**	**7**	**13**	**20**	**12**	**12**	**4**	**17**

Sapendo che $K = 8$, il flusso di chiavi è:

$$
\begin{aligned}
z_1 &= (K + 1 - 1) \ mod\ 26 = 8 \\
z_2 &= (K + 2 - 1) \ mod\ 26 = 9 \\
z_3 &= (K + 3 - 1) \ mod\ 26 = 10 \\
z_4 &= (K + 4 - 1) \ mod\ 26 = 11 \\
z_5 &= (K + 5 - 1) \ mod\ 26 = 12 \\
z_6 &= (K + 6 - 1) \ mod\ 26 = 13 \\
z_7 &= (K + 7 - 1) \ mod\ 26 = 14 \\
z_8 &= (K + 8 - 1) \ mod\ 26 = 15 \\
z_9 &= (K + 9 - 1) \ mod\ 26 = 16 \\
z_{10} &= (K + 10 - 1) \ mod\ 26 = 17 \\
z_{11} &= (K + 11 - 1) \ mod\ 26 = 18 \\
z_{12} &= (K + 12 - 1) \ mod\ 26 = 19
\end{aligned}
$$

Ora, cifrando il messaggio si ha:

$$
\begin{aligned}
e_{z_1}(s) &= (\pi(S) + z_1) \ mod\ 26 = 3 \\
e_{z_2}(p) &= (\pi(P) + z_2) \ mod\ 26 = 20 \\
e_{z_3}(r) &= (\pi(R) + z_3) \ mod\ 26 = 12 \\
e_{z_4}(u) &= (\pi(U) + z_4) \ mod\ 26 = 5 \\
e_{z_5}(c) &= (\pi(C) + z_5) \ mod\ 26 = 10 \\
e_{z_6}(h) &= (\pi(H) + z_6) \ mod\ 26 = 19 \\
e_{z_7}(n) &= (\pi(N) + z_7) \ mod\ 26 = 6 \\
e_{z_8}(u) &= (\pi(U) + z_8) \ mod\ 26 = 9 \\
e_{z_9}(m) &= (\pi(M) + z_9) \ mod\ 26 = 9 \\
e_{z_{10}}(m) &= (\pi(M) + z_{10}) \ mod\ 26 = 10 \\
e_{z_{11}}(e) &= (\pi(E) + z_1 1) \ mod\ 26 = 25 \\
e_{z_{12}}(r) &= (\pi(R) + z_1 2) \ mod\ 26 = 21
\end{aligned}
$$

cioè **DUMFKTGJJKZV**.

Volendo invece decriptare lo stesso testo appena cifrato si ha:

$$
\begin{aligned}
d_{z_1}(D) &= (\pi^{-1}(D) - z_1) \ mod\ 26 = 18 \\
d_{z_2}(U) &= (\pi^{-1}(U) - z_2) \ mod\ 26 = 15 \\
d_{z_3}(M) &= (\pi^{-1}(M) - z_3) \ mod\ 26 = 17 \\
d_{z_4}(F) &= (\pi^{-1}(F) - z_4) \ mod\ 26 = 20 \\
d_{z_5}(K) &= (\pi^{-1}(K) - z_5) \ mod\ 26 = 2 \\
d_{z_6}(T) &= (\pi^{-1}(T) - z_6) \ mod\ 26 = 7 \\
d_{z_7}(G) &= (\pi^{-1}(G) - z_7) \ mod\ 26 = 13 \\
d_{z_8}(J) &= (\pi^{-1}(J) - z_8) \ mod\ 26 = 20 \\
d_{z_9}(J) &= (\pi^{-1}(J) - z_9) \ mod\ 26 = 12 \\
d_{z_{10}}(K) &= (\pi^{-1}(K) - z_{10}) \ mod\ 26 = 12 \\
d_{z_{11}}(Z) &= (\pi^{-1}(Z) - z_{11}) \ mod\ 26 = 4 \\
d_{z_{12}}(V) &= (\pi^{-1}(V) - z_{12}) \ mod\ 26 = 17
\end{aligned}
$$

che corrisponde al testo in chiaro di partenza.