Azzolini Riccardo 2021-03-08

Tecniche di sostituzione: cifratura polialfabetica

1 Cifratura polialfabetica

Le tecniche di **cifratura polialfabetica** sono fondate sull'idea di utilizzare diverse sostituzioni monoalfabetiche (diversi alfabeti[1]), in modo che ciascuna lettera del plaintext venga cifrata con un cifrario monoalfabetico diverso.

Esistono tanti diversi schemi di cifratura polialfabetica, ma essi hanno in comune due elementi:

- la definizione di un insieme di sostituzioni monoalfabetiche utilizzate;
- l'uso della chiave per determinare quale sostituzione applicare a ciascuna lettera.

2 Cifratura di Vigenère

L'esempio più noto di cifratura polialfabetica è la cifratura di Vigenère, nel quale:

- come insieme di sostituzioni monoalfabetiche si considerano 26 cifrari di Cesare (cioè il cifrario di Cesare con tutte le 26 possibili chiavi, $k = 0, \dots, 25$);
- la sostituzione da usare per l'n-esima lettera del plaintext è indicata dall'n-esima lettera della chiave.

Quest'ultima regola implica che la chiave debba essere lunga quanto il plaintext: siccome in molti casi ciò non sarebbe pratico, tipicamente si usa una chiave più corta, che viene ripetuta fino a ottenere la lunghezza desiderata.

Per eseguire la cifratura e la decifratura è utile disporre di una tabella contenente tutti i cifrari di Cesare:

[1] Quando si parla di usare diversi alfabeti nel contesto della cifratura polialfabetica, ciò non significa usare simboli diversi (in genere, l'insieme dei simboli dell'alfabeto del testo cifrato rimane sempre lo stesso), ma piuttosto mapping (sostituzioni) diversi tra i simboli del plaintext e i simboli del ciphertext. Se un mapping viene denotato elencando le lettere dell'alfabeto cifrato nell'ordine delle corrispondenti lettere dell'alfabeto in chiaro, si può pensare ai diversi mapping come alfabeti diversi che sono formati dalle stesse lettere disposte in ordini diversi.

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

Una lettera della chiave determina il valore di k da utilizzare per il cifrario di Cesare in base, ad esempio, alla solita corrispondenza tra lettere e numeri: `a` corrisponde a $k = 0$, `b` corrisponde a $k = 1$, e così via, fino ad arrivare a `z`, che corrisponde a $k = 25$. Allora, per semplificare la lettura della tabella mostrata prima, si possono scrivere direttamente al posto dei valori di k le lettere corrispondenti:

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Adesso, a scopo illustrativo, si supponga di voler cifrare il plaintext `meet me after the toga party` con la chiave `test`. Il primo passo, come già detto, è ripetere la chiave fino ad arrivare alla lunghezza del plaintext:

```
testtesttesttesttesttes
meetmeafterthetogaparty
```

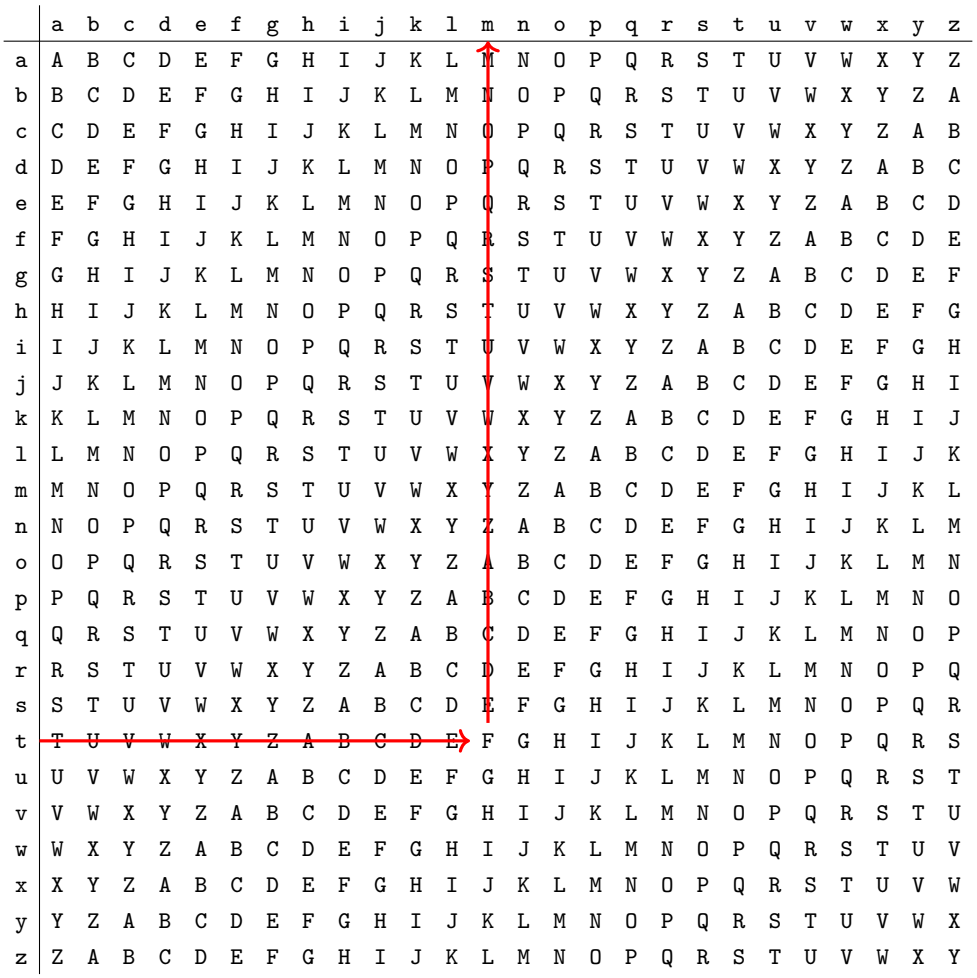
A questo punto, si può iniziare a cifrare la prima lettera. Per farlo, si legge nella tabella la lettera situata all'intersezione della riga corrispondente alla lettera della chiave e della colonna corrispondente alla lettera del plaintext (o viceversa, perché la tabella è simmetrica):

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

La prima lettera del testo cifrato è allora `F`. Ripetendo il procedimento per le restanti lettere, si ottiene:

`FIWMFISYMIJMAILHZEHTKXQ`

La decifratura avviene leggendo la tabella al contrario: nella riga (o colonna) corrispondente alla lettera della chiave si cerca la lettera del testo cifrato, e la colonna (riga) in cui essa si trova indica la lettera del testo in chiaro. Ad esempio, la decifratura della prima lettera (`F`) avviene in questo modo:



2.1 Crittoanalisi

Con il cifrario di Vigenère, ogni lettera ha 26 omofoni, quindi la sua frequenza sarebbe idealmente nascosta nel ciphertext, se non fosse che la chiave si ripete in modo periodico: con una chiave di n lettere, tutte le lettere (e i digrammi, trigrammi, ecc.) del ciphertext situate a n posizioni di distanza l'una dall'altra sono cifrate con una stessa sostituzione monoalfabetica, quindi su di esse è possibile fare l'analisi delle frequenze.

Ad esempio, un attacco di crittoanalisi potrebbe procedere in un modo simile a questo:

1. Facendo l'analisi delle frequenze sull'intero testo cifrato, si osserva che le frequenze di tutte le lettere sono relativamente uniformi, quindi si deduce che è stata impiegata la cifratura polialfabetica, e si suppone che si tratti in particolare della cifratura di Vigenère.

2. Per tentare di scoprire la lunghezza della chiave, si cercano nel testo cifrato delle lettere (o digrammi, ecc.) ripetute, e si ipotizza che la distanza tra le ripetizioni corrisponda alla lunghezza della chiave.
3. Si fa l'analisi delle frequenze sulle lettere che, in base all'ipotesi sulla lunghezza della chiave, dovrebbero essere state cifrate con la stessa sostituzione, eventualmente riprovando con diverse lunghezze della chiave finché non si riesce a decifrare il messaggio.

3 One-Time Pad

Per tentare di risolvere il problema della ripetizione della chiave sono state proposte varie soluzioni. Un esempio è la tecnica *autokey*: essa usa la chiave una volta per cifrare un primo frammento del messaggio, dopodiché ricava la chiave da usare per il frammento successivo in base al frammento cifrato finora, e così via. In questo modo, gli attacchi di crittoanalisi diventano più difficili, ma ancora non impossibili, perché nelle chiavi ricavate a partire dai frammenti di ciphertext rimangono delle informazioni sui pattern presenti nel plaintext.

L'unica soluzione che funziona "perfettamente" è utilizzare una chiave che sia:

- *lunga quanto il messaggio*,
- *completamente casuale*,
- *utilizzabile una sola volta*.[2]

Una chiave che soddisfa tali condizioni può essere usata nel cifrario di Vigenère, oppure si può utilizzare un altro schema, introdotto da Vernam, che prende il nome di **One-Time Pad**[3] (OTP). Esso rappresenta ciascuna lettera (simbolo) come una sequenza di bit, e usa l'operatore XOR ($\oplus$) per eseguire la cifratura e la decifratura: se P_i, K_i e C_i indicano rispettivamente l'i-esima lettera del plaintext, della chiave e del ciphertext, allora la formula per la cifratura è $C_i = P_i \oplus K_i$, mentre quella per la decifratura è $P_i = C_i \oplus K_i$ (il funzionamento di queste formule è già stato spiegato in precedenza).

Gli schemi di cifratura con una chiave casuale monouso lunga quanto il plaintext sono gli unici di cui è possibile dimostrare la **sicurezza incondizionata** (e, infatti, tale proprietà fu dimostrata da Shannon nel 1948). Tale proprietà significa che questo tipo di cifrario è inviolabile anche da parte di un attaccante che dispone di potenza di calcolo illimitata, perché:

[2] Utilizzare ogni chiavi una sola volta è una buona idea per qualunque schema di cifratura, ma in questo caso tale condizione è specificata esplicitamente perché serve, insieme alla condizione che la chiave sia casuale, a garantire che un'attaccante non abbia alcuna informazione sulla chiave.

[3] Il termine *one-time pad* deriva dal fatto che, in passato, le chiavi per questo tipo di schemi di cifratura venivano scritte su dei foglietti (*pad*) da usare una volta sola (*one-time*).

- la casualità della chiave garantisce che il ciphertext non mantenga alcuna informazione sui pattern presenti nel plaintext (frequenze delle lettere, ecc.);
- a un ciphertext corrispondono più plaintext potenzialmente validi, ottenuti utilizzando chiavi diverse per la decifratura, quindi un attaccante non può essere in grado di riconoscere il plaintext corretto, il che impedisce anche attacchi a forza bruta.

Quest'ultimo punto merita un approfondimento. Siccome le chiavi sono lunghe quanto il plaintext e completamente casuali, lo spazio dei messaggi e lo spazio delle chiavi coincidono: ad esempio, con chiave di n bit si possono cifrare i messaggi corrispondenti a tutte le possibili sequenze di n bit, e l'insieme delle chiavi di n bit coincide appunto con tutte le possibili sequenze di n bit. Osservando poi che, fissato un qualunque plaintext, con ciascuna chiave si ottiene un ciphertext diverso (sia con Vigenère che con lo XOR, ogni modifica di un simbolo della chiave si riflette direttamente nel corrispondente simbolo del ciphertext), si deduce che ciascun plaintext può essere cifrato (con uguale probabilità, dato che le chiavi casuali sono equiprobabili) in tutti i possibili ciphertext (della stessa lunghezza), e allo stesso modo ciascun ciphertext può essere decifrato in tutti i possibili plaintext. Allora, nel tentare un attacco a forza bruta, l'attaccante otterrebbe tutti i possibili messaggi, senza alcuna indicazione di quale sia quello corretto.

Ad esempio, si consideri il seguente ciphertext di 6 lettere, che potrebbe essere stato ottenuto applicando il cifrario ci Vigenère a un qualche plaintext di 6 lettere con una chiave casuale anch'essa di 6 lettere:

```
QPAFXX
```

Due esempi di plaintext ugualmente plausibili sono:

- `attack`, ottenuto decifrando con la chiave `qwhfvn`;
- `defend`, ottenuto decifrando con la chiave `nlvbku`.

3.1 Problemi

Lo schema one-time pad ha dei grossi limiti che ne rendono difficile l'utilizzo pratico (se tali limiti non ci fossero, allora tutti gli altri schemi di cifratura simmetrica, che non godono della proprietà di sicurezza incondizionata, non avrebbero di fatto ragione di esistere):

- Generare una chiave veramente casuale non è banale. ad esempio, i calcolatori possono facilmente generare dei numeri *pseudocasuali*, ma, come suggerisce il termine, questi non sono completamente casuali.

- La distribuzione di una chiave segreta lunga quanto il messaggio ha una complessità uguale a quella dell'invio del messaggio stesso, quindi la cifratura con one-time pad sposta solo il problema della sicurezza dal canale usato per l'invio del messaggio al canale usato per l'invio della chiave. Allora, in molti casi sarebbe possibile mandare direttamente il messaggio sul canale sicuro predisposto per la chiave.