

# Crittografia classica: Pollux



# Cos'è la crittografia

La parola crittografia deriva da *Kryptós* (nascosto) e *graphía*(scrittura) che sono le due parole greche che compongono il termine *crittografia*. Possiamo definire la crittografia come un sistema pensato per rendere illeggibile un messaggio a chi non possiede la soluzione per decodificarlo. La crittografia può essere di due tipi: moderna e classica. Un modo per cifrare e decifrare i messaggi di un tempo fa è proprio quella di Pollux che andremo a vedere.

# Cifratura Morse

Per passare dalla frase chiara alla cifra Pollux dobbiamo prima fare uso del codice morse che, come è noto, prevede solo tre simboli: punto, linea e spazio. Ad ogni numero e lettera viene associato un diverso identificatore come andremo a vedere in tabella:

<i>Lettera</i>	<i>Morse</i>	<i>Lettera</i>	<i>Morse</i>	<i>Lettera</i>	<i>Morse</i>
0	-----	C	---.	O	---
1	.-----	D	...-	P	....-
2	..----	E	.-	Q	---..
3	...---	F	....-	R	...-
4	....--	G	---.	S	...-
5	.....	H	....-	T	-
6	-----	I	..-	U	...-
7	----.	J	....-	V	....-
8	-----	K	---.	W	...-
9	-----	L	....-	X	....-
A	.-	M	--	Y	....-
B	....	N	..-	Z	....-

# Esempio Morse

chiaro    I N V I A R E P R O V V I S T E  
Morse    ..t-.t...-t..t.-t.-.t.t.--.t.-.t---t...-t...-t..t...t-t.

Tabella Morse:

Lettera	Morse	Lettera	Morse	Lettera	Morse
0	-----	C	....	O	---
1	.....	D	...-	P	....
2	.....	E	.-	Q	----
3	.....	F	....	R	...-
4	.....	G	---.	S	...-
5	.....	H	....	T	-..
6	.....	I	..-	U	...-
7	....-	J	....	V	....
8	.....	K	---.	W	....
9	.....	L	....	X	....
A	.-.	M	--.	Y	....
B	....	N	..-	Z	....

# Funzionamento Pollux

La cifratura Pollux si appoggia sul codice Morse che prevede il punto, la linea e lo spazio. Ognuno di questi simboli viene cifrato con un sistema di sostituzione con omofoni ovvero ad un segno chiaro possono corrispondere diversi segni cifrati. Per realizzare la cifratura avremmo bisogno di due liste, una cifrante ed una decifrante come andremmo a vedere nell' esempio.

# Esempio Pollux

chiaro	I	N	V	I	A	R	E	P	R	O	V	V	I	S	T	E
Morse	.	.	-	.	.	-	.	.	-	.	-	.	-	-	.	.
cifrato	Y	N	Z	O	S	J	Q	W	G	B	C	Q	S	U	Y	P

<i>Lista cifrante</i>		
Punto	.	A, F, G, M, N, Q, S, W, Y
Linea	-	B, E, H, K, L, O, P, T, X
Spazio	+	C, D, I, J, R, U, V, Z

<i>Lista decifrante</i>			
A	.	N	.
B	-	O	-
C	+	P	-
D	+	Q	.
E	-	R	+
F	.	S	.
G	.	T	-
H	-	U	+
I	+	V	+
J	+	W	.
K	-	X	-
L	-	Y	.
M	.	Z	+

# Alcuni accorgimenti...

- Nella cifratura pollux il messaggio cifrato può arrivare ad essere lungo tre o quattro volte rispetto al testo chiaro
- Per la sicurezza della cifra al momento della cifratura gli omofoni devono essere distribuiti in modo casuale
- Possiamo usare anche come omofoni le 10 cifre ma avremmo una minor sicurezza dato che sono di meno rispetto alle lettere dell'alfabeto

# Fonti:

- <http://www.crittologia.eu/critto/pollux.html>
- <http://www.crittologia.eu/critto/js/pollux.html>