Il cifrario bifido di Delastelle

Il cifrario bifido di Delastelle è un cifrario poligrafico basato sulla matrice 5x5 usata per la prima volta nella scacchiera di Polibio, dispositivo inventato dagli antichi greci.

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

	1	2	3	4	5
1	UN	B	C	D	E
2	F	sol	H	I / J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

L’inventore

Il metodo è dovuto a Félix-Marie Delastelle una tra i massimi crittologi francesi del XIX secolo.

Ci sono pochi dettagli biografici, si sa che fosse figlia di un marinaio e seguiva la sua passione di crittografia come hobby.

Il metodo

- Il messaggio chiaro viene spezzato in blocchi di cinque caratteri ciascuno; se l'ultimo blocco non è esattamente di cinque, gli ultimi posti sono riempiti di X.
- Ogni lettera del blocco viene cifrata con due cifre e cioè con l'indice di riga e l'indice di colonna, che vengono scritte in verticale sotto la lettera chiara.
- Le cifre vengono ora riscritte in orizzontale riga dopo riga ottenendo un messaggio con un numero di cifre doppio dell'originale.
- A questo punto ogni coppia di numeri viene ritrasformata in lettera sempre secondo la matrice. Ne risulta il messaggio cifrato da trasmettere.

La matrice

	1	2	3	4	5
1	C	O	M	P	U
2	T	E	R	A	B
3	D	F	G	H	I
4	J	K	L	N	Q
5	S	V	X	Y	Z

esempio

1 Si voglia cifrare il messaggio: `URGE INVIO RINFORZI`

2 che viene così scomposto e cifrato:

```
URGEI-NVIOR-INFOR-ZIXXX
12323 45312 34312 53555
53325 42523 54223 55333
```

3 Il messaggio in cifre viene ora raggruppato a due a due e riconvertito in lettere, ottenendo così il messaggio cifrato:

```
12 32 35 33 25 45 31 24 25 23 34 31 25 42 23 53 55 55 53 33
 O  F  I  G  B  Q  D  A  B  R  H  D  B  K  R  X  Z  Z  X  G
```

fonti

- https://www.cmswiki.net/risorse-sviluppo/il-cifrario-bifido-di-delastelle
- http://www.crittologia.eu/critto/delastelle.html
- Google immagini

FINE