- CRITTOGRAFIA CLASSICA -

CESARE

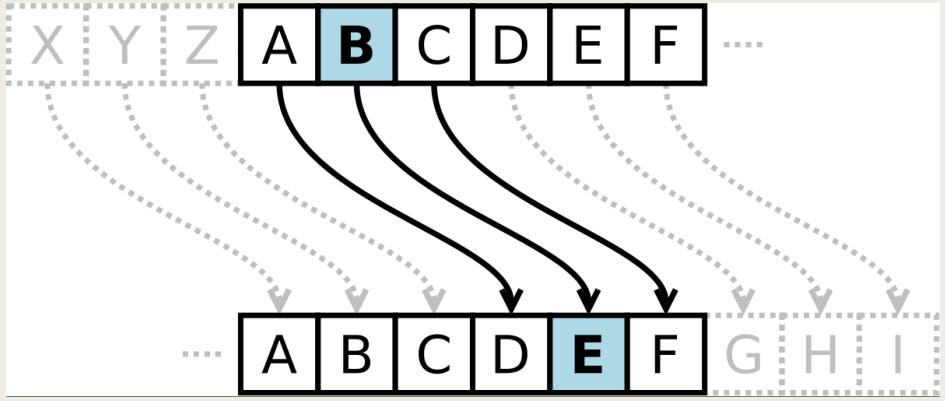
Bastari Mirco

Storia del cifrato

- Il cifrario di Cesare prende il nome da Giulio **Cesare**, che lo utilizzava per proteggere i suoi messaggi segreti. Cesare utilizzava in genere **una chiave di 3 per il cifrario.** Al tempo era sicuro perché gli avversari spesso non erano neanche in grado di leggere un testo in chiaro, men che mai uno cifrato
- Anche **Augusto**, suo nipote, lo utilizzava con **chiave 1**, ma senza ripartire da sinistra in caso di fine dell'alfabeto. A→B; B→C; Z→AA

Cos’è la cifratura Cesare?

- In crittografia il cifrario di Cesare è **uno dei più antichi algoritmi** crittografici
- È un cifrario **a sostituzione monoalfabetica** in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova **un certo numero di posizioni dopo nell'alfabeto.**
- Questi tipi di cifrari sono detti anche **cifrari a sostituzione** o **cifrari a scorrimento**



Funzionamento

- Alfabeto Italiano – 21 Caratteri

Testo in chiaro	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
Testo cifrato	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

- Es CASA → FDVD TESTO → ZHVZR

Funzionamento

- Alfabeto Latino – 26 Caratteri

Testo in chiaro	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
Testo cifrato	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

- Es CASA → FDVD TESTO → WHVWR

Fonti

- http://www.crittologia.eu/critto/caesar.htm
- https://informaticapubblica.com/cosa-e-la-crittografia-capiamolo-con-il-metodo-di-giulio-cesare/
- http://www.cardano.pv.it/studenti/matedida/crittografia/matematica.htm#giulio