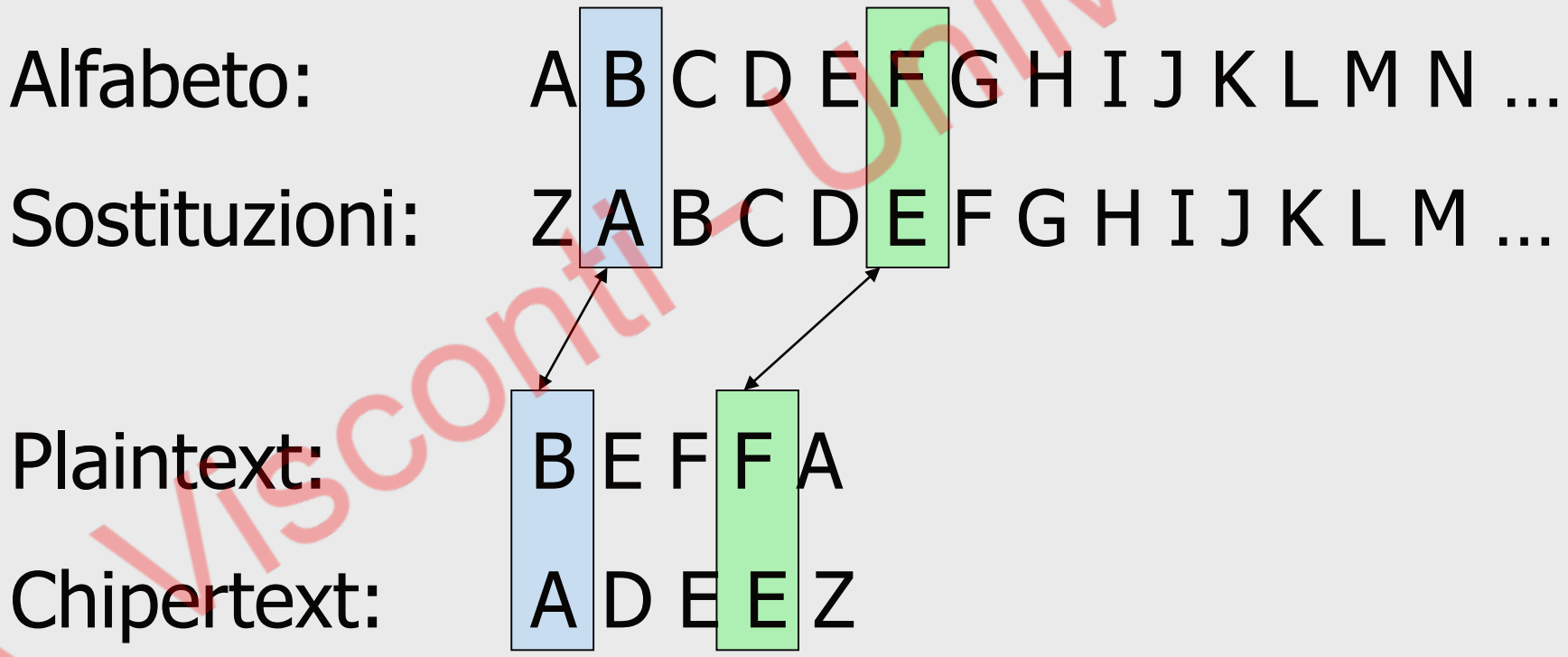
Monoalfabetici a sostituzione

Una lettera viene sempre sostituita con la stessa lettera

- **Cesare (precedente il 150 aC)**



Monoalfabetici a sostituzione

Una lettera viene sempre sostituita con la stessa lettera

- **Il quadrato di Polibio (150 aC)**

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

B	E	F	F	A
BA	EA	AB	AB	AA

Monoalfabetici: Crittosistemi affini

La lettera a_i viene sostituita con la lettera

$$a_{ki+h} \mod 26$$

La chiave è la coppia (k, h) con:

$$k, h \in \{0, 1, 2, \ldots, 25\} \quad e$$

$$\underline{MCD(k, 26) = 1}$$

Quante chiavi ha un crittosistema affine?

$$12 \times 26 = 312$$

Ci sono anche chiavi banali…

Crittosistemi affini: attacco frequenze

Attacco basato sull'analisi delle frequenze

Italiano	
E	11 ,79
A	11 ,74
I	11 ,28
O	9 ,83
N	6 ,88
L	6 ,51
R	6 ,37
T	5 ,62
S	4 ,98

Inglese	
E	12 ,31
T	9 ,59
A	8 ,05
O	7 ,94
N	7 ,19
I	7 ,18
S	6 ,59
R	6 ,03
H	5 ,14

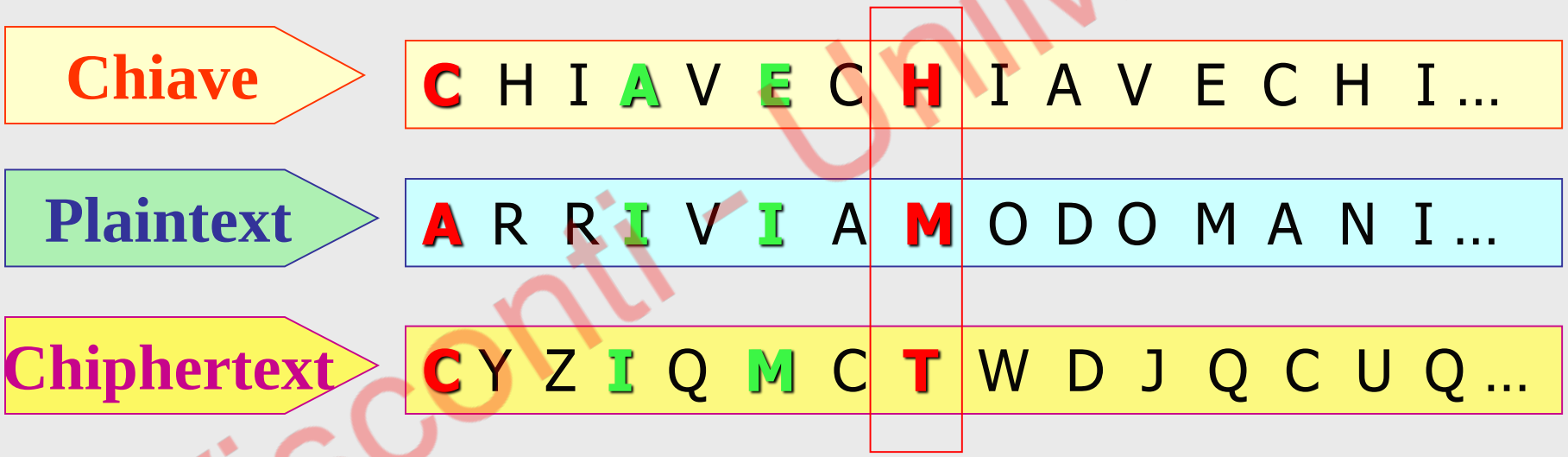
Polialfabetici a sostituzione: Quadr. Vigenère

Inventato nel XVI Secolo

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

Vigenère: Codifica e Decodifica

Una parola chiave mnemonica (lettere distinte) serve a selezionare l'alfabeto di codifica



Decodifica: processo inverso

Vigenère: Attacco di Kasiski

A R R I V I A M O … C A R R I A R M A

C H I A V E C H I … E C H I A V E C H

C Y Z I Q M C T G … G C Y Z I V ….

Lettere che nel crittotesto occupano la stessa posizione modulo p, probabilmente usano lo stesso Cesare

Polialfabetici a sostituzione: Autoclave

Girolamo Cardàno, XVI secolo.

Il plaintext viene accodato chiave ed usato come estensione della chiave stessa

E	C	C	O	I	L	T	E	M	A	D	E	S	A	M	E	…			
O	A	S	I	S	E	C	C	O	I	L	T	E	M	A	D	…			
S	C	U	W	A	P	V	G	A	I	O	X	W	M	M	H	…			

Polialfabetici a sostituzione: Playfair

Inventato nel 1854 da Wheatstone. Le 25 lettere dell'alfabeto (i=j) sono disposte in una matrice 5x5:

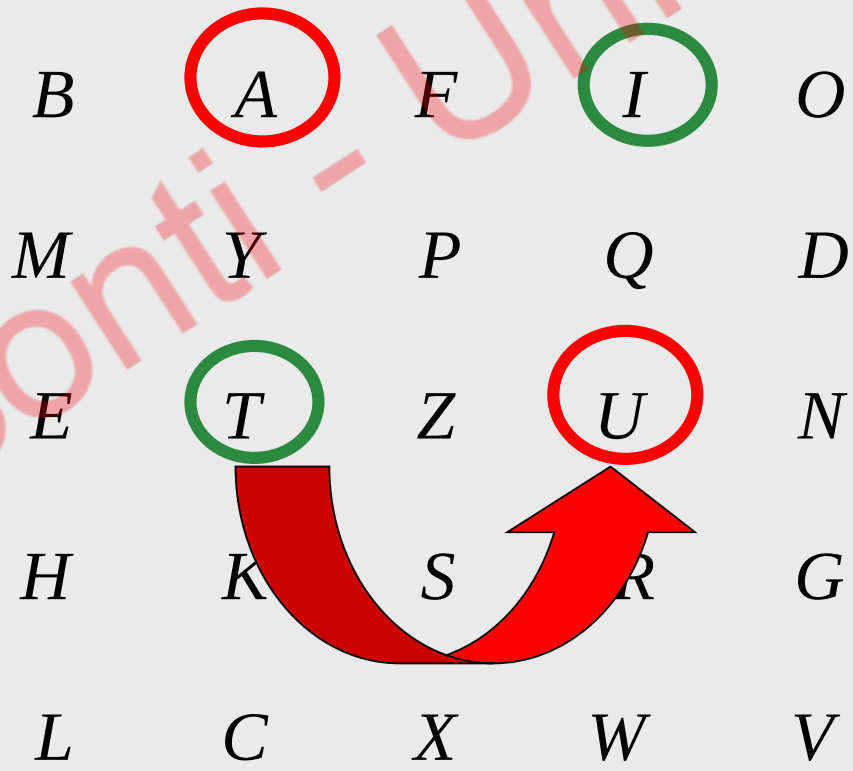
Chiave mnemonica da trascrivere nel quadrato tralasciando eventuali ripetizioni: BAFFI ➔ BAFI

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

Polialfabetici a sostituzione: Playfair

Per cifrare prendo 2 lettere alla volta dopo aver tolto spazi e punteggiatura.

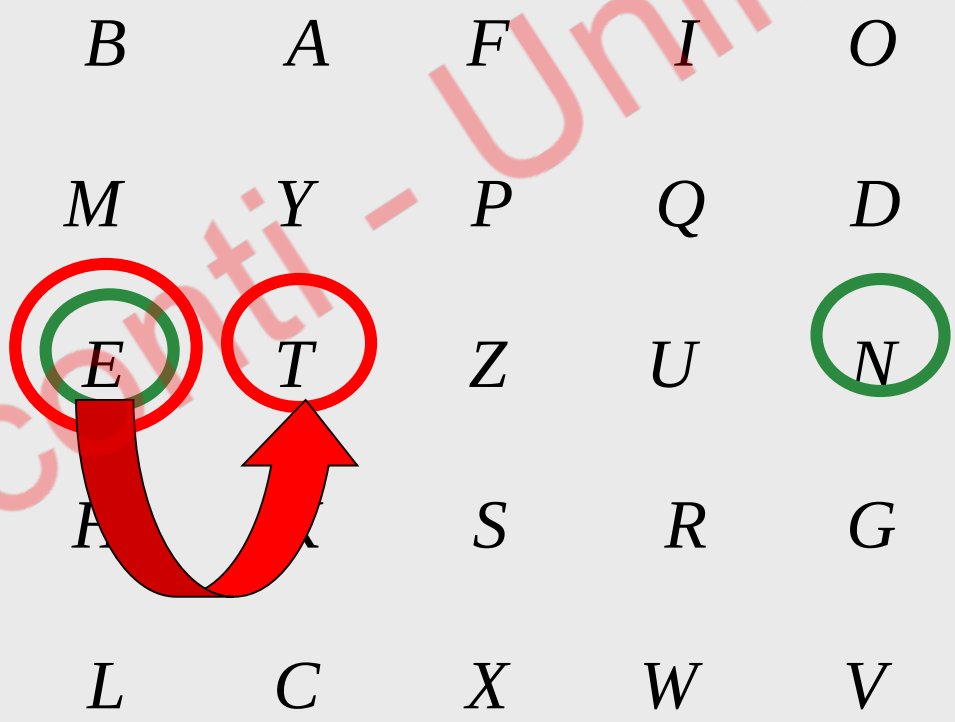
Due lettere su righe e colonne **diverse**. Cifro ***ti*** con ***UA***.



Polialfabetici a sostituzione: Playfair

Due lettere sulla **stessa** riga. Cifro ***en*** con ***TE***.

NB: Attenzione allo shift a dx!!



Polialfabetici a sostituzione: Playfair

Due lettere sulla **stessa** colonna. Cifro ***fz*** con ***PS***. Attenzione allo shift in basso!!

Per decifrare inverto il procedimento mettendo le frecce al contrario. **PS** andra' in ***fz***.

Hill: codifica/decodifica

Insieme delle chiavi

$$\mathcal{K} = \{\text{matrice K} \mid \text{ord K} = n \times n \ \wedge \exists\, K^{-1} \bmod 26\}$$

$\mathbf{E_K}$: $\mathbf{K\ d^T = c^T}$

$\mathbf{D_K}$: $\mathbf{K^{-1}\ c^T = d^T}$

Esempio: decodifica

$c = hiat \Rightarrow [h, i],\ [a, t] \Rightarrow [7, 8],\ [0, 19]$

$K^{-1}\,[7, 8]^T = [7, 4]^T \Rightarrow [h, e]$

$K^{-1}\,[0, 19]^T = [11, 15]^T \Rightarrow [l, p]$

$\Rightarrow \quad p = help$

One-time pad - Verme

- ***Chiave:*** **un vettore binario CASUALE $\underline{k}$ di lunghezza n "sufficientemente grande",** ***usato una sola volta***
- ***Plaintext:*** **un vettore binario $\underline{p}$ di lunghezza $l \leq n$**
- ***Crittotesto:*** **la somma binaria $\underline{c} = \underline{p} + \underline{k}'$, dove $\underline{k}'$ è il vettore formato dalle prime l componenti di $\underline{k}$**