CRITTOGRAFIA

Testi di riferimento :

Dat@Game Hoepli - P.Camagni, R. Nikolassy

InfoChef Hoepli - P.Camagni, R. Nikolassy

Definizione

Pag. 100 DataG@me. Pag. 79 InfoChef

Le modalità di protezione

Uno dei metodi di protezione a disposizione per salvaguardare i propri dati da occhi indiscreti è la **crittografia**, che consente di codificarli rendendoli inaccessibili a chi non ha autorizzazione a utilizzarli. Un tipico esempio di crittografia durante la navigazione è rappresentato dal protocollo https, riconoscibile dal simbolo di un lucchetto collocato nella barra del browser.

Crittografia

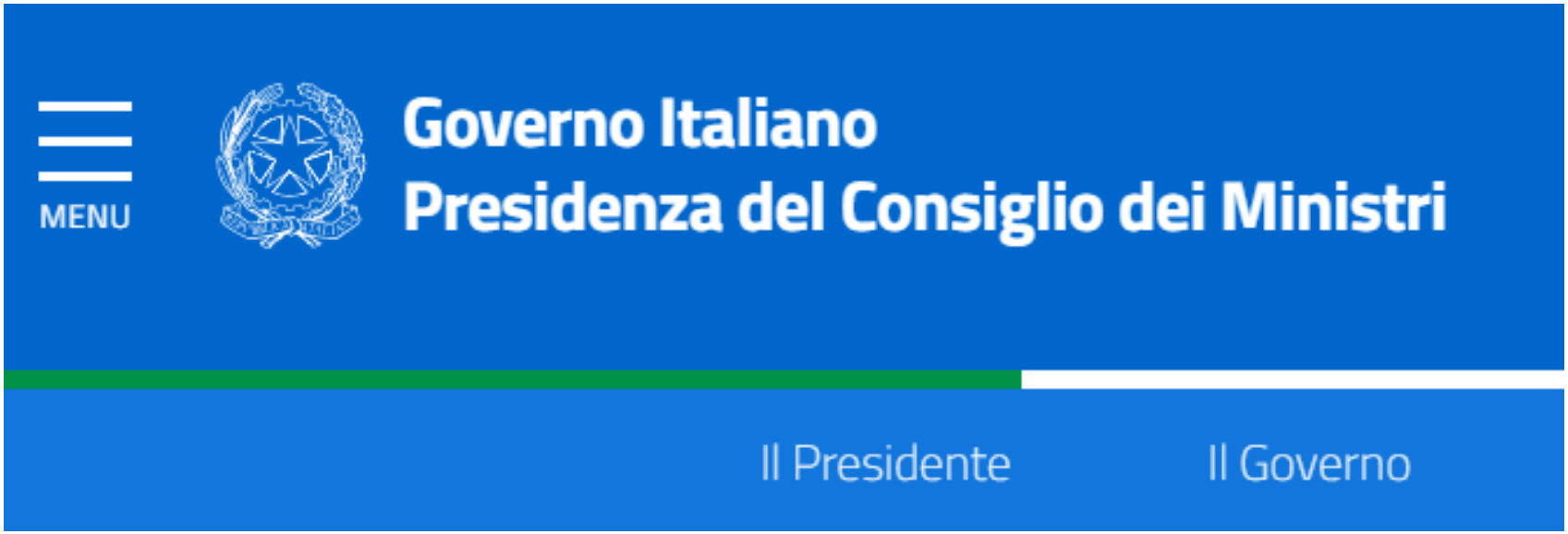
La crittografia è la tecnica che permette di rendere un messaggio incomprensibile alle persone non autorizzate a leggerlo. Si tratta di una cifratura del messaggio. Ogni sistema di crittografia ha due parti essenziali: un algoritmo (per codificare e decodificare) e una chiave: quest'ultima consiste in informazioni che, combinate con il testo "in chiaro" elaborato attraverso l'algoritmo, daranno il testo codificato.

https

Esempio: NETFLIX

http

Esempio: GOVERNO



Algoritmi

- Cifrario di Cesare (50 a.C)
  cifrario storico utilizzato da Giulio Cesare per proteggere i propri messaggi segreti.

Algoritmi

- Cifrario di Cesare (50 a.C)
  cifrario storico utilizzato da Giulio Cesare per proteggere i propri messaggi segreti.
- Cifrario **OTP** (One Time Pad/Password) (1947)
  cifrario storico utilizzato nella Guerra Fredda per la comunicazione con le spie.

Algoritmi

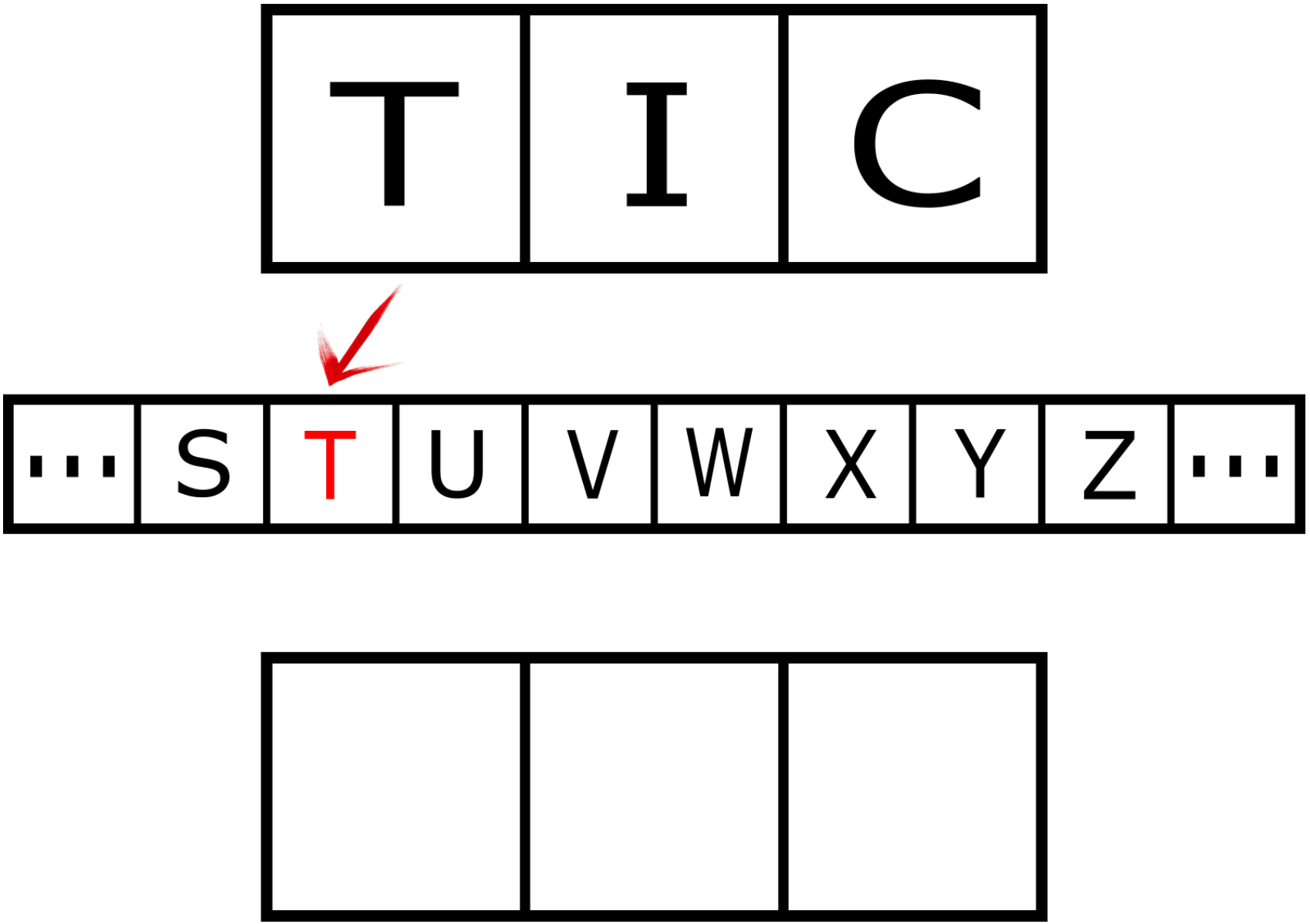
- Cifrario di Cesare (50 a.C)
  cifrario storico utilizzato da Giulio Cesare per proteggere i propri messaggi segreti.
- Cifrario **OTP** (One Time Pad/Password) (1947)
  cifrario storico utilizzato nella Guerra Fredda per la comunicazione con le spie.
- Modello **RSA** (Rivest–Shamir–Adleman) (1977)
  modello a chiave asimmetrica utilizzato ancora oggi nelle comunicazioni in rete.

Cifrario di Cesare

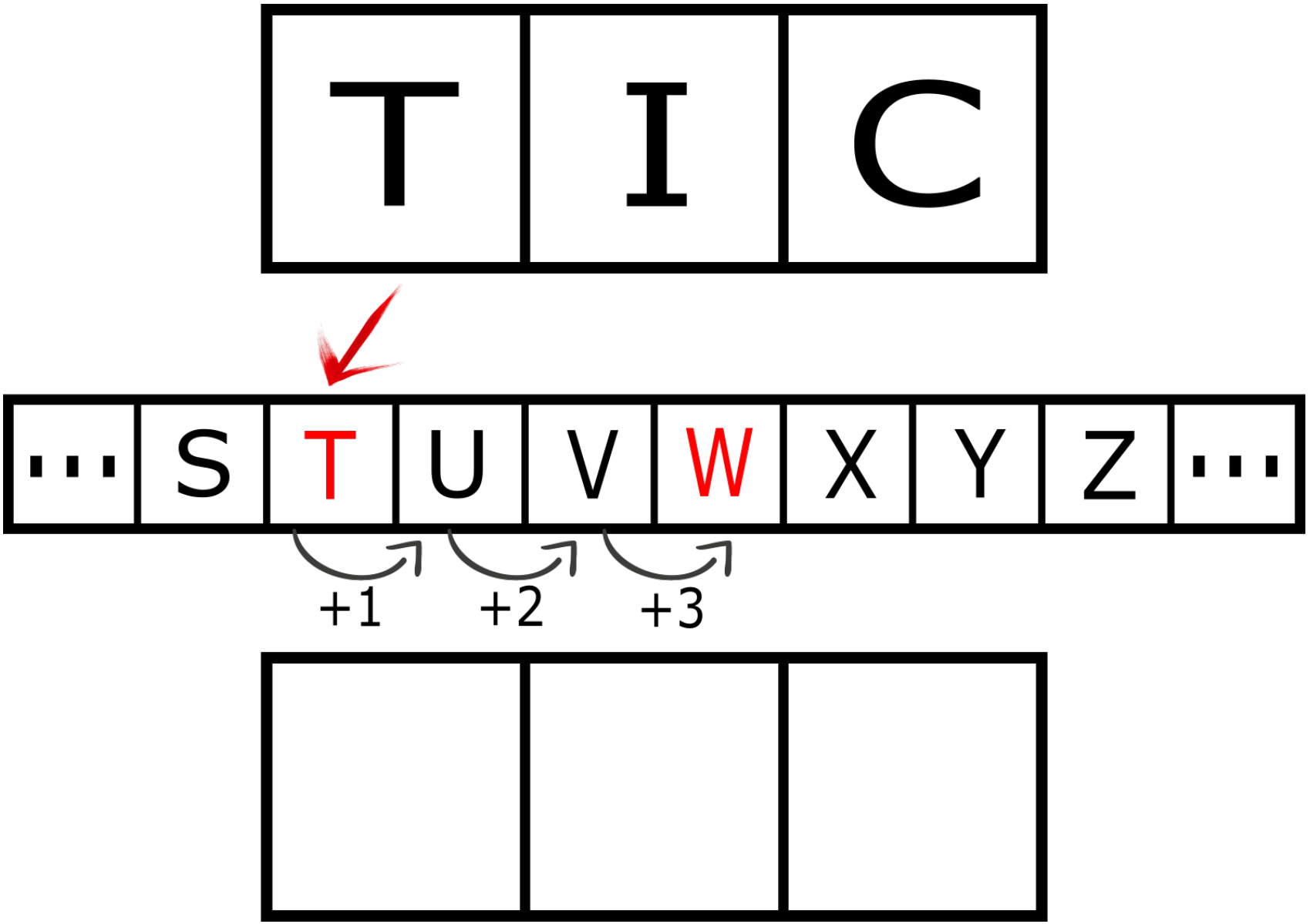
Cifrario molto semplice e oramai non più utilizzato che consiste nel cifrare un testo cifrando ogni lettera con la terza lettera successiva dell'alfabeto:

- la **CHIAVE** è l'informazione '+3'.
- l' **ALGORITMO** consiste nell'applicare la chiave ad ogni lettera per cifrare, e nell'applicare la chiave in negativo ad ogni lettera per decifrare.

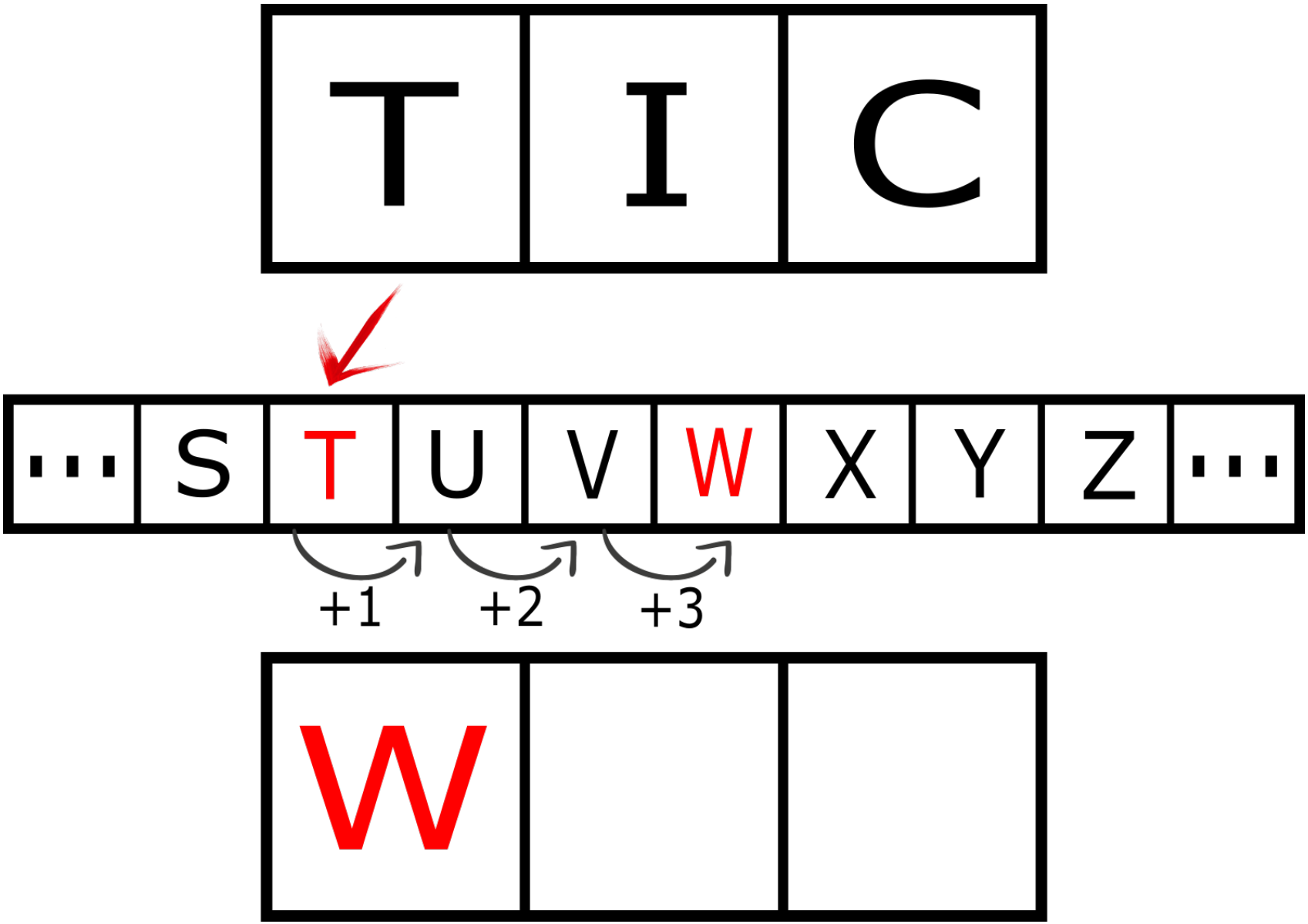
Cifrario di Cesare



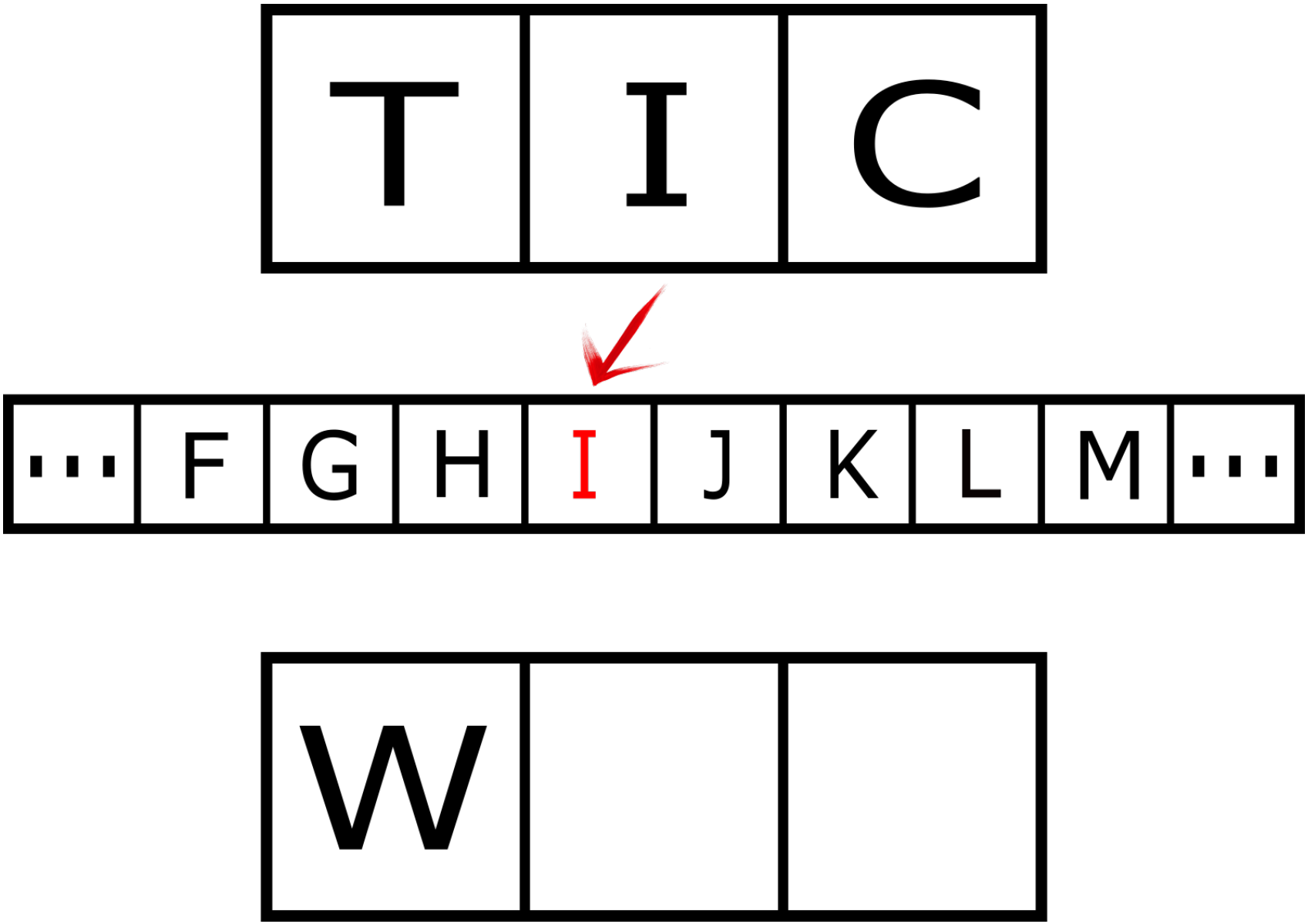
Cifrario di Cesare



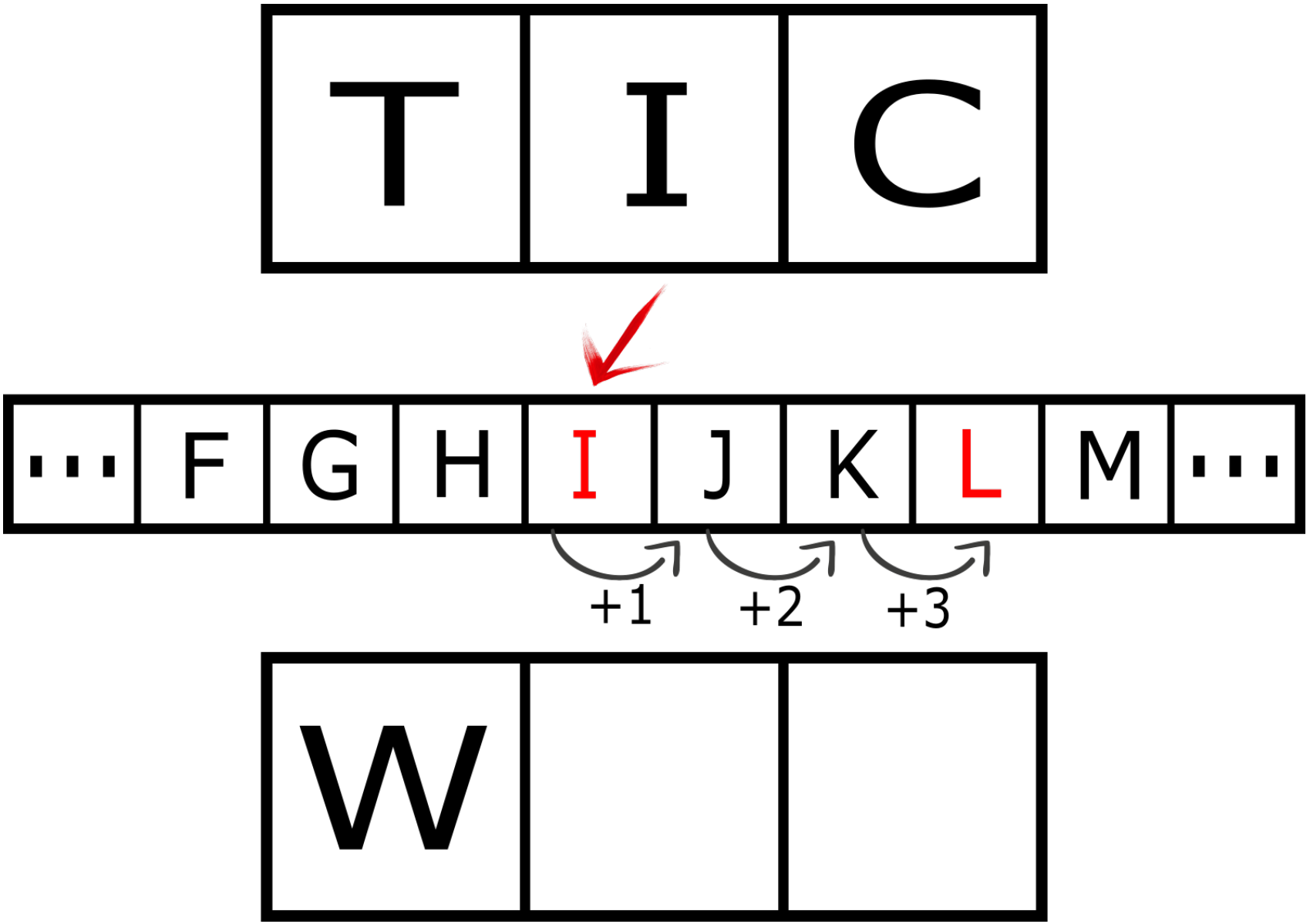
Cifrario di Cesare



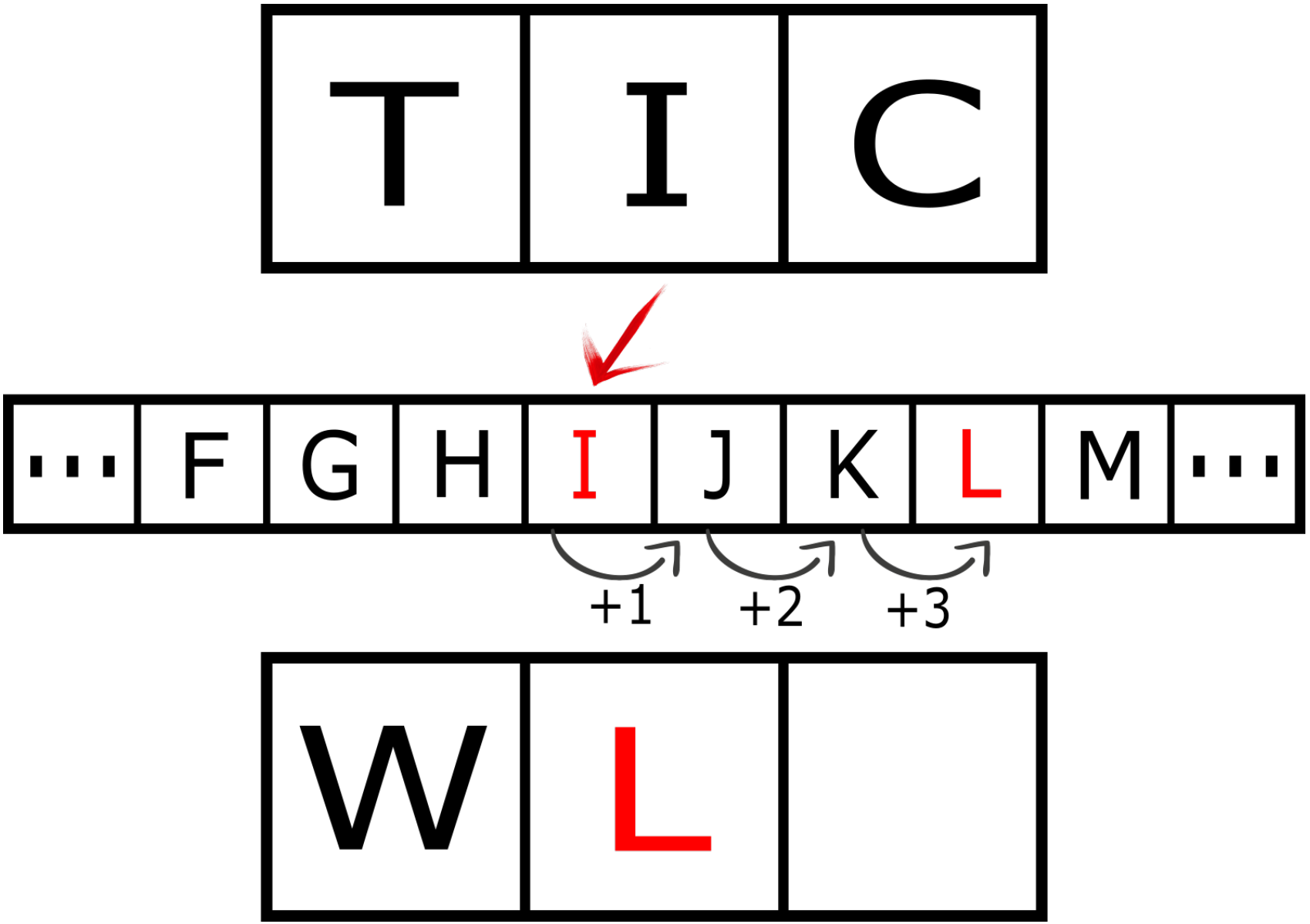
Cifrario di Cesare



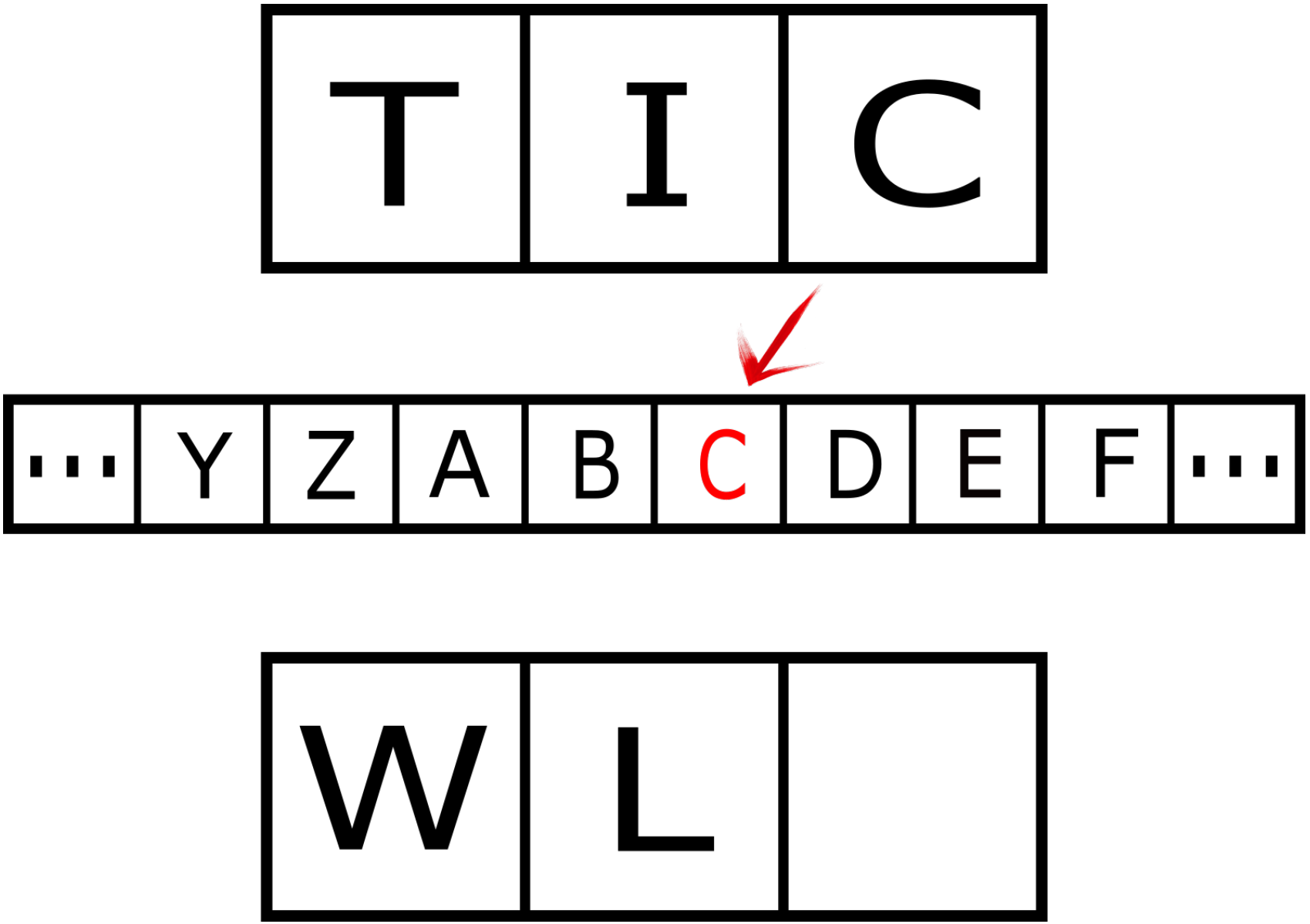
Cifrario di Cesare



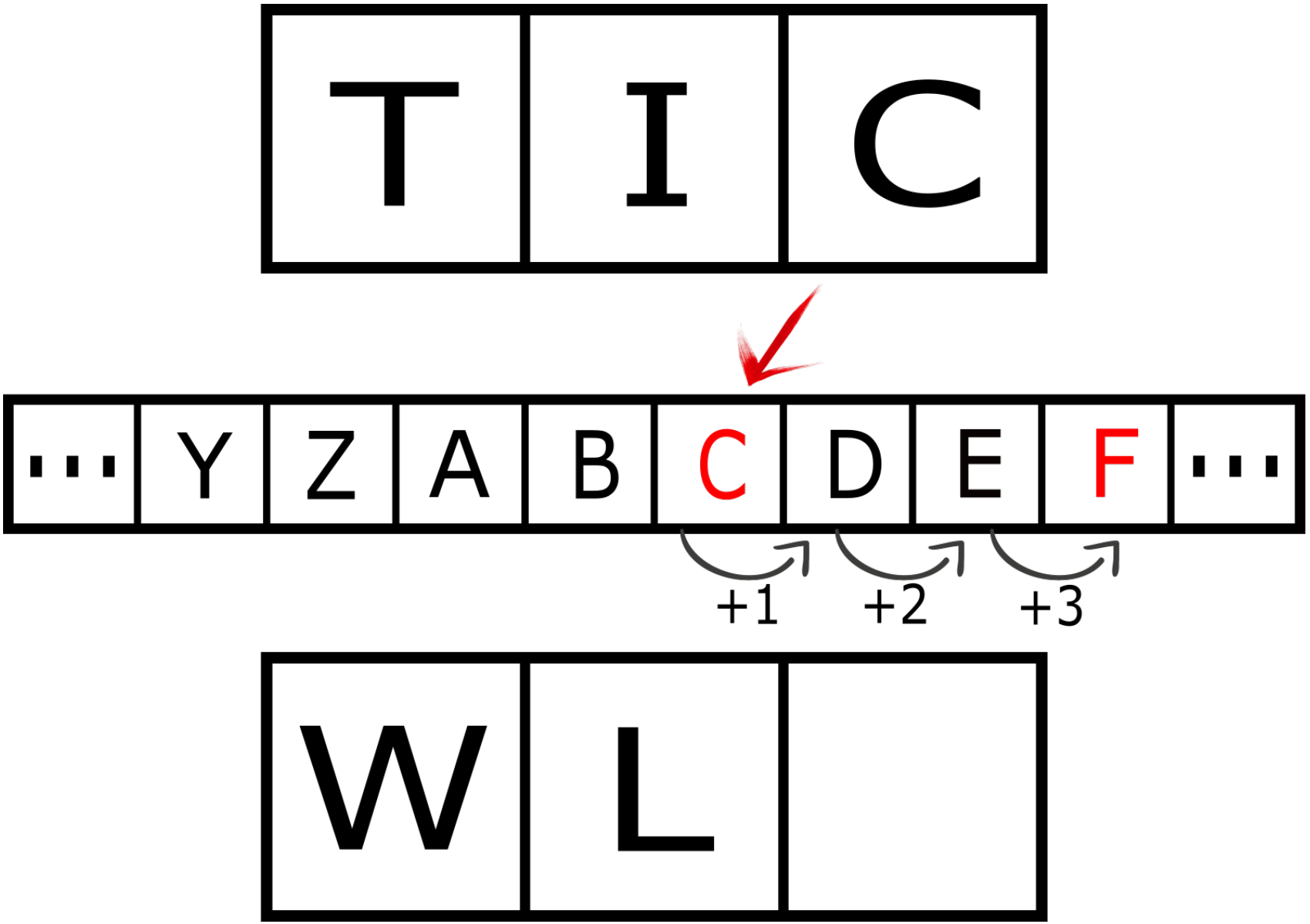
Cifrario di Cesare



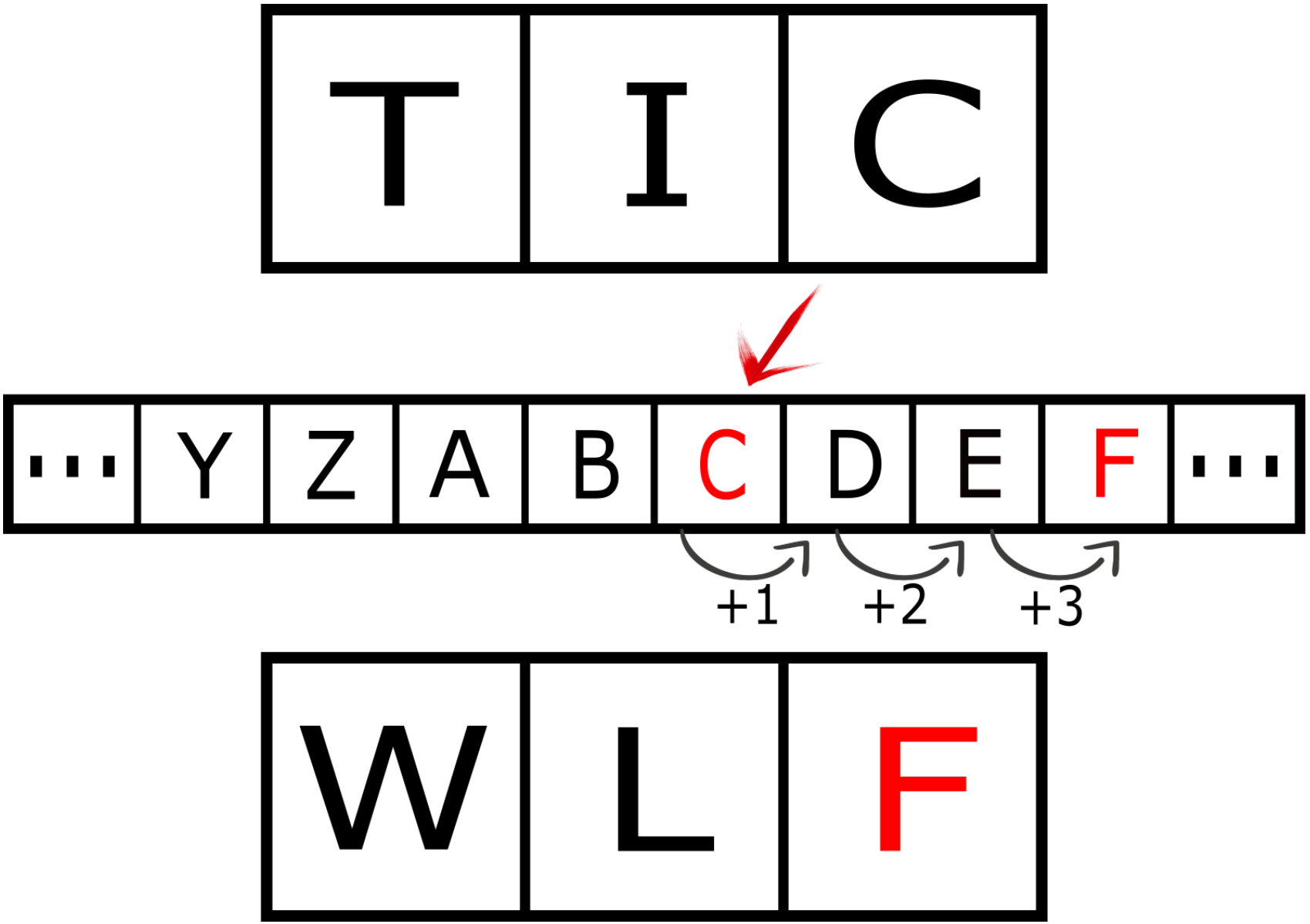
Cifrario di Cesare



Cifrario di Cesare



Cifrario di Cesare

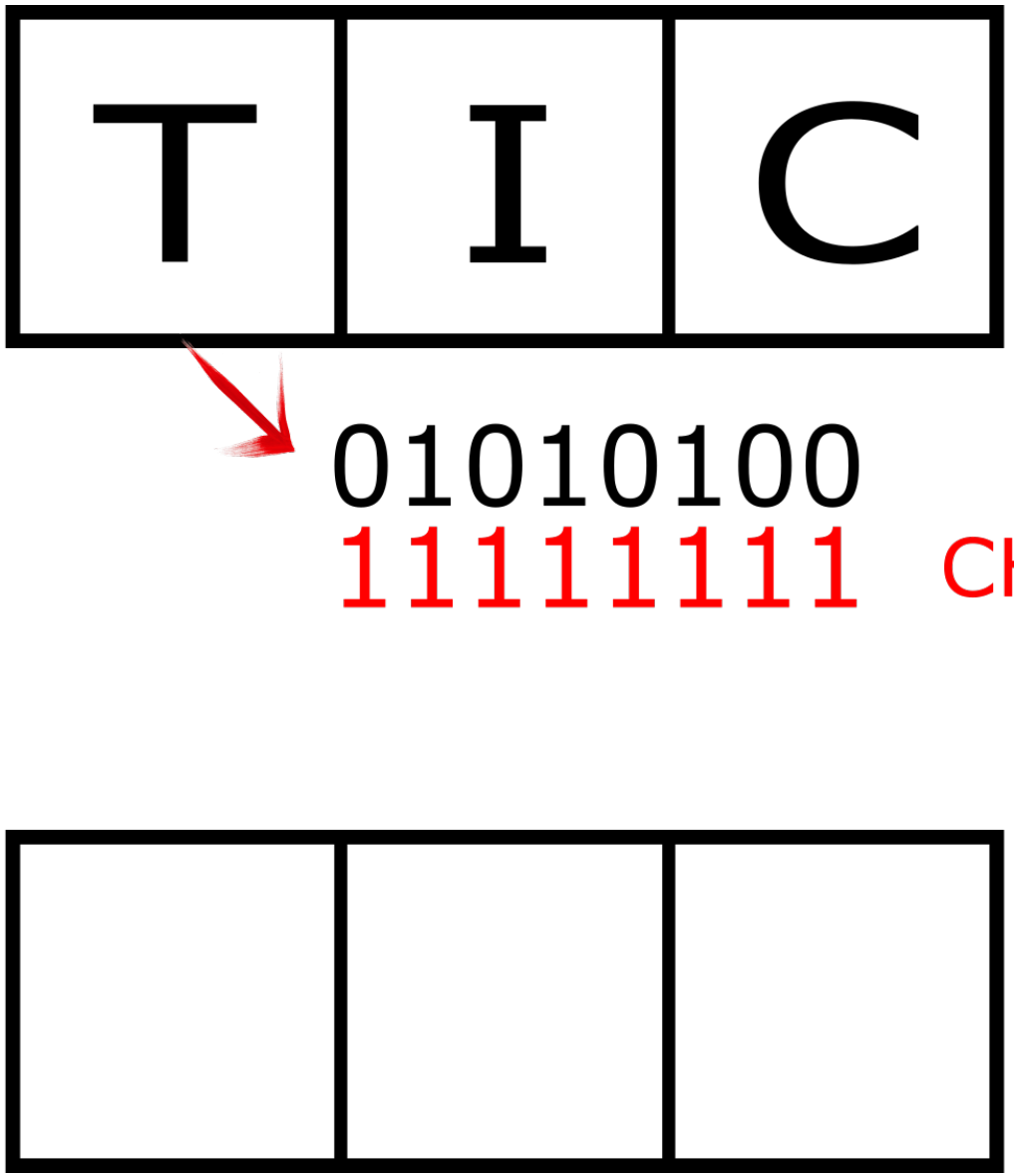


Cifrario OTP

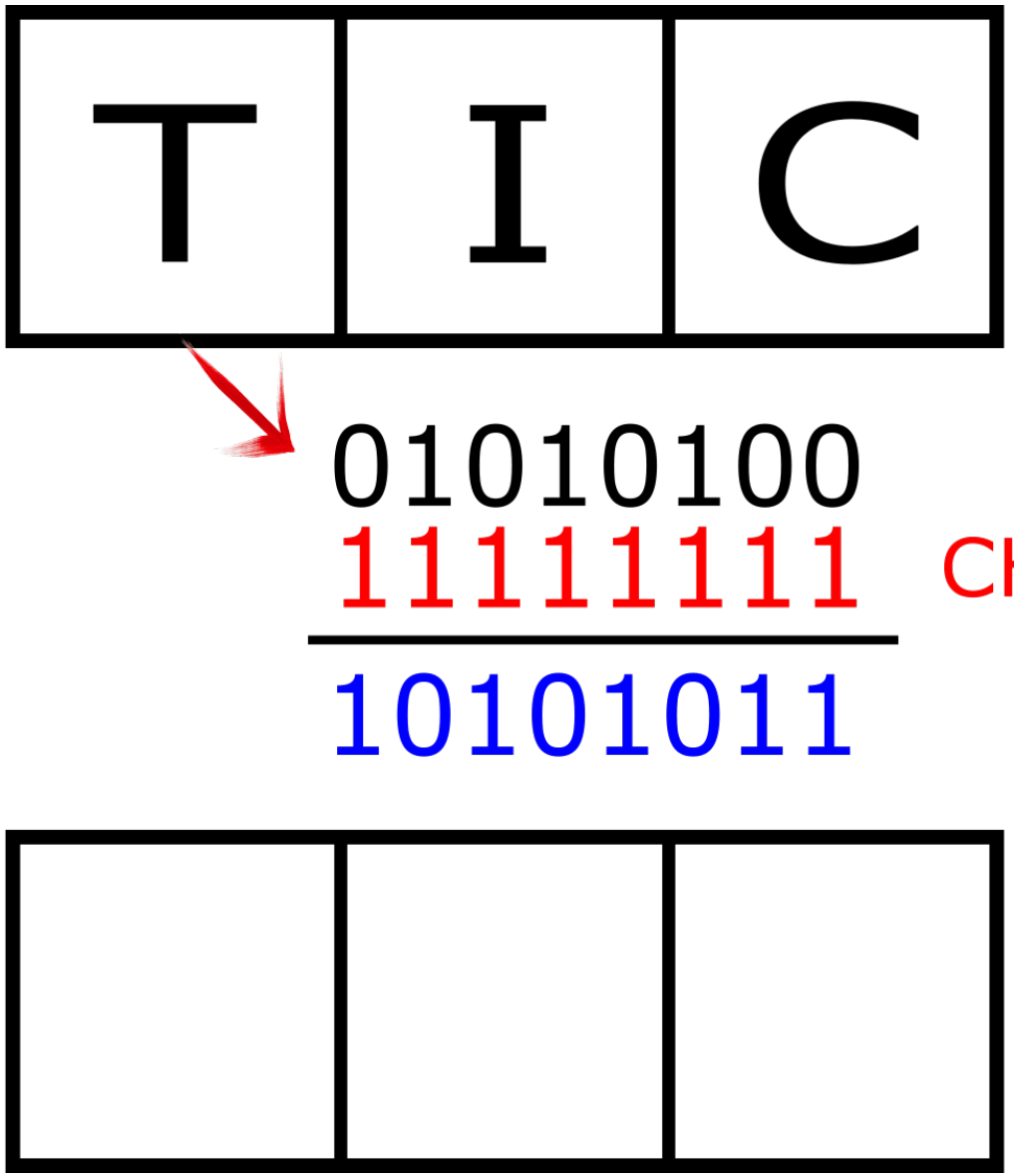
Cifrario semplice utilizzato ancora oggi ad esempio nelle autenticazioni a due fattori dove viene inviata una password utilizzabile una volta sola. La sua sicurezza è stata comprovata da una dimostrazione matematica, il cifrario si è guadagnato il titolo di 'Cifrario Perfetto'.

- la **CHIAVE** è una sequenza di 0,1. Deve essere lunga quanto il testo da cifrare e non è riutilizzabile: One Time.
- l' **ALGORITMO** consiste nell'eseguire l'operazione di XOR tra il testo da cifrare in binario e la chiave. Quest'operazione viene utilizzata sia per cifrare che per decifrare.

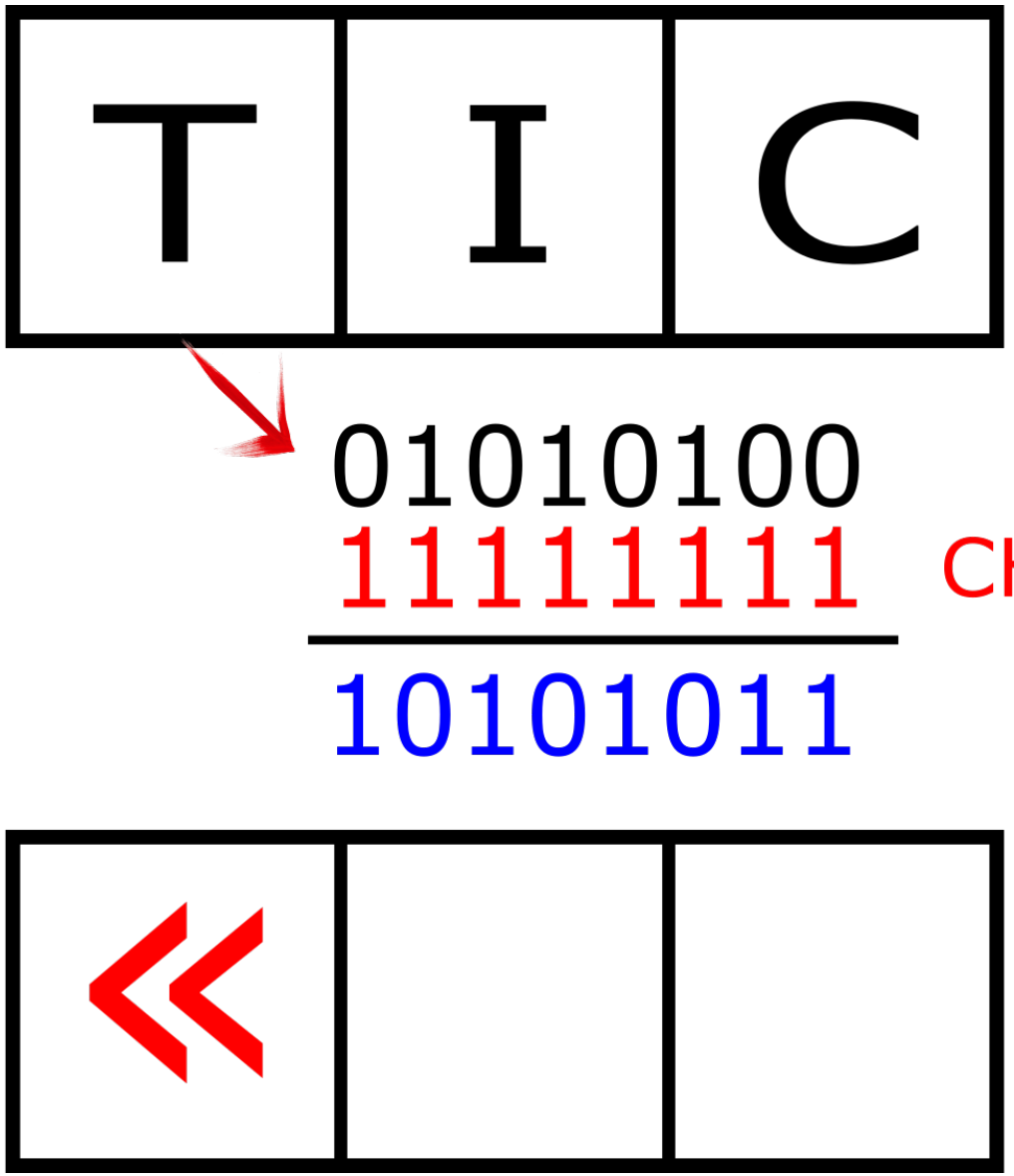
Cifrario OTP



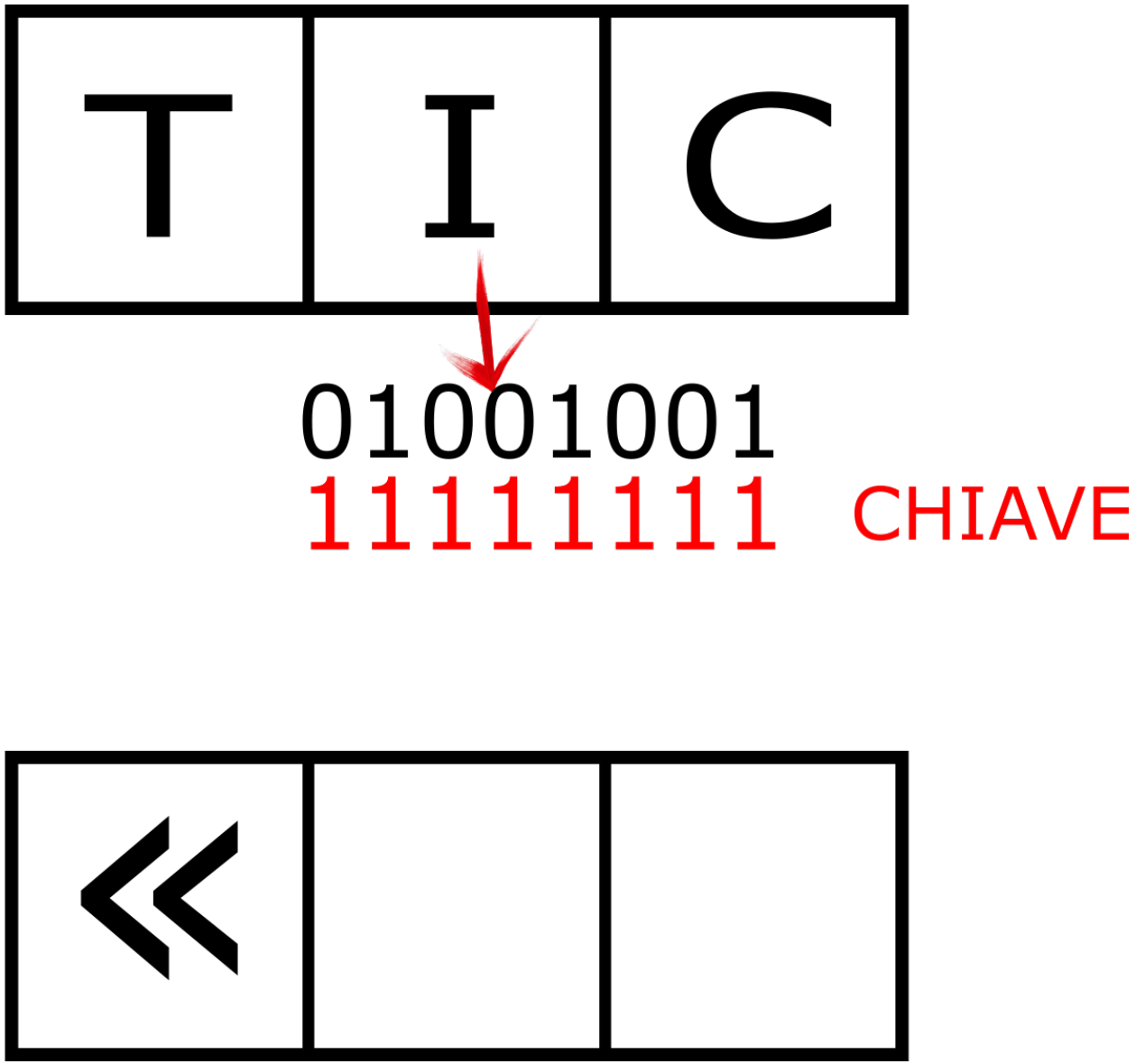
Cifrario OTP



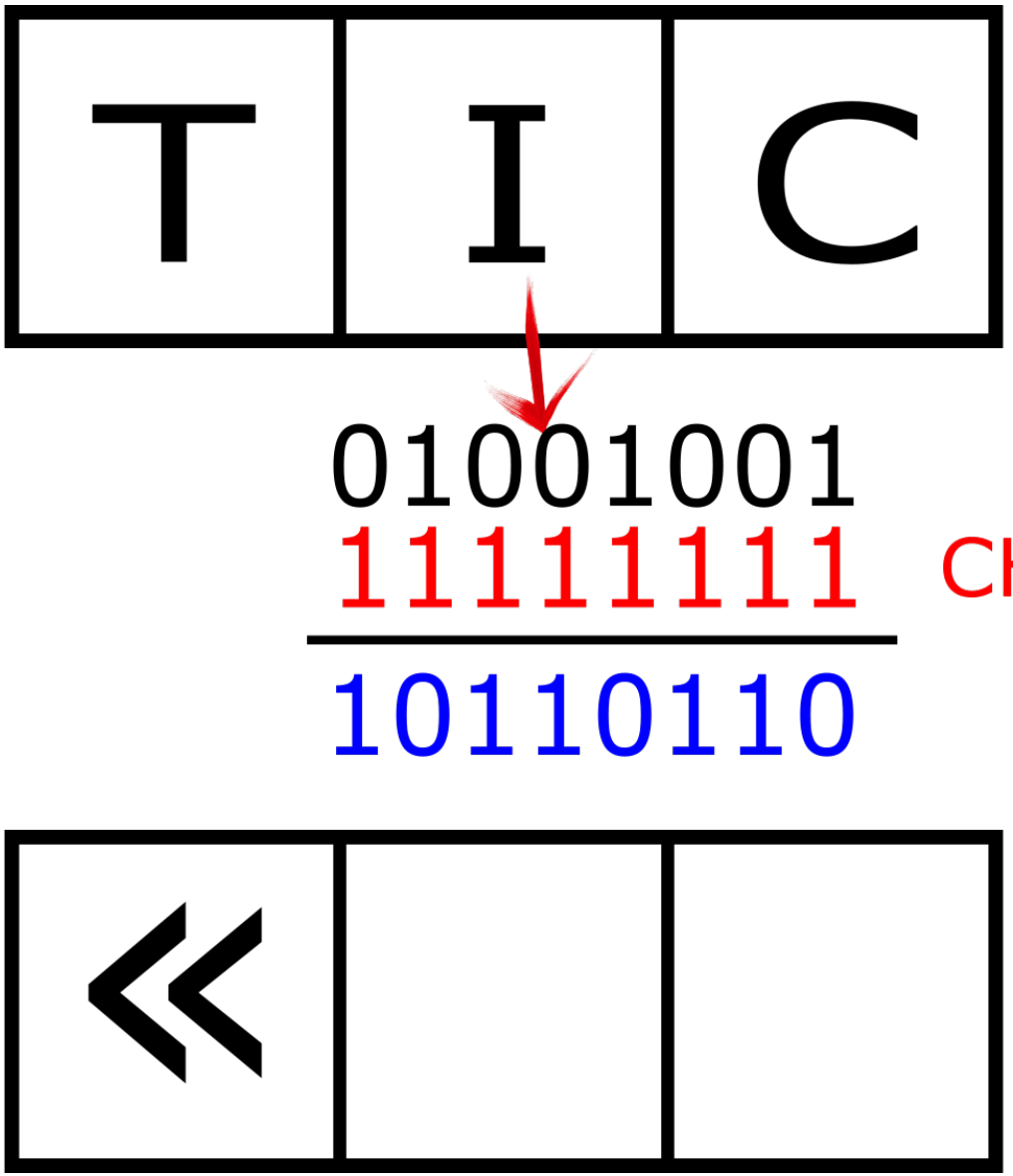
Cifrario OTP



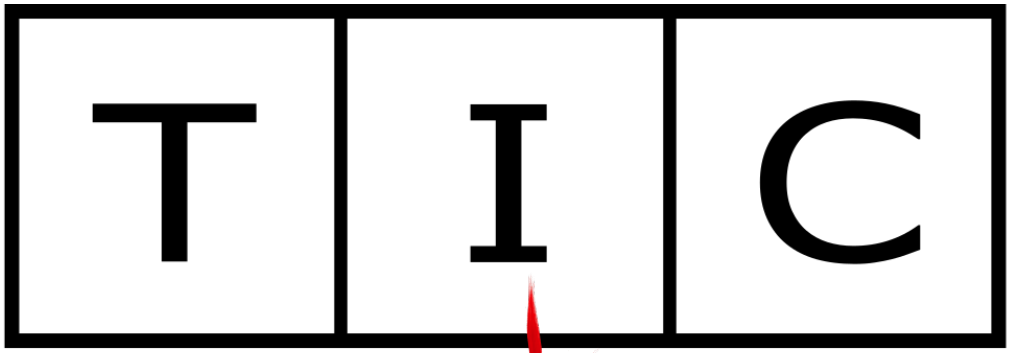
Cifrario OTP



Cifrario OTP



Cifrario OTP



XOR

0 0 = 0

0 1 = 1

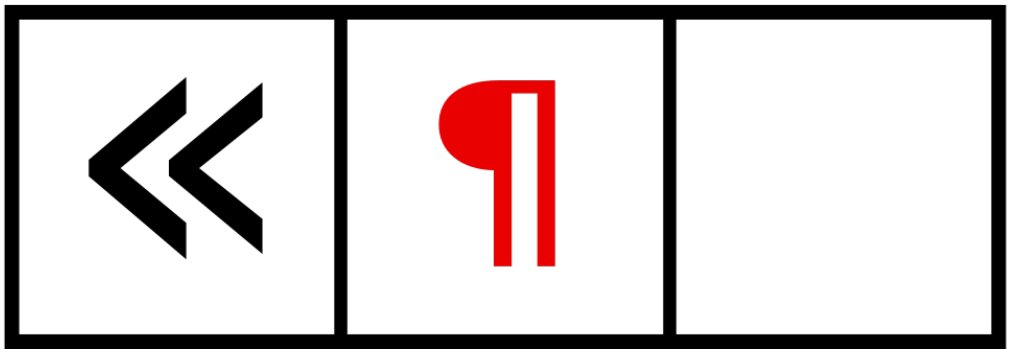
1 0 = 1

1 1 = 0

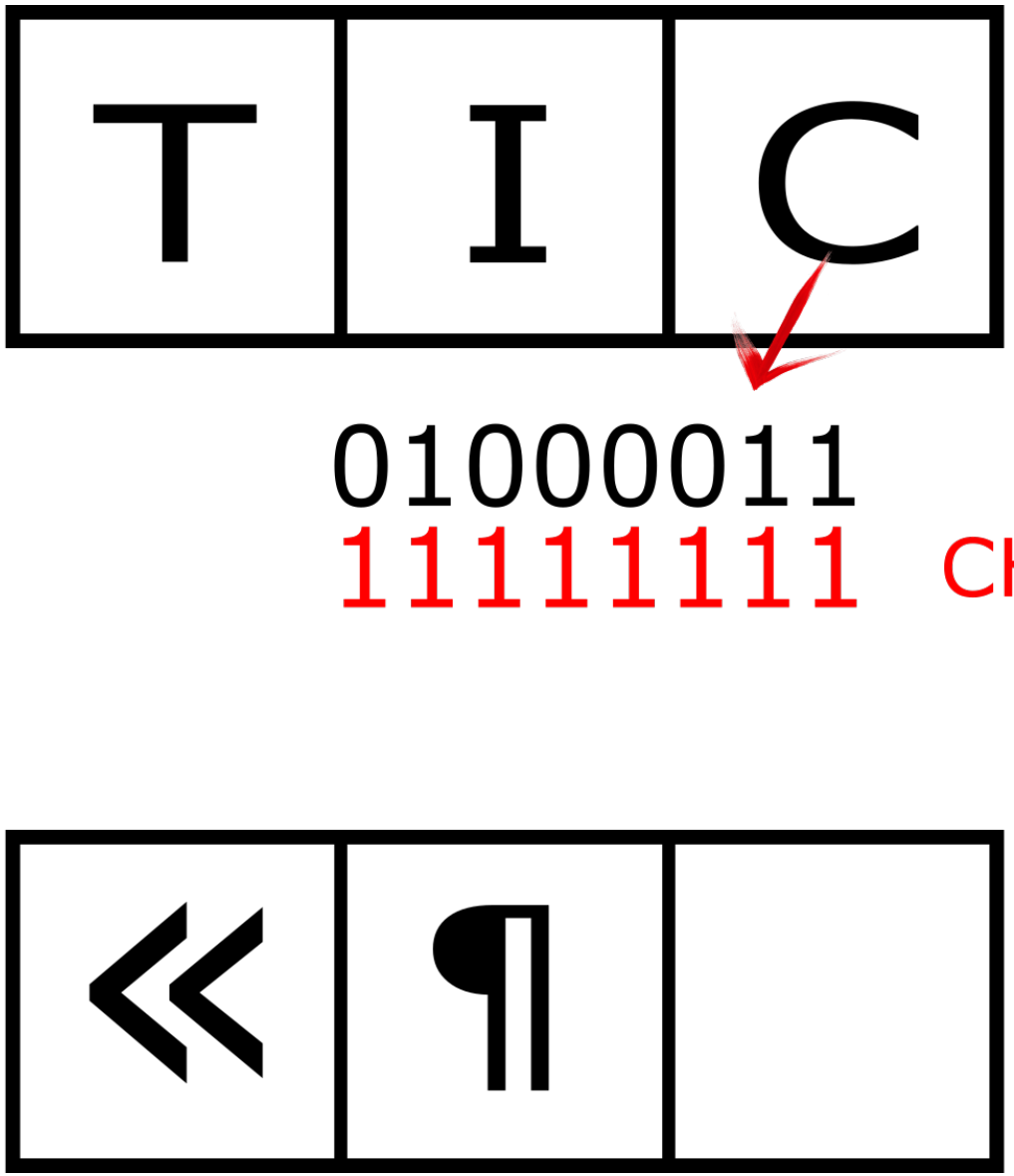
01001001

11111111 CHIAVE

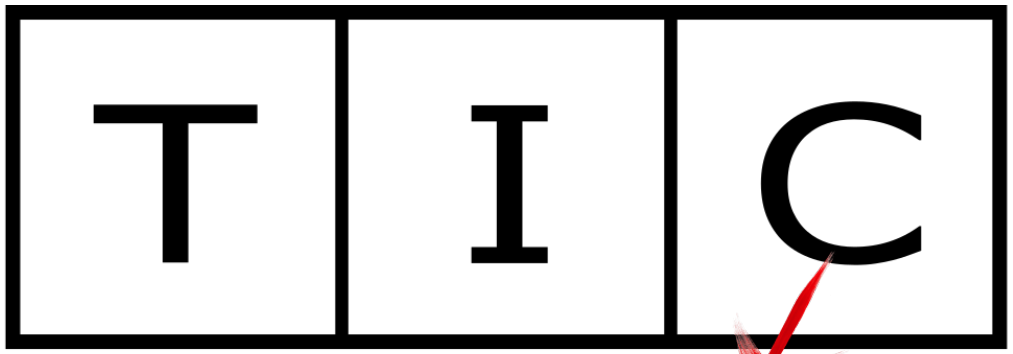
10110110



Cifrario OTP



Cifrario OTP



XOR

0 0 = 0

0 1 = 1

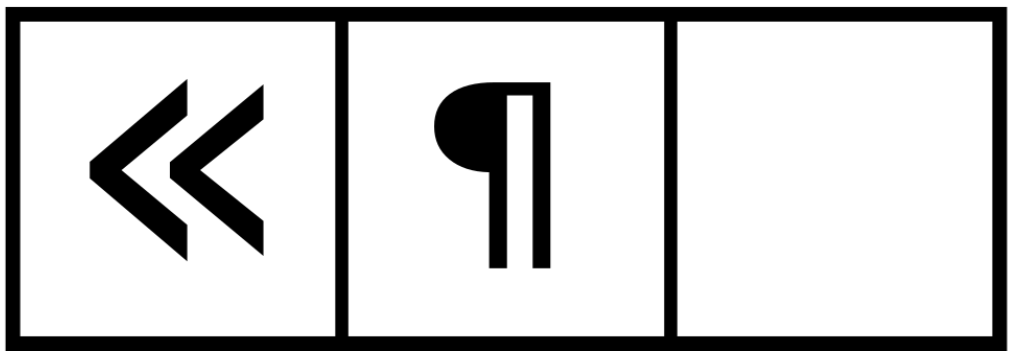
1 0 = 1

1 1 = 0

01000011

11111111 CHIAVE

10111100



Cifrario OTP

T	I	C

XOR

0 0 = 0
0 1 = 1
1 0 = 1
1 1 = 0

01000011
11111111 CHIAVE
10111100

«	¶	¼

Modello RSA

Modello basato sull'utilizzo di chiavi asimmetriche per crittare informazioni da una sorgente ad un destinatario e viceversa. Questo modello è utilizzato ancora oggi per le comunicazioni in rete ad esempio tra clienti e banche o tra utenti e siti web e sta alla base di altri sistemi di sicurezza come i certificati digitali o la firma digitale.

Ogni entità all'interno della rete possiede due chiavi:

- la **CHIAVE PRIVATA** è una sequenza di caratteri privata e segreta. E' l'unica chiave in grado di decifrare messaggi cifrati con la **chiave pubblica**. Messaggi cifrati con la chiave privata possono essere decifrati solo dalla chiave pubblica.
- la **CHIAVE PUBBLICA** è una sequenza di caratteri pubblica e non segreta. E' l'unica chiave in grado di decifrare messaggi cifrati con la **chiave privata**. Messaggi cifrati con la chiave pubblica possono essere decifrati solo dalla chiave privata.

Modello RSA

ELENA

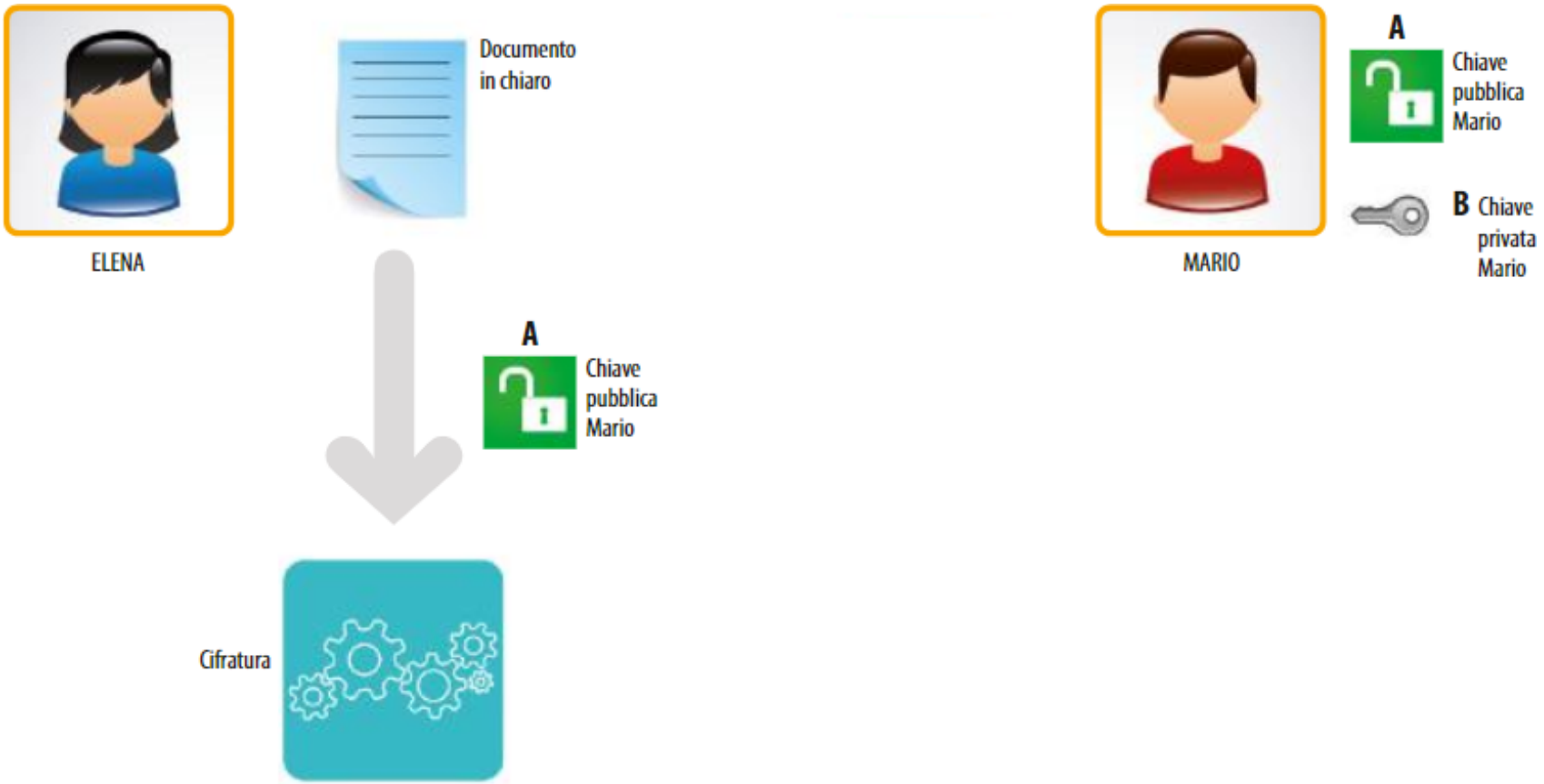
Documento in chiaro

MARIO

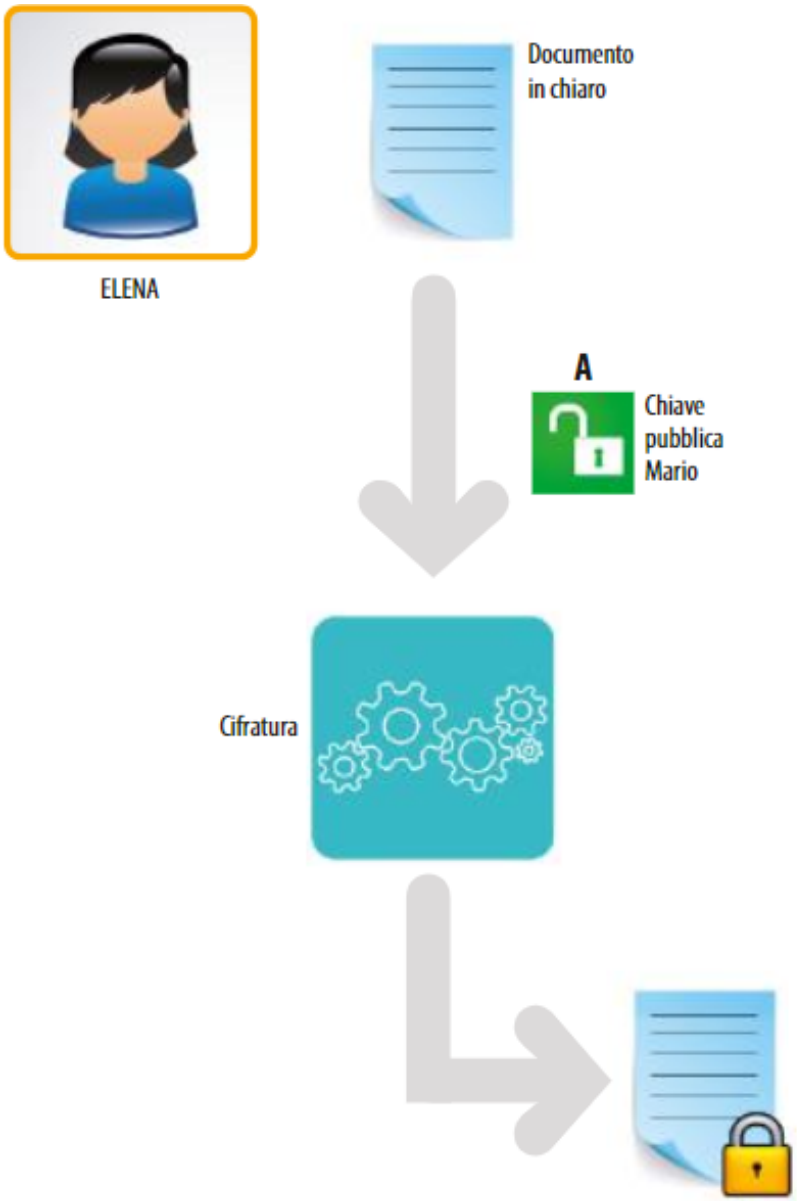
A Chiave pubblica Mario

B Chiave privata Mario

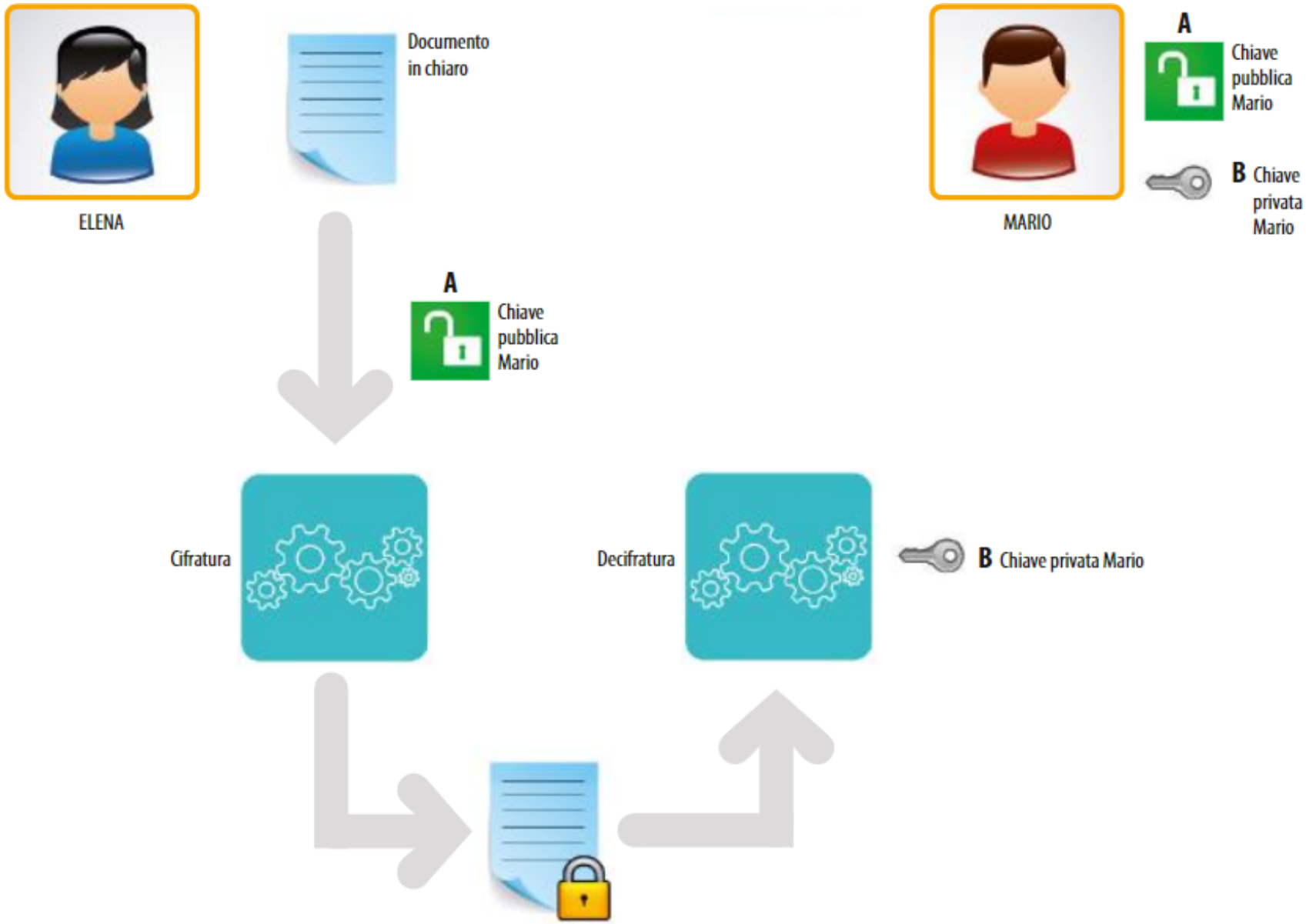
Modello RSA


ELENA
Documento
in chiaro
A
Chiave
pubblica
Mario
Cifratura
MARIO
A
Chiave
pubblica
Mario
B Chiave
privata
Mario

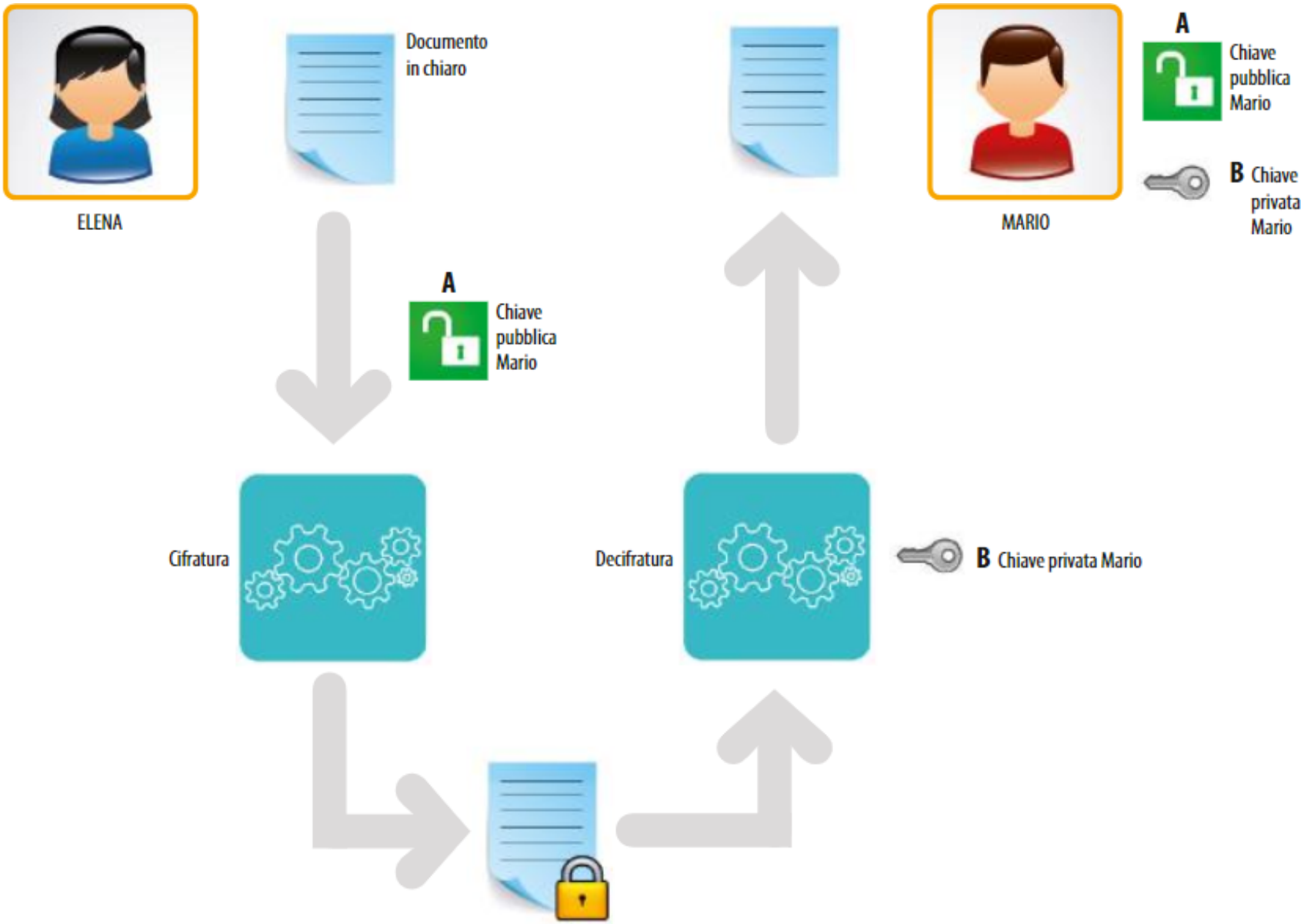
Modello RSA


ELENA
Documento in chiaro
A
Chiave pubblica Mario
Cifratura
MARIO
A
Chiave pubblica Mario
B
Chiave privata Mario

Modello RSA


ELENA
Documento in chiaro
MARIO
A
Chiave pubblica Mario
B Chiave privata Mario
A
Chiave pubblica Mario
Cifratura
Decifratura
B Chiave privata Mario

Modello RSA


ELENA
Documento in chiaro
A
Chiave pubblica Mario
Cifratura
Decifratura
B Chiave privata Mario
MARIO
A
Chiave pubblica Mario
B Chiave privata Mario

Modello RSA

Esempio: NETFLIX