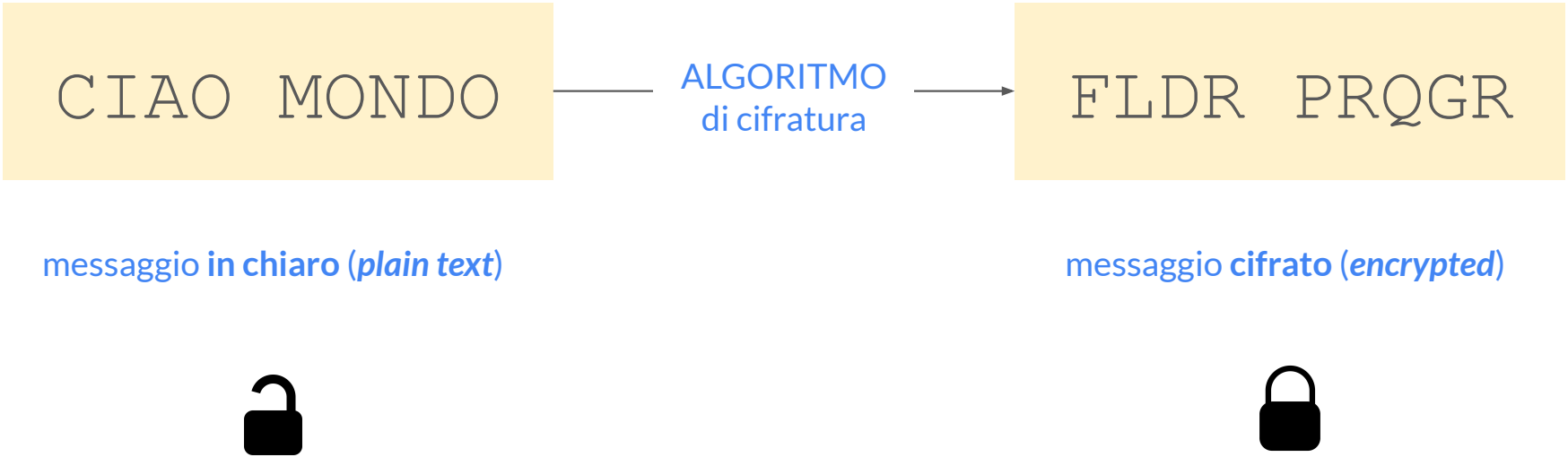
Mini introduzione alla crittografia

16 settembre 2025

Cifratura (*encryption*) di un messaggio



Un semplicissimo algoritmo di cifratura: il **cifrario di Cesare**

Algoritmo: ogni lettera dell'alfabeto (26 lettere) viene spostata in avanti di **3 posizioni**.

Ad esempio: `A → D  B → E  C → F  Z → C`

In generale, possiamo spostare un lettera in avanti di un numero arbitrario di posizioni: questo numero viene chiamato **chiave** del cifrario.

Semplice attività

Scambiatevi (brevi) messaggi cifrati con il cifrario di Cesare, comunicando la chiave al destinatario.

App per il cifrario di Cesare

Attraverso la programmazione (**coding**), possiamo costruire un'applicazione per cifrare e decifrare messaggi di testo in modo automatico.

Il linguaggio di programmazione che utilizzeremo (per questo e per altri progetti) è il **python** →

Live: https://onecompiler.com/python/43wth77nt

cesare.py > cifrario_cesare

```python
def cifrario_cesare(testo, chiave):
    risultato = ""

    for char in testo:
        if char.isalpha():
            base = ord('A') if char.isupper() else ord('a')
            risultato += chr((ord(char) - base + chiave) % 26 + base)
        else:
            risultato += char

    return risultato


# MESSAGGIO E CHIAVE
messaggio = "CIAO MONDO!"
chiave = 3

messaggio_cifrato = cifrario_cesare(messaggio, chiave)
print("Testo originale:", messaggio)
print("Testo cifrato:  ", messaggio_cifrato)
```

Cifrario di Vigenère

- Ogni lettera del messaggio in chiaro viene spostata in avanti di un numero **variabile** di posizioni

- La chiave del cifrario è costituita da una parola, ad esempio `CIAO`

Messaggio in chiaro:	A	V	E		C	E	S	A	R	E
Chiave:	C	I	A	O	C	I	A	O	C	I
Spostamento:	2	8	0	13	2	8	0	13	2	8
Messaggio cifrato:	C	D	E		E	M	S	O	T	M

Live: https://onecompiler.com/python/43wv8qjq4

Compiti

1. Il messaggio `LNBJAN LR OJ DW KJOOX` è stato codificato usando il cifrario di Cesare, di cui però non conosci la chiave. Riesci a trovare la chiave e a decodificare il messaggio?

2. L'ultima parola (in chiaro) del messaggio precedente è la chiave da utilizzare per decifrare il messaggio

   `IAN UVAIFUOAYT JL IWQLTRO DF QSIYYCHRFKC, HTAQLNRSOTN`

   Cosa nasconde?