

# DECIFRATURA

## 1. Messaggio cifrato: HSNFRGH

Analizzando le cifrature più comuni, sono partito con l'ipotesi più semplice: il Cifrario di Cesare, che sposta ogni lettera di un certo numero di posizioni. Ho provato a decifrare "HSNFRGH" con uno **shift inverso da 1 a 5**, per vedere se l'output fosse qualcosa di sensato. Con lo shift -3 ho trovato EPICODE usando l'alfabeto italiano, con alfabeto inglese si ottiene EPKCODE.

Lettera originale	Posizione originale	Shift -3	Nuova lettera
H	7	4	E
S	16	13	P
N	11	8	I
F	5	2	C
R	15	12	O
G	6	3	D
H	7	4	E

**Risultato:**  
**HSNFRGH → EPICODE**

---

## 2. Messaggio cifrato: QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi

Ho applicato lo stesso metodo di cui prima. Vedendo il tipo di messaggio si intuisce la cifratura Base64.

Ogni 4 caratteri Base64 rappresentano 3 byte. Divido il messaggio in gruppi da 4 e mostro cosa rappresentano.

Blocco Base64	Byte decodificati (in esadecimale)	ASCII risultante
QWJh	41 62 61	Aba
IHV6	20 76 7a	vz
b2Vi	6f 65 62	oeb
dHl2	74 79 76	tyv
bmdy	6e 67 72	ngr
IHB1	20 70 75	pu
ciB6	72 20 7a	r z
ciBh	72 20 61	r a
ciBu	72 20 6e	r n
cHBi	70 70 62	ppb
ZXRi	65 74 62	etb

**Messaggio finale dopo decodifica completa unendo tutti i gruppi:**

Aba vzoebtyvngr pur zr ar nppbetb

Il messaggio è ancora incomprensibile, però dalla struttura sembra nuovamente che sia stato usato il Cifrario di Cesare. Dopo diversi tentativi, il messaggio che ha senso compiuto l'ho ottenuto spostando di 13 lettere le lettere originali, che corrisponde a ROT13 in quanto la posizione della lettera 13 è esattamente a metà dell'alfabeto, quindi +13 e -13 sono la stessa cosa. Lo mostro con una tabella qui di seguito.

Lettera originale	Posizione originale	ROT13	Nuova Lettera
A	0	13	N
b	1	14	o
a	0	13	n
	-	-	
v	21	8	i
z	25	12	m
o	14	1	b
e	4	17	r
b	1	14	o
t	19	6	g
y	24	11	l
v	21	8	i
n	13	0	a
g	6	19	t
r	17	4	e
	-	-	
p	15	2	c
u	20	7	h
r	17	4	e
	-	-	
z	25	12	m
r	17	4	e
	-	-	
a	0	13	n
r	17	4	e
	-	-	
n	13	0	a
p	15	2	c
p	15	2	c
b	1	14	o
e	4	17	r
t	19	6	g
b	1	14	o

**Risultato:**

**Aba vzoebtyvngr pur zr ar nppbetb → Non imbrogliate che me ne accorgo**