

Decifrare la seguente chiave:

QWJhIHZ6b2VidHI2bmdyIHB1ciB6ciBhciBucHBiZXRi

Andiamo sul sito jst.io – incolliamo il Token soprastante tra i 2 punti del primo e ultimo Token e premiamo invio(come in screenshot).

Il risultato è l'analisi finale del token.

Le informazioni che abbiamo sono:

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpIHZ6b2VidHI2bmdyIHB1ciB6ciBhciBucHBiZXRi.Sf1KxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE
<pre>{ "alg": "HS256", "typ": "JWT"}</pre>
PAYLOAD: DATA
<pre>"Aba vzoebtyvngr pur zr ar nppbetb"</pre>
VERIFY SIGNATURE
<pre>HMACSHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), your-256-bit-secret)</pre> <div><input type="checkbox"/> secret base64 encoded</div>

- PAYLOAD:

Plaintext: "Aba
vzoebtyvngr pur zr ar
nppbetb"

(Questo è il codice cifrato
da decriptare).

Altra info è che il
token è di 256 bit.

Utilizziamo il nostro alfabeto:

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.

Cerchiamo ora, di capire come decifrare il plaintext: "Aba vzoebtyvngr pur zr ar nppbetb".

Analizzando il testo notiamo subito "Aba".

Ragionandoci capiamo che si riferisce a una parola di 3 lettere in cui la prima e l'ultima che si ripetono.

Per logica mi viene da pensare a parole come: 'Oro', 'Ara', 'Non', 'Ama'.

Come parola chiave prenderemo 'Non' che è la parola più logica da pensare in questo contesto, con questa info procediamo di conseguenza:

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 A-B

A-B←

Ora che abbiamo inserito A e B su N e O – continuiamo tutto l'alfabeto riempiendo tutta la riga sottostante fino a riempimento.

Adesso decifriamolo:

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

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 →Lettere di riferimento slittate di 13

(calcolando che il pc conta dallo 0)

"Aba vzoebtyvngr pur zr ar nppbetb"

"Non imborgilate che me ne accorgo"→ Messaggio finale.

C'è un errore voluto, immagino, dal proprietario del Token, per vedere chi riusciva a decifrarlo e chi no.
Molto simpatico!