Esercizio S3_L4

Consegna:

Esercizio di oggi: Crittografia.

Dato un messaggio cifrato cercare di trovare il testo in chiaro:

Messaggio cifrato: "HSNFRGH"

Secondo esercizio

QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi

Buon divertimento

Svolgimento:

Prima parte

Analizzando la stringa iniziale, mi è subito sembrato che si trattasse di un cifrario di Cesare.

Osservando che la prima e l'ultima lettera erano uguali, ho ipotizzato che potesse trattarsi di una vocale ripetuta, e ho quindi provato ad applicare un ROT7, attribuendo alla lettera "H" il valore di "A". Tuttavia, la parola risultante non aveva alcun significato comprensibile.

h → a

s → l

n → g

f → y

r → k

g → z

h → a

Successivamente, **provando con la vocale "E"**, ho testato una ROT3, e spostando ogni lettera indietro di tre posizioni nell'alfabeto ho ottenuto la parola "**EPKCODE**", molto simile a "**EPICODE**". È plausibile che quest'ultima fosse la parola originaria da criptare.

L'uso della lettera "K" al posto della "I" potrebbe essere dato dal fatto che la "K" non fa parte dell'alfabeto italiano standard, ma è presente in alfabeti stranieri. Supponendo l'impiego del solo alfabeto italiano, il messaggio decifrato corretto sarebbe appunto "EPICODE".

e → h
p → s
i → l
c → f
o → r
d → g
e → h

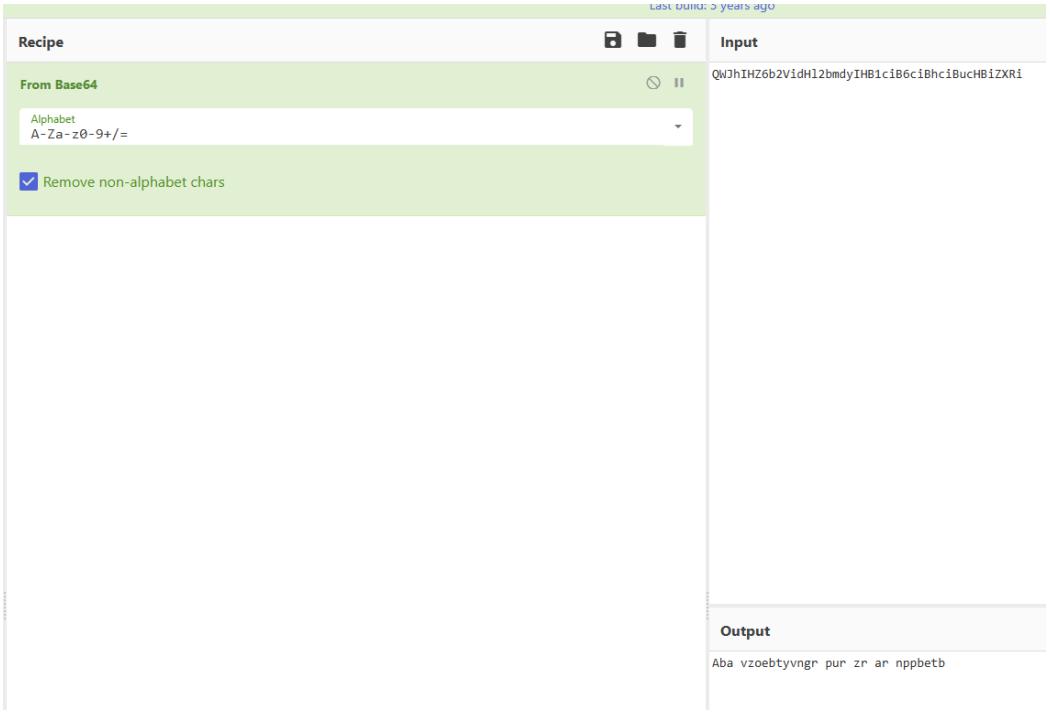
Seconda parte

Il secondo quesito chiede di decifrare la seguente stringa:

QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi

Anche stavolta, avendo già esperienza con il tipo di struttura, mi accorgo essere una cifratura in Base64.

Apro quindi cyberchief.io ed incollo la stringa utilizzando il "From Base64". La decifratura mi restituisce però un output inaspettato:



Aba vzoebtyvngr pur zr ar npgbetb

Provo dunque a reinserire la stringa e utilizzo la modalità di rilevamento automatica disponibile nel sito web; cyberchief mi conferma che la stringa è codificata con Base64 e quindi l'output deve essere corretto.

Analizzando meglio la stringa decodificata intuisco che potrebbe essere stata cifrata ancora una volta con il cifrario di cesare.

Prendo come inizio la prima parola e mi soffermo, **come in precedenza**, sulla **prima e l'ultima lettera** e provo mentalmente a cambiarle in contemporanea per tentare di trovare quale parola di 3 lettere, con **prima e terza uguali tra loro**, possa aver senso.

Su due piedi ho **escluso la possibilità che tutte e 3 le lettere potessero essere delle vocali e consonanti.** Ed ho quindi proceduto a **tentativi**; per ogni vocale cercavo di formare una parola avente una consonante come lettera centrale e, per ogni consonante sostituivo la centrale con una vocale.

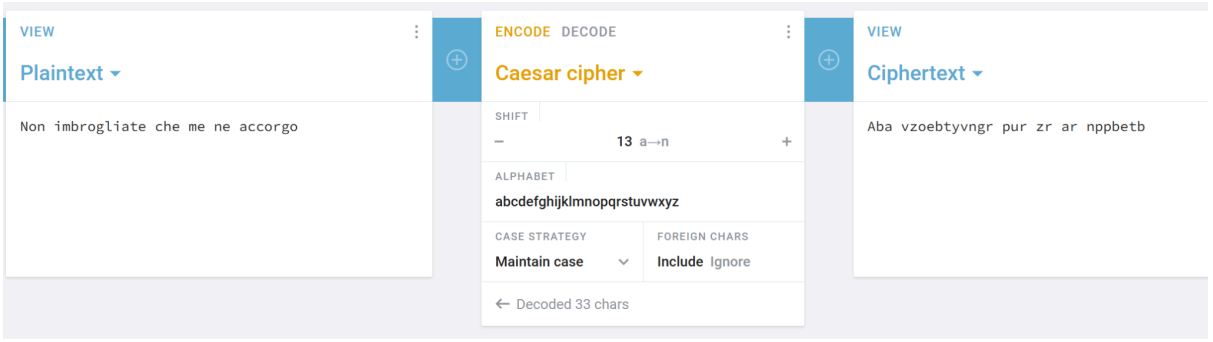
Non sapendo il linguaggio in cui la frase sarebbe stata scritta ho quindi considerato anche parole per lo meno in lingua inglese.

Ho quindi proceduto in questo modo volendo stilare una lista prima di applicare la ROT a tutta la frase.

- a_a → Ala? Ada? Ana?
- b_b -> Bob?
- c_c → ??
- d_d -> Dad?
- e_e → Ele?
- g_g →??
- h_h →??
- i_i →??
- l_l → Lol?
- m_m → Mum?
- **n_n → Non?**

Avevo finalmente trovato una parola sensata in lingua italiana.

A quel punto ho cercato su internet un decoder online e con sorpresa ho scoperto di aver "sprecato tempo" inutilmente in quanto sarebbe stato sufficiente sin dall'inizio incollare la frase e rapidamente cambiare ROT per decriptare il codice con diverse rotazioni.



"Non imbrogliate che me ne accorgo"

Questa era la frase criptata da due algoritmi. Prima un cifrario di Cesare in ROT13 e successivamente il suo output era stato cifrato in Base64.

Conclusione:

Questo esercizio ha dimostrato come sia utile combinare diversi strumenti (analisi manuale, prove empiriche, e tool online) per risolvere problemi crittografici. In particolare, l'uso di **ROT13 + Base64** è una tecnica comune per oscurare testi in modo semplice ma efficace.