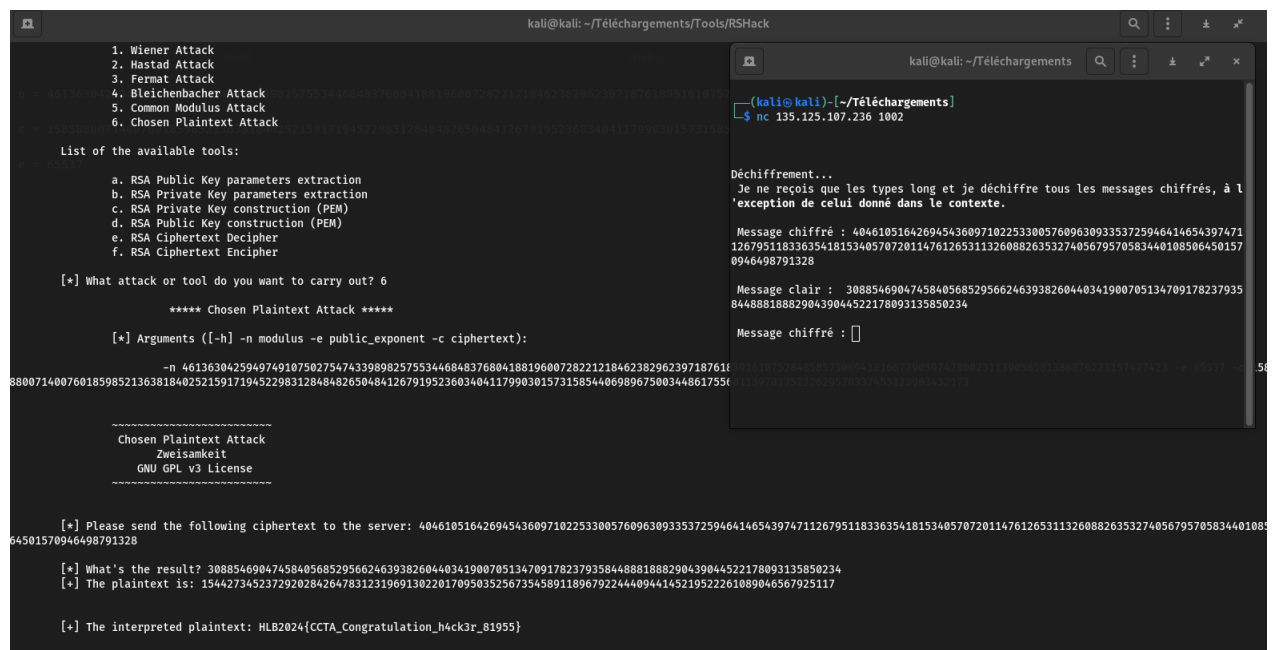


korp_station

Writeup pour CACT

C'est un challenge RSA on nous donne les valeurs de n, c, e ainsi qu'un serveur qui déchiffrait nos entrées à l'exception de celle du challenge évidemment. Ça sentait **Chosen Plaintext Attack**. Pour vérifier mon intuition j'ai utilisé RShack.



```
kali@kali: ~/Téléchargements/Tools/RShack

1. Wiener Attack
2. Hastad Attack
3. Fermat Attack
4. Bleichenbacher Attack
5. Common Modulus Attack
6. Chosen Plaintext Attack

List of the available tools:

a. RSA Public Key parameters extraction
b. RSA Private Key parameters extraction
c. RSA Private Key construction (PEM)
d. RSA Public Key construction (PEM)
e. RSA Ciphertext Decipher
f. RSA Ciphertext Encipher

[*] What attack or tool do you want to carry out? 6

***** Chosen Plaintext Attack *****

[*] Arguments ([-h] -n modulus -e public_exponent -c ciphertext):

-n 46136304259497491075027547433989825755344684837680418819600728221218462382962397187611
88007140076018598521363818402521591719452298312848482650484126791952360340411799030157315854406989675003448617551

-----
Chosen Plaintext Attack
Zweisamkeit
GNU GPL v3 license
-----

[*] Please send the following ciphertext to the server: 404610516426945436097102253300576096309335372594641465439747112679511833635418153405707201147612653113260882635327405679570583440108504501570946498791328

[*] What's the result? 308854690474584056852956624639382604403419007051347091782379358448881888290439044522178093135850234
[*] The plaintext is: 154427345237292028426478312319691302201709503525673545891189679224440944145219522261089046567925117

[*] The interpreted plaintext: HLB2024{CCTA_Congratulation_h4ck3r_81955}
```

Flag : HLB2024{CCTA_Congratulation_h4ck3r_81955}