

CTF:Qualifications Stage
Auteur:foundhack



C'est un challenge de cryptographie. Dès que j'ai vu le challenge, je me suis directement connectée au serveur avec la commande nc.



J'ai téléchargé le fichier .txt et j'ai vu que c'était du RSA. Comme je suis sur le serveur, nous avons ces messages : le serveur reçoit uniquement des réponses de type long. Je me suis

dit que si je factorise le n , je n'aurai pas directement la clé. Et la valeur de n était infactorisable. J'ai alors pensé à l'attaque par texte clair choisi (Chosen Plaintext Attack). J'ai lancé directement mon outil RSHack que j'utilise souvent pendant les CTFs RSA.

```
#      GNU GPL v3
##### kali@kali: ~/Bureau/RSHack

List of the available attacks:

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? █
```

Voici comment j'ai procédé :

```
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 46136304259497491075027547433989825755344684837680418819600728221218462382962397187618591610752848585750694
18166779059742800231139056581386876223157477423 -e 65537 -c 15858800714007601859852136381840252159171945229831284848265048412679195236
03404117990301573158544069896750034486175560113978175222629578337455123963432173 █
```

J'ai obtenu des résultats de type long que je devais envoyer au serveur pour qu'il les déchiffre.

```
#####
Chosen Plaintext Attack
Zweisamkeit
GNU GPL v3 License
#####

[*] Please send the following ciphertext to the server: 4046105164269454360971022533005760963093353725946414654397471126795118
336354181534057072011476126531132608826353274056795705834401085064501570946498791328

[*] What's the result? █
```

```

(kali@kali)-[~]
$ nc 135.125.107.236 1002
Déchiffrement...
Je ne reçois que les types long et je déchiffre tous les messages chiffrés, à l'exception de celui donné dans le contexte.
Message chiffré : 404610516426945436097102253300576096309335372594641465439747112679511833635418153405707201147612653113260882635327
4056795705834401085064501570946498791328
Message clair : 308854690474584056852956624639382604403419007051347091782379358448881888290439044522178093135850234
Message chiffré : 

```

Lorsque j'ai reçu les messages en clair, je les ai envoyés à mon outil RSHack pour qu'il les déchiffre.

```

[*] Please send the following ciphertext to the server: 4046105164269454360971022533005760963093353725946414654397471126795118
336354181534057072011476126531132608826353274056795705834401085064501570946498791328
[*] What's the result? 308854690474584056852956624639382604403419007051347091782379358448881888290439044522178093135850234
[+] The plaintext is: 154427345237292028426478312319691302201709503525673545891189679224440944145219522261089046567925117
    Lorsque j'ai eu le messages en clair j'ai copier ça et j'ai renvoyer à mon outils Rshack
[+] The interpreted plaintext: HLB2024{CCTA_Congratulation_h4ck3r_81955}

```

```

(kali@kali)-[~/Bureau/RSHack]
$ 

```

Et voilà, j'ai le flag : **HLB2024{CCTA_Congratulation_h4ck3r_81955}**

Écrit par : foundhack

```

[*] Please send the following ciphertext to the server: 4046105164269454360971022533005760963093353725946414654397471126795118
336354181534057072011476126531132608826353274056795705834401085064501570946498791328
[*] What's the result? 308854690474584056852956624639382604403419007051347091782379358448881888290439044522178093135850234
[+] The plaintext is: 154427345237292028426478312319691302201709503525673545891189679224440944145219522261089046567925117
    Lorsque j'ai eu le messages en clair j'ai copier ça et j'ai renvoyer à mon outils Rshack
[+] The interpreted plaintext: HLB2024{CCTA_Congratulation_h4ck3r_81955}

```

```

(kali@kali)-[~/Bureau/RSHack]
$ 

```