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.

Voici comment j'ai procédé :

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

```
┌──(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 :  40461051642694543609710225330057609630933537259464146543974711267951183363541815340570720114761265311326088263532740567957058344010850645015709464987913280
40567957058344010850645015709464987913328

 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: 40461051642694543609710225330057609630933537259464146543974711267951183
3363541815340570720114761265311326088263532740567957058344010850645015709464987913280

       [*] What's the result? 308854690474584056852956624639382604403419007051347091782379358448881888290439044522178093135850234
       [+] The plaintext is: 1544273452372920284264783123196913022017095035256735458911896792244409441452195222610890465679251170

       [+] 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: 40461051642694543609710225330057609630933537259464146543974711267951183
3363541815340570720114761265311326088263532740567957058344010850645015709464987913280

       [*] What's the result? 308854690474584056852956624639382604403419007051347091782379358448881888290439044522178093135850234
       [+] The plaintext is: 1544273452372920284264783123196913022017095035256735458911896792244409441452195222610890465679251170

       [+] The interpreted plaintext: HLB2024{CCTA_Congratulation_h4ck3r_81955}

┌──(kali㉿kali)-[~/Bureau/RSHack]
└─$
```