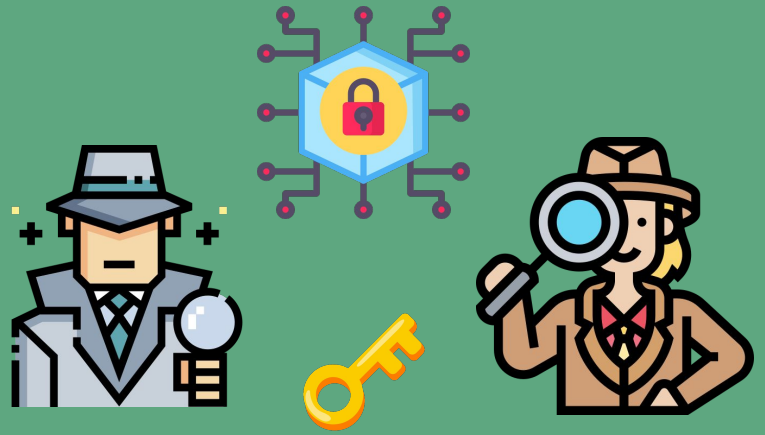
Detetives criptográficos



Precisa-se de detetives

Um renomado criptógrafo faleceu e deixou sua valiosa herança escondida.
Para encontrá-la, é necessário seguir uma trilha de pistas criptográficas, cada uma revelando um segredo crucial para o próximo passo.

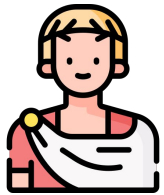
LabSEC
Laboratório de Segurança em Computação

cpqd

Passo 1

A jornada segue para um cofre sombrio, onde a próxima pista está trancada. A chave para abrí-lo está escondida na mensagem abaixo, protegida pela cifra do imperador. Decifre-a para revelar primeira pista.

D mruqdgd frqwlqxd qr dutxlyr vrpeulr. Xvh DHV frp fkdyh vhjuhgr h prgr gh rshudfdr FEF



LabSEC
Laboratório de Segurança em Computação

cpqd

Passo 2

A jornada continua e o trabalho do detetive é árduo! Utilize a pista do **Passo 1** para decifrar a mensagem cifrada no *arquivo sombrio*.

Dica: a mensagem foi cifrada usando o *openssl*. Use os conhecimentos da semana 2 para decifrá-la.

Passo 3

O próximo arquivo será revelado por uma chave secreta K.
Essa chave foi calculada utilizando o protocolo do senhor D e do senhor H.

Use os parâmetros revelados no **Passo 2** e seus conhecimentos sobre exponenciação modular para atacar o protocolo e descobrir K.

Dica: a aula S3A2 pode ajudar, discutimos uma questão muito parecida lá!

Passo 4

Duas dicas competem pela verdade, apenas a assinatura digital revelará qual guia para o tesouro final.

Verifique a assinatura *s.bin* para descobrir qual dica seguir.
O arquivo com a chave pública foi revelado pelo valor de K no **Passo 3**.

Dica: a aula S4A2 pode ajudar com essa verificação

Passo 5

A jornada está chegando ao fim! Use as dicas do passo anterior para decifrar a mensagem final.

Dica: a verdade(.py) pode auxiliar nesse processo.

LabSEC
Laboratório de Segurança em Computação

cpqd

Parabéns!