Rapport de Projet : CryptoHack

Victor Bailleul Sébastien Leglise

Université de Caen Normandie / ENSICAEN

Année 2025-2026

Plan de la présentation

Contexte du projet

- Présentation de la plateforme CryptoHack.
- Rôle de la cryptographie en cybersécurité.
- Intérêt des CTF pour l'apprentissage.

Objectifs du challenge

- Quel est le but ?
- Quelle vulnérabilité est exploitée ?

Méthode de résolution

- Étape 1 : ...
- Étape 2 : ...
- Étape 3 : ...

Résultat et Flag

- Le flag obtenu est :
- `crypto{...}`

Objectifs du challenge

Forger une signature RSA valide

- Voter pour Pedro sans clé privée
- Exploiter l'exposant faible $e = 3$
- Obtenir le flag

Attaque par racine cubique

$$\text{Signature } s = \sqrt[3]{\text{Message}}$$

$$s^3 \equiv \text{Message} \pmod{N}$$

- Message court = "VOTE FOR PEDRO"
- Pas de padding = vulnérabilité

Résultat et Flag

Signature forgée validée !

Flag obtenu

`crypto{y0ur_v0t3_i5_my_v0t3}`

- Vote accepté par le serveur
- Attaque réussie en quelques secondes

Bilan du projet

- Compétences acquises.
- Difficultés rencontrées.
- Perspectives et suite possible.

Questions ?