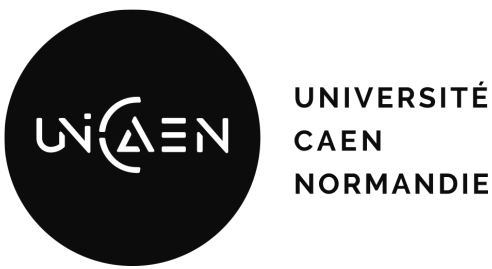
Rapport de Projet : CryptoHack

Victor Bailleul Sébastien Leglise

Université de Caen Normandie / ENSICAEN

Année 2025-2026



Plan de la présentation

Contexte du projet

La plateforme CryptoHack

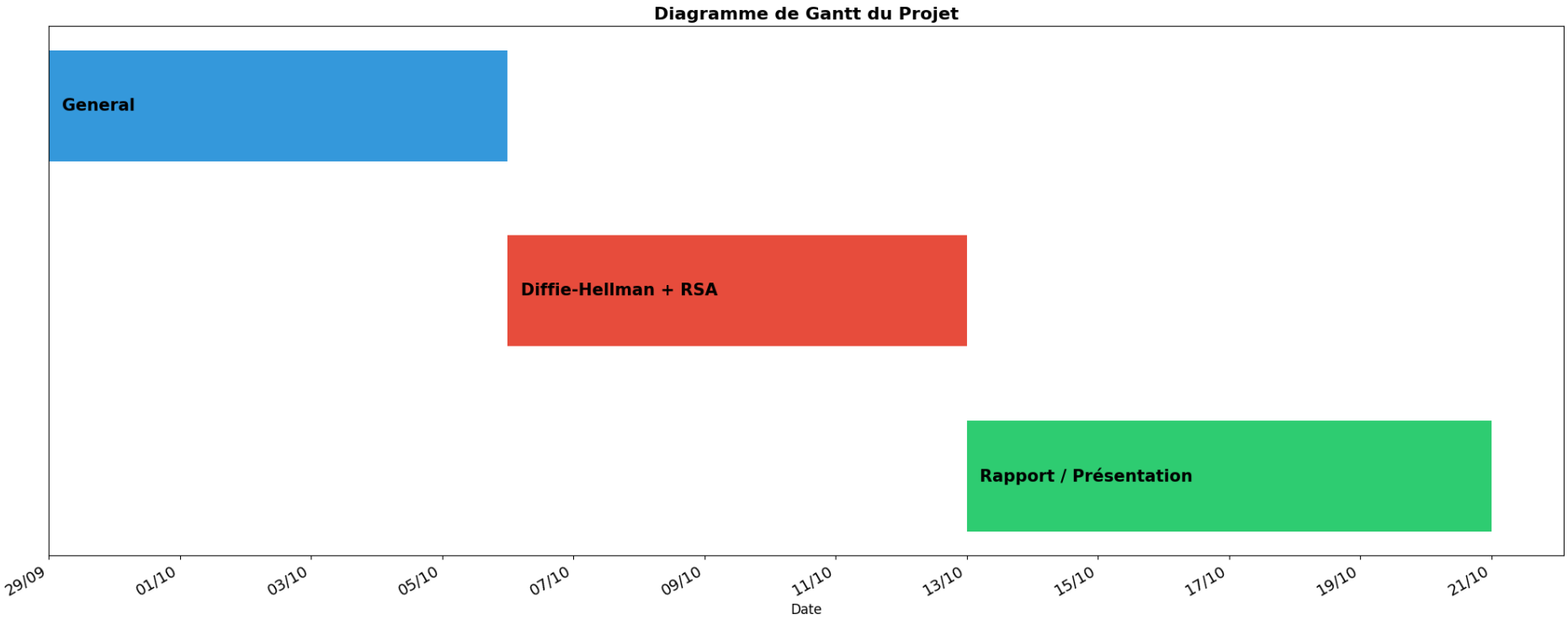
- Plateforme d'apprentissage dédiée à la cryptographie moderne.
- Approche pratique : résolution de défis à difficulté croissante.
- Objectif : enseigner les concepts fondamentaux et avancés.

L'intérêt des challenges de type CTF (*Capture The Flag*)

- **Principe :** *Gamification* de l'apprentissage en cybersécurité.
- **Bénéfices :**
  - Ancrage des connaissances par la pratique.
  - Développement de compétences techniques (analyse, résolution de problèmes).

Organisation du projet

Planification



Organisation du projet

Travailler en binôme

Répartition des tâches individuelles

	Catégorie de challenges abordées
Victor	General/**Encoding**, General/**XOR**, **Diffie-Hellman**
Sébastien	General/**Mathematics**, General/**Data Formats**, **RSA**

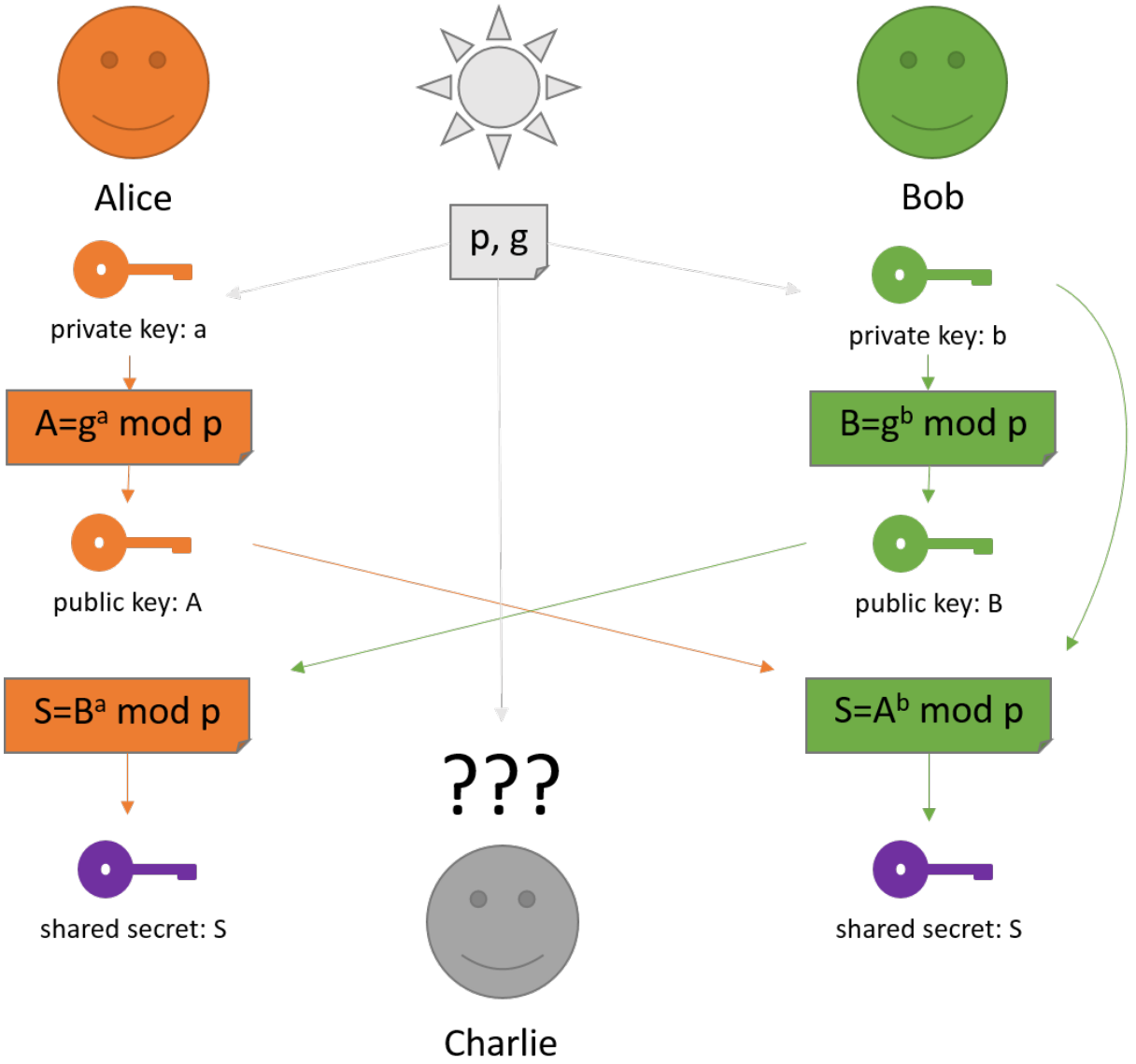
Travail commun et collaboration

L'ensemble du projet a été géré via un dépôt Git partagé sur GitHub. Cette approche nous a permis de :

- **Centraliser le code** et les documents du projet.
- **Suivre les versions** pour éviter les conflits et les pertes de données.
- **Collaborer de manière asynchrone** sur les différentes parties du rapport et du code.

Diffie-Hellman : *Man-in-the-middle | Export grade*

Objectifs



Diffie-Hellman : *Man-in-the-middle | Export grade*

Méthode de résolution

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

Diffie-Hellman : *Man-in-the-middle | Export grade*

Résultat

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

Objectifs du challenge

Forger une signature RSA valide

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

Méthode de résolution

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 ?