UNIVERSITÉ
CAEN
NORMANDIE

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

Projet CryptoHack

Rapport de Communication – Master 1 Cybersécurité

Alexis Debra Martin Vicquelin

Université de Caen – Année 2025–2026

Octobre 2025

Plan de la présentation

Objectif du projet

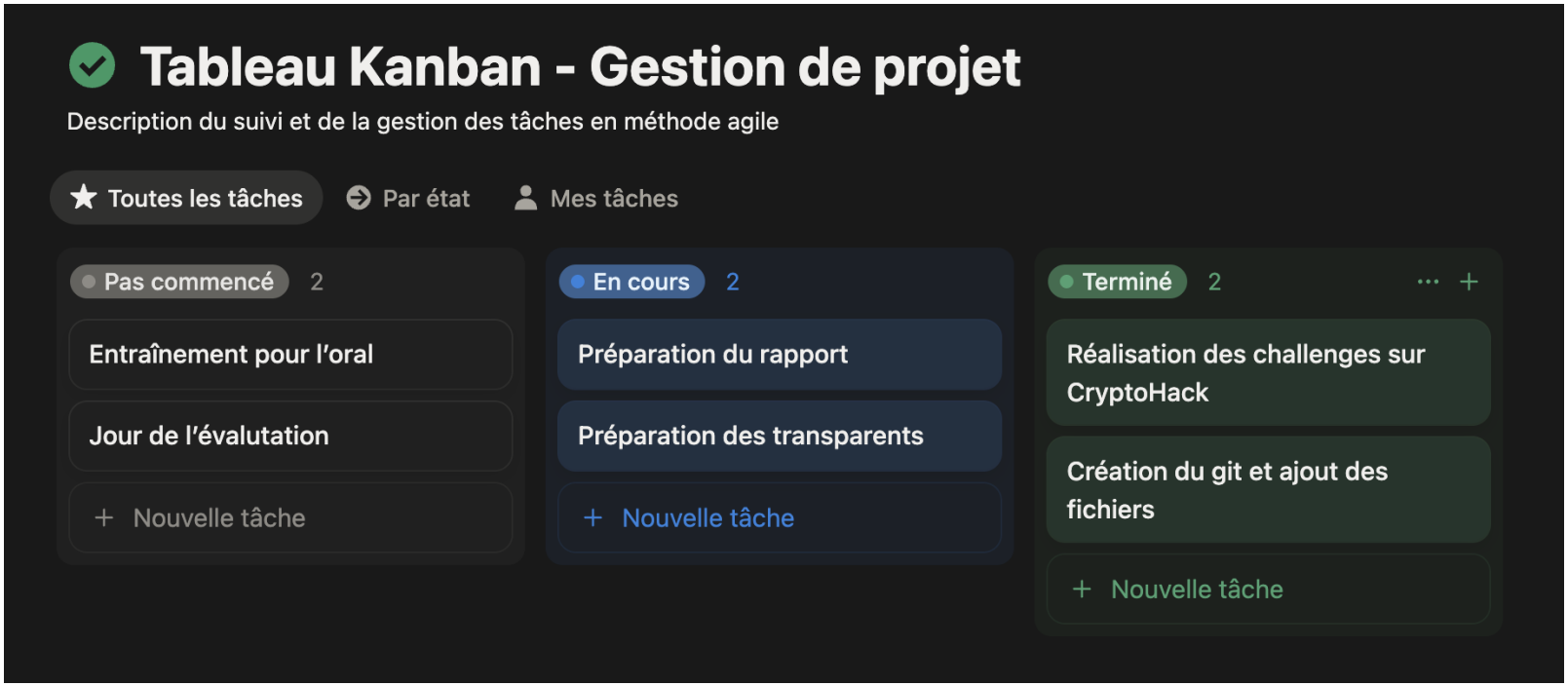
- Réaliser un mini-projet dans le cadre du cours de **Communication**.
- Mettre en pratique les outils vus en cours : LaTeX, Git, gestion de projet agile.
- Résoudre plusieurs **challenges de cryptographie** sur CryptoHack.

Thèmes principaux : arithmétique modulaire, RSA, Diffie-Hellman, AES, sécurité web (JWT, TLS).

Présentation de CryptoHack

- Plateforme interactive d'apprentissage de la cryptographie.
- Les challenges couvrent mathématiques, chiffrement symétrique/asymétrique, protocoles réseau.
- Chaque défi s'appuie sur du code Python et un concept théorique.

Organisation et outils



Outils utilisés :

- **GitHub** – versionnement et partage du code
- **LaTeX** – rédaction du rapport et des slides
- **Notion (Kanban)** – suivi agile des tâches

Challenge 1 — Lemur XOR (Fondamentaux)

Objectif : comprendre l'opération XOR et son rôle dans le chiffrement.

Principe

Appliquer un XOR pixel par pixel entre deux images pour révéler une image cachée :

```
for x in range(lemur.width):
    for y in range(lemur.height):
        l = lemur.getpixel((x, y))
        f = flag.getpixel((x, y))
        flag.putpixel((x, y), tuple(a^b for a, b in zip(l,f)))
```

Résultat : illustration de la réversibilité du XOR $\rightarrow$ base du chiffrement par flot.

Challenge 2 — RSA Signatures

Objectif : comprendre la signature numérique RSA.

- Calcul de l'empreinte SHA256 du message.
- Chiffrement de cette empreinte avec la clé privée.
- Vérification avec la clé publique.

Résultat : authentification et intégrité du message prouvées sans le révéler.

Challenge 3 — Diffie-Hellman

Objectif : trouver un générateur dans un groupe multiplicatif fini.

Théorème

α est un générateur si

$$\alpha^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \quad \forall q \mid (p-1)$$

Résultat : illustration du choix d'un bon générateur pour sécuriser l'échange de clé.

Challenge 4 — AES (Chiffrement symétrique)

Objectif : comprendre les mécanismes internes d'AES. **Fonctions principales :**

- `ShiftRows()` : diffusion horizontale.
- `MixColumns()` : mélange vertical.
- `Inv_ShiftRows()` et `Inv_MixColumns()` : déchiffrement.

Résultat : compréhension des notions de *confusion* et *diffusion*.

Bilan et apprentissages

Difficultés rencontrées :

- Manipulation mathématique (groupes, totient, inverse mod n)
- Gestion du temps entre théorie et pratique

Compétences acquises :

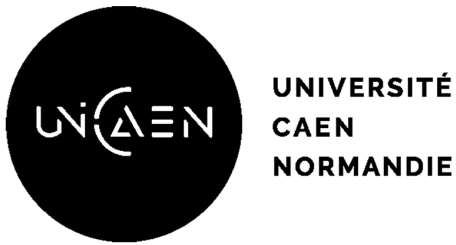
- Meilleure compréhension de RSA, AES, Diffie–Hellman
- Pratique de la cryptanalyse en Python
- Utilisation d'outils pro : Git, Notion, LaTeX

Conclusion et perspectives

- Projet concret liant théorie et pratique en cryptographie.
- Mise en œuvre complète : Python, Git, LaTeX, gestion de projet agile.
- Volonté de poursuivre sur :
  - Cryptographie moderne (ECC, post-quantique)
  - Plateformes de défis (CryptoHack, TryHackMe)
- Nos profils :
  - **Alexis Debra — ScaRed**
  - **Martin Vicquelin — mv9lagrintaa**

Merci pour votre attention !

Questions ?



Projet CryptoHack – Master 1 Cybersécurité, Université de Caen (2025–2026)