HAI709I - TD 9

Rocco Mora

24 Novembre, 2025

Exercice 1 :

Étant donné un algorithme $\mathcal{A}$ qui résout le problème de factorisation, montrez un algorithme $\mathcal{A}'$ qui résout le problème RSA.

Exercice 2 :

Définissez formellement l'expérience CDH et la notion de difficulté associée. Ensuite, étant donné un algorithme $\mathcal{A}$ qui résout le problème du logarithme discret, montrez un algorithme $\mathcal{A}'$ qui résout le problème calculatoire de Diffie-Hellman.

Exercice 3 :

Soit $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ un schéma de chiffrement à clé privée CPA-sûr. Nous construisons le protocole d'échange de clés suivant :

- Alice échantillonne $m_A \leftarrow \texttt{Gen}(1^n)$ et l'envoie à Bob.
- Bob échantillonne la clé k_B et la chiffre sous la forme $m_B \leftarrow \texttt{Enc}_{m_A}(k_B)$, puis envoie m_B à Alice.
- Alice calcule $k_A := \texttt{Dec}_{m_A}(m_B)$.

Prouvez que le schéma ci-dessus est un protocole d'échange de clés correct, mais qu'il n'est pas EAV-sûr.

Exercice 4 :

Considérez le protocole d'échange de clés suivant :

- Alice choisit de manière uniforme $k, r \in \{0,1\}^n$ et envoie $s := k \oplus r$ à Bob.
- Bob choisit uniformément $t \in \{0,1\}^n$, et envoie $u := s \oplus t$ à Alice.
- Alice calcule $w := u \oplus r$ et envoie w à Bob.
- Alice affiche k et Bob affiche $w \oplus t$.

Montrez qu'Alice et Bob produisent la même clé. Analysez la sécurité du schéma (c'est-à-dire prouvez sa sécurité ou montrez une attaque concrète).