



Documents non autorisés. Détaillez vos réponses.

Exercice 1.

1. Décrire le fonctionnement de la signature RSA.
2. Alice a pour clef publique $(n, e) = (143, 7)$ et clef privée $d = 103$. Vérifier que ce choix convient.
3. Calculer la signature d'Alice pour le message $m = 5$.
4. Alice a signé le message $m = 79$ par la signature $\sigma = 118$. Vérifier que cette signature est correcte.

Exercice 2.

Soit n un entier produit de deux nombres premiers distincts p et q . On note e , un nombre premier avec $\varphi(n)$. Alice utilise la signature RSA avec (n, e) pour clef publique. On note d sa clef privée.

1. Oscar récupère les signatures valides σ_1 et σ_2 de deux messages m_1, m_2 dans $\mathbb{Z}/n\mathbb{Z}$, signés par Alice. Montrer comment Oscar peut construire la signature valide d'un autre message.

2. Oscar souhaite obtenir la signature valide d'Alice d'un message $m \in \mathbb{Z}/n\mathbb{Z}$, signifiant "Alice doit 1000 € à Oscar". Montrer, en utilisant la question précédente, comment Oscar peut arriver à ses fins en demandant à Alice de signer deux messages apparemment anodins.

3. Montrer comment Oscar peut construire un message (peut-être sans sens) et sa signature valide, sans interaction avec Alice.

4. On utilise maintenant une fonction de hachage h à valeurs dans $\mathbb{Z}/n\mathbb{Z}$. Alice signe un message m en calculant $\sigma = h(m)^d$ dans $\mathbb{Z}/n\mathbb{Z}$. On dit qu'une signature σ' d'un message m' est valide si et seulement si $\sigma'^e = h(m')$ dans $\mathbb{Z}/n\mathbb{Z}$. À quelle condition l'attaque de la première question ne fonctionne plus ?

5. Si h est à sens unique, l'attaque de la question 3. est-elle possible ?

6. On suppose que h n'est pas résistante à la 2e pré-image. Oscar récupère la signature valide σ d'un message m . Montrer comment Oscar peut construire une signature valide pour un message différent de m .