TD 11 : Signatures Numériques

christina.boura@uvsq.fr

17 avril 2018

Exercice 1 *Calculer et vérifier une signature RSA*

On suppose qu'Alice a comme clé publique $(n, e) = (143, 7)$ et comme clé privée $d = 103$.

1. Vérifier que ces deux choix sont conformes au protocole RSA (on suppose connaître $143 = 11 \cdot 13$).
2. Calculer la signature d'Alice pour le message $m = 3$. (**Indice** : $3^{15} \equiv 1 \mod 143$ et $3^6 \equiv 14 \mod 143$)
3. Alice a signé le message $m = 15$ par la signature $s = 141$. Vérifier que cette signature est valide.

Exercice 2 *Vérification d'une signature RSA*

Les signatures suivantes ont été obtenues avec la clé publique $(n, e) = (77, 7)$. Lesquelles parmi ces signatures sont valides ?

1. $(m, s) = (31, 3)$
2. $(m, s) = (37, 9)$
3. $(m, s) = (25, 9)$

Exercice 3 *Attaque sur la signature RSA*

Supposons que n soit un entier produit de deux nombres premiers distincts p et q. Soit e un entier premier avec $\phi(n)$. Alice utilise la signature RSA avec (n, e) comme clé publique. On note d sa clé privée.

1. Oscar récupère les signatures valides s_1 et s_2 de deux messages m_1, $m_2 \in \mathbb{Z}_n$, signés par Alice. Montrer comment Oscar peut construire la signature valide d'un autre message.
2. Montrer comment Oscar peut construire un message (possiblement sans sens) et sa signature valide, sans interaction avec Alice.

Exercice 4 *Aspects calculatoires*

Un aspect important à étudier dans le cas des signatures numériques est la quantité de calcul nécessaire pour (i) signer et (ii) vérifier une signature. On étudie ici la complexité calculatoire du protocole de la signature RSA.

1. Combien de multiplications avons nous besoin en moyenne afin de (i) signer un message avec un exposant aléatoire et (ii) vérifier la signature avec l'exposant $e = 2^{16}+1$. On suppose que le module n est de ℓ bits et que l'algorithme *square and multiply* est utilisé pour l'exponentiation modulaire. Dériver des expressions générales en fonction de ℓ.
2. Quelle action est plus longue, la signature ou la vérification ?
3. On dérive maintenant des estimations pour la vitesse des implémentations logicielles. On adopte le modèle suivant : L'ordinateur opère sur des données de 32 bits. Par conséquent, chaque variable, en particulier le module n et x (base de l'exponentiation) sont représentés comme des chaînes de $m = \lceil \ell/32 \rceil$ éléments. On suppose qu'une multiplication ou un élévation au carré de deux de ces variables modulo n nécessitent m^2 unités de temps (une unité de temps est un cycle d'horloge multipliée par une constante plus grande de 1 qui dépend de l'implémentation). Noter qu'on ne multiplie jamais avec les exposants d et e. Ceci signifie, que la longueur en bits de l'exposant n'influence pas

le temps d'une opération individuelle (multiplication ou élévation au carré). Combien de temps a-t-on besoin pour effectuer ou vérifier une signature si l'unité de temps d'un ordinateur est 100 nsec et n est de 512 bits ? Combien de temps ça prend si n est de 1024 bits ?

Exercice 5 *Confidentialité et authenticité*
Supposons qu'on souhaite protéger des regards indiscrets le contenu du message signé. Expliquer comment atteindre la confidentialité du message en prouvant en même temps son authenticité. Décrire en détail les calculs à effectuer en cas d'utilisation du système RSA.

Exercice 6 *Attaque de l'homme du milieu sur le schéma de signature*
Dans un schéma de signature, Bob signe un message m et l'envoie avec sa signature s ainsi que sa clé publique à Alice. Oscar peut mettre en place une attaque de type "homme du milieu" en replaçant la clé publique de Bob par sa propre clé publique. Son but est de replacer le message de Bob par un message de son choix, tout en envoyant à Alice une signature qu'elle vérifierait comme valide. Montrer toutes les étapes de l'attaque.