

ENSI BOURGES : MASTER « SÉCURITÉ INFORMATIQUE »

Systemes cryptographiques : signature électronique

Emmanuel Bresson – ÉNS-DGA

1. Signature RSA. (★)

1. Calculer le module N et l'entier $\varphi(N)$ associés aux nombres premiers $p = 17$ et $q = 23$.
 2. Quels sont les exposants secrets de signature associés aux exposants publics $e = 11$ et $e = 13$?
 3. Quelle est la signature de $m = 100$?
 4. Vérifier que la vérification fonctionne.
-

2. Signature et chiffrement. (★★)

Si l'on souhaite obtenir une double fonctionnalité de confidentialité et d'authenticité / intégrité, il peut être utile de regrouper signature et chiffrement. Alice et Bob possèdent chacun un couple de clés privées/publiques, et ont à leur disposition deux schémas, un cryptosystème (E, D) et un schéma de signature (S, V) .

On suppose qu'Alice veut envoyer à Bob un message m à la fois signé et chiffré. Alice chiffre m avec la clé publique de Bob : $c := E_{Bob}(m)$; puis elle signe le chiffré : $\sigma := S_{Alice}(c)$. Finalement elle envoie le couple (c, σ) à Bob.

1. Comment Bob utilise-t-il ce schéma ?
 2. Quel est le danger potentiel de ce genre de méthode ?
 3. Proposer une autre mise en œuvre pour obtenir les mêmes fonctionnalités.
-

3. Signature El Gamal. (★)

On considère la méthode de signature d'El Gamal, avec $p = 467, g = 2, x = 65$

1. Justifier la validité du choix de p et g .
2. Calculer la clé publique $y = g^x \bmod p$.
3. Calculer la signature du message $m = 100$ en utilisant les valeurs aléatoires $k = 64$ et $k = 213$.

4. Vérifier que la vérification fonctionne.

4. Attaques sur la signature d'El Gamal. (★★★)

On présente tout d'abord une attaque utilisant un message connu. On note p, g les paramètres du système et y la clé publique de Bob (L'attaquant Charlie ne connaît pas x tel que $y = g^x$); pour les applications numériques, on prendra $p = 467, g = 2$. On suppose que Charlie dispose d'un message m et de sa signature (a, b) .

1. Vérifier la validité de la signature de $m = 100$ avec $a = 337, b = 9$ (prendre $y = 316$).
 2. Soit $(r, s, t) = (1, 3, 4)$. Vérifier que $\text{pgcd}(ra - tb, p - 1) = 1$ et calculer $u = (ra - tb)^{-1} \bmod (p - 1)$.
 3. Montrer que $\alpha = a^r g^s y^t \bmod p = 365$ et $\beta = \alpha b \bmod (p - 1) = 319$ est la signature d'un message μ que l'on calculera.
 4. Que dire de la valeur aléatoire k sous-jacente à cette contrefaçon ?
-

5. Attaques sur la signature d'El Gamal. (★★★)

Voici maintenant des attaques résultant de la mauvaise utilisation du système d'El Gamal. On note p, g les paramètres du système et y la clé publique de Bob. Pour les applications numériques, on conserve $p = 467, g = 2$.

1. On suppose que Charlie découvre la valeur aléatoire k utilisée dans la signature. Que peut-il faire par la suite ?
 2. Exploiter cette idée avec les valeurs suivantes : $p = 467, g = 2, y = 78$; tester les deux cas : $m = 50, a = 416, b = 156$ et $m = 25, a = 245, b = 292$. **Les valeurs de k manquaient dans la feuille originale. 1^{er} cas : $k = 35$, 2^e cas : $k = 337$.**
 3. On suppose maintenant que Bob utilise plusieurs fois la même valeurs k . On suppose que Charlie dispose des signatures (a, b_1) et (a, b_2) sur les messages m_1 et m_2 respectivement. Ecrire les équations de validité et en déduire une relation entre k, m_1, m_2, b_1, b_2 .
 4. On suppose que $\text{pgcd}(b_1 - b_2, p - 1) = 1$. Calculer $k \bmod (p - 1)$.
 5. Exploiter cette idée sur l'exemple suivant : $y = 465, a = 195, m_1 = 77, b_1 = 341, m_2 = 99, b_2 = 155$.
-

6. Fonctions de hachage. (★★)

On rappelle qu'une fonction de hachage h est définie d'un ensemble M de messages vers un ensemble E d'empreintes. On dit que h est à sens unique s'il est calculatoirement difficile de trouver un message produisant une empreinte donnée. On dit que h est sans collisions (ou résistante aux collisions) s'il est calculatoirement difficile de trouver deux messages différents produisant la même empreinte.

1. On considère le cas où $|M| > 2|E|$. Justifier cette considération d'un point de vue pratique.
 2. On suppose que l'on sait inverser la fonction de hachage (i.e., qu'elle n'est pas à sens unique). Proposer un algorithme qui trouve une collision ou s'arrête en affichant « Échec ».
 3. Évaluer la probabilité de succès d'un tel algorithme.
 4. En déduire que le fait d'être résistante aux collisions entraîne la propriété d'être à sens unique.
-

7. Fonction de hachage de Chaum-van Heijst-Pfitzmann. (★★★)

Soit p un nombre premier tel que $q = (p-1)/2$ soit également premier. On désigne par g et h deux éléments d'ordre q dans \mathbb{Z}_p^* et on considère la fonction de hachage H suivante : pour tout $(m_1, m_2) \in \mathbb{Z}_{q-1}^* \times \mathbb{Z}_{q-1}^*$, on pose $H(m_1, m_2) := g^{m_1} h^{m_2} \pmod p$.

1. Quel est l'ensemble des empreintes ?
 2. On suppose connue une collision $H(m_1, m_2) = H(m_3, m_4)$. Ecrire l'équation satisfait par m_1, m_2, m_3, m_4 . Quelles sont les valeurs possibles de $d = \text{pgcd}(m_2 - m_4, p - 1)$?
 3. En examinant chacune des valeurs possibles pour d , calculer le logarithme discret de h en base g . Que vaut $\log_h g$?
 4. Exploiter cette idée avec les valeurs suivantes : $p = 383, g = 2, h = 3, m_1 = 400, m_2 = 100, m_3 = 10, m_4 = 17$.
 5. En déduire qu'une collision sur cette fonction de hachage est au moins aussi difficile que le problème du logarithme discret.
-