CRYPTA - TD 3
2020-2021

Énoncé

Exercice 1 : Sécurité du protocole de signature de Boyd

Nous considérons un protocole de signature numérique où la clé publique est un couple d'entiers (N, g) et la clé secrète est un entier r vérifiant :

1. N est le produit de deux nombres premiers distincts p et q (*i.e.* N est un module RSA) ;
2. r est un diviseur premier de $p-1$;
3. g est un élément d'ordre r dans $(\mathbb{Z}/N\mathbb{Z})^*$.

Nous notons k la taille en bits des nombres premiers p et q et ℓ la taille en bits de l'entier r. La signature σ d'un entier m de taille ℓ est la racine m-ième de g dans $(\mathbb{Z}/N\mathbb{Z})^*$ (*i.e.* $\sigma^m \equiv g \bmod N$).

1.a] Montrer que si r ne divise pas $q-1$, alors la connaissance de (N, g) permet de factoriser l'entier N.

Nous supposerons dans la suite de l'exercice jusqu'à la question 4(a) que :

4. r divise $q-1$;

1.b] Proposer un algorithme probabiliste qui, prenant en entrée deux entiers k et ℓ, retourne un triplet (N, g, r) vérifiant les propriétés (i)–(iv) et comparer la complexité de l'algorithme de signature avec celle de la signature RSA classique.

1.c] Bris total.

(i) Donner un algorithme de complexité $O(2^{\ell/2})$ opérations dans le groupe $(\mathbb{Z}/N\mathbb{Z})^*$ permettant de retrouver r à partir de la clé publique (N, g).

(ii) Montrer que si r est connu alors il est possible de factoriser N en $O(N^{1/4}/r)$ opérations dans le groupe $(\mathbb{Z}/N\mathbb{Z})^*$.
Indication : en notant $p = xr + 1$ et $q = yr + 1$ et $(N-1)/r = ur + v$ avec $0 \leq v < r$, on pourra utiliser un algorithme de logarithme discret pour retrouver la « retenue » c définie par $x + y = v + cr$ et montrer que sa connaissance est suffisante pour retrouver p et q.

1.d] Contrefaçon universelle.

(i) Montrer qu'il existe un algorithme polynomial qui prenant en entrée N et un entier m premier avec r, retourne un entier γ tel que $m\gamma \equiv 1 \mod r$. En déduire une contrefaçon universelle sous une attaque à clé seule contre le schéma de signature de Boyd.

Nous supposerons désormais que :

2' r est un diviseur *composé* de $p-1$ de taille ℓ ;

et qu'il est difficile de calculer un multiple de r (et nous ne supposons plus que la condition *(4)* est vérifiée).

(ii) Montrer que la connaissance de la signature de deux messages m_1 et m_2 premiers entre eux permet de calculer la signature du message produit $m = m_1 m_2$ (et réciproquement). En déduire une contrefaçon universelle sous une attaque à deux messages choisis.

Nous supposerons désormais que :

5. La signature σ d'un message $m \in \{0,1\}^*$ est la racine $H(m)$-ième de g (*i.e.* $\sigma^{H(m)} = g$) où $H : \{0,1\}^* \to \{0,1\}^\ell$ est une fonction de hachage cryptographique (dans la suite nous supposerons que H se comporte comme une fonction aléatoire).

1.e] Contrefaçon existentielle. Montrer que la connaissance d'un ensemble de messages $\{m, m_1, \ldots, m_t\}$ vérifiant :

— $H(m) = a_1 \cdot a_2 \cdots a_t$ où les a_i sont des entiers deux à deux premiers entre eux ;

— a_i divise $H(m_i)$ pour $i \in \{1, \ldots, n\}$

est suffisante pour réaliser une contrefaçon existentielle sous une attaque à messages choisis.
En déduire que le schéma n'est pas résistant aux contrefaçons existentielles lorsque ℓ est significativement plus petit que k.

Exercice 2 :

Protocole de signature d'ElGamal naïf

Génération des clés : Le signataire choisit un nombre premier p et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Il tire uniformément aléatoirement $x \in (\mathbb{Z}/(p-1)\mathbb{Z})$ et calcule $y = g^x \bmod p$. La clé publique est (p, g, y) et la clé secrète associée est x.

Signature : Pour signer un message $m \in (\mathbb{Z}/(p-1)\mathbb{Z})$, le signataire tire uniformément aléatoirement $k \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ et calcule $r = g^k \bmod p$. Il calcule $s = (m - xr)/k \bmod p - 1$ et la signature est le couple (r, s).

Vérification : Un couple (r, s) est une signature valide de $m \in (\mathbb{Z}/(p-1)\mathbb{Z})$ si et seulement si $(r, s) \in (\mathbb{Z}/(p-1)\mathbb{Z})^2$ et

$$g^m = y^r r^s \bmod p.$$

Supposons que le générateur g de $(\mathbb{Z}/p\mathbb{Z})^*$ est égal à 2 et que $p \equiv 1 \mod 4$.

2.a] Montrer que le logarithme discret de $q = (p-1)/2$ en base $g = 2$ est égal à $(p-3)/2$.

2.b] En déduire que, avec ce choix de générateur, le protocole de signature d'ElGamal naïf n'est pas résistant aux contrefaçons universelles sous une attaque sans message (ou à clé seule).