1 Signature El-Gamal

Soit p un nombre premier et h une fonction de hachage. Soit g un élément générateur de $G = (\mathbb{Z}/p\mathbb{Z})^*$. On considère le protocole de signature suivant :

- KeyGen $\rightarrow (pk = (p, b, g), sk = a \xleftarrow{\$} [0, p-2])$ avec $b = g^a$
- Sign$(m, sk) = \sigma = (m, r, s)$ avec $r = g^k \mod p$ où k est un élément de $[2, p-2]$ différent à chaque utilisation et $s = k^{-1}(h(m) - ra) \mod p-1$. Si $s = 0$ recommencer avec un autre k.
- Verif(m, σ, pk) retourne 1 si et seulement si $0 \leq r \leq p-1$ et $g^{h(m)} = b^r r^s \mod p$

1. Quels sont les propriétés que doit vérifier une signature ?
2. Montrer que la fonction de vérification est correcte.
3. A priori, quel élément un attaquant doit calculer pour signer. Imaginer une attaque pour trouver cet élément.
4. Quel est la taille de p à choisir pour que le système de signature ne soit pas vulnérable à cette attaque.
5. Peut-on, en terme de temps de calcul, utiliser ce système en pratique ?

Importance de k

6. Montrer que si un même élément k est utilisé deux fois il est possible de retrouver la clef secrète a.

Importance de la condition $0 \leq r \leq p-1$

Supposons que le protocole ne vérifie pas cette condition. Soit (m, r, s) une signature valide. On veut se servir de cette signature pour signer un message m'. Pour cela on calcule

$$u = h(m')h(m)^{-1} \mod p-1 \text{ et } s' = su \mod p-1$$

On trouve ensuite r' tel que $r' = ru \mod p-1$ et $r' = r \mod p$.

7. A quelle condition ces calculs sont-ils possible ?
8. Vérifier que (m', r', s') est une signature valide.
9. En supposant que la fonction h est sans collision, comparer la sécurité du protocole à celle du logarithme discret.

Importance de la fonction de hachage

Supposons que l'on utilise pas de fonction de hachage ($h(m) = m$ dans le protocole), on va réaliser une autre falsification : Soient i, j des entiers dans $[0, p-2]$, on cherche r sous la forme $g^i b^j \mod p$

10. Montrer que la relation $g^{h(m)} = b^r r^s$ est équivalente à $g^{y-is} = b^{r+js} \mod p$.
C'est en particulier le cas si $y - is$ et $r + js$ sont congrus à $0 \mod p-1$

11. A quelle condition ce système admet-il une solution ? Déterminer (r, s, y) en fonction de i et j.

12. Pourquoi cette attaque est-elle moins puissante que la précédente ?

2 Fonction de Chaum, Van Heijst et Pfitzmann

2.1 Préliminaires mathématiques.

Soit p un nombre premier. Un élément x de $\mathbb{Z}/p\mathbb{Z}^*$ est un générateur si tous les éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont des puissances de x (modulo p). Dans ce cas, si $x^i = x^j \mod p$, alors $i = j \mod p-1$.
Lemme de Gauss : Si a divise bc et que a est premier avec b, alors a divise c.

2.2 Description de la fonction

Considérons un (grand) nombre premier q, choisi de telle sorte que $p = 2q+1$ est premier lui aussi. On prend aussi deux générateurs de α et β du groupe $\mathbb{Z}/p\mathbb{Z}^*$. La fonction de hachage prend en entrée deux nombres x et y dans l'intervalle $\{0, ..., q-1\}$ et calcule : $H(x, y) = \alpha^x \beta^y \mod p$.

1. Supposons que q s'écrive sur n bits. Quelle sont les tailles (en bits) de l'entrée de H et de sa sortie ?

2. Quelle est (en fonction de n) la complexité asymptotique du calcul de H ?

3. Comment faire pour hacher des messages plus long sans augmenter la taille de q ?

4. Comme on a supposé que α était un élément primitif, alors on sait qu'il existe λ tel que $\beta = \alpha^\lambda \mod p$. Si α et β nous sont imposés, déterminer λ revient à résoudre un problème algorithme usuel en cryptologie à clef publique. Lequel ?

5. Ce problème est-il facile à résoudre, pour de grandes valeurs de p ?

6. Montrez que si on connaît la valeur de λ, alors on peut facilement forger des collisions pour la fonction.

2.3 Résistance aux collisions

On a donc vu que si on connaît le logarithme discret de β en base α, alors on peut fabriquer des collisions. L'objectif des questions suivantes est de montrer la réciproque : si on arrive à trouver une seule collision, on est capable de calculer le logarithme discret de β.

1. Expliquez pourquoi cela garantit la résistance aux collisions de la fonction de hachage.

2. Supposons qu'on ait une collision sur H, c'est-à-dire deux paires $(x, y) \neq (u, v)$ telles que $H(x, y) = H(u, v)$. Justifiez qu'on a alors : $\alpha^{x-u} = \beta^{v-y} \mod p$.

3. Justifiez qu'on a :
$$\lambda(v - y) - (x - u) = 0 \mod p - 1$$

4. . On pose $d = PGCD(z - y, p - 1)$. Rappelons que c'est le plus grand entier (positif) qui divise à la fois $z-y$ et $p-1$. En utilisant le fait que z et y sont strictement inférieurs à q, montrez que d est strictement inférieur à q (on peut supposer que $z - y > 0$).

5. En utilisant le fait que d divise $p - 1$ et le lemme de Gauss, justifier que d vaut soit 1, soit 2.

6. Dans le cas où $d = 1$, justifiez qu'il y a une seule valeur de λ possible, et trouvez comment on peut la calculer facilement.
   Le cas où $d = 2$ est plus pénible, car l'équation en λ a deux solutions, et il est plus difficile de les calculer. C'est néanmoins possible, et on peut tester laquelle des deux solutions réalise effectivement $\beta = \alpha^\lambda$. On peut donc calculer le logarithme de β dans tous les cas.

3 Examen 2022

3.1 Questions courtes

1. Expliquer le fonctionnement de l'échange de clef Diffie-Hellman. Quelle est l'hypothèse de complexité associée ?

2. Quelle attaque est possible contre un chiffrage par substitution ? (Détailler l'attaque ne pas donner seulement le nom).

3. Dans le cadre d'un tirage aléatoire d'entiers entre 1 et N, quel est l'ordre de grandeur du nombre de tirage qu'il faut pour tirer deux fois le même entier avec probabilité $\frac{1}{2}$? (donner juste la valeur, pas les calculs).

4. Soit $H_1 : \{0, 1\}^n \to \{0, 1\}^m$ et $H_2 : \{0, 1\}^m \to \{0, 1\}^l$ deux fonctions de hachage avec $n > m > l$. Est-ce que H définie par $H(x) = H_2(H_1(x))$ est une fonction de hachage ?

5. Soit p un nombre premier de 256 bits. On considère la fonction $h : \mathbb{N} \to \mathbb{Z}/p\mathbb{Z}$ qui a un entier n associe $7^n \mod p$. Quelles sont les trois propriétés que doit vérifier une fonction de hachage ? Quelles sont celles vérifiées par h ?

3.2 RSA est-il vraiment NP-difficile ?

1. Écrire un algorithme prenant en entrée un entier n et renvoyant un diviseur premier de n en testant successivement tous les diviseurs possibles.
2. Quel est la complexité de l'algorithme ?
3. Peut-on utiliser cet algorithme pour résoudre le problème RSA ? Que concluez-vous ?

3.3 Algorithme pas de bébé - pas de géant

Soient G un groupe cyclique d'ordre n et g un générateur de G. On pose $b = \lceil \sqrt{n} \rceil$.

1. Soit h un élément de G. Montrer qu'il existe $(q; r) \in \{0, ..., b-1\}^2$ vérifiant $g^{bq}h = g^r$.
2. En déduire un algorithme donnant le logarithme discret d'un élément de G en base g de complexité $O(\sqrt{n})$.
3. Quel est l'espace en mémoire nécessaire à l'exécution de cet algorithme ?
4. Supposons $G = (\mathbb{Z}/31\mathbb{Z})^*$. Calculer le logarithme discret de 15 en base 3 par cette méthode.
5. Comparer (en terme de performance) cet algorithme aux autres algorithmes que vous connaissez pour ce problème.

3.4 LSFR

1. Calculer les deux premiers octets de la suite générée par le LFSR de degré $m = 8$, ayant comme coefficients (1, 1, 0, 1, 1, 0, 0, 0) et initialisé par 11111111.

   On mène une attaque à clair connu contre un chiffrement à flot dont la suite a été produite par un seul LFSR. On suppose connaître le message clair 1001 0010 0110 1101 1001 0010 0110 ainsi que le message chiffré 1011 1100 0011 0001 0010 1011 0001.
2. Quel est le degré (taille du registre) du LFSR ?
3. Quel est le vecteur d'initialisation ?
4. Déterminer les coefficients de rétroaction du LFSR.
5. Bonus : que signifie LSFR ?

3.5 Protocole d'encryption d'El-Gamal

Alice choisit un groupe G cyclique d'ordre q dans lequel l'hypothèse décisionnelle de Diffie-Hellman est vérifiée et g un générateur de G. Elle tire un élément x aléatoirement dans $\{0, 1, .., q-1\}$ et calcule $h = g^x$. Elle publie la clef publique $pk = (G, g, h)$ et conserve la clef secrète $sk = x$.
Pour envoyer un message m, Bob tire un élément r aléatoirement dans $\{0, 1, .., q-1\}$. Il calcule $c_1 = g^r$ et $c_2 = m.h^r$ et envoie comme chiffré $c = (c_1, c_2)$.

1. Comment Alice retrouve t-elle le message m à partir du chiffré ?
2. Rappeler l'hypothèse décisionnelle de Diffie-Hellman.
3. Si l'hypothèse n'est pas vérifiée, comment un attaquant peut-il retrouver le message ?

   On suppose que l'on est en possession d'un algorithme $\mathcal{A}$ qui déchiffre une instance d'El-Gamal avec une probabilité p. On veut se servir de cette algorithme pour résoudre le logarithme discret dans G.
4. A partir de l'algorithme $\mathcal{A}$ construire un algorithme qui, sur une instance (g^a, g^b, g^c) renvoie si $ab = c$ avec une probabilité p'.
5. En supposant que $c = ab$ avec une probabilité $\frac{1}{2}$, quel est la probabilité de succès de cet algorithme ?

3.6 Puzzles de Merkle

On considère le protocole à clef publique suivant. Alice génère un nombre n d'instance dont la solution contient une paire de nombre (id_n, key_n). Elle envoie les instances à Bob qui en résout une aléatoirement et envoie id_n à Alice. La clef partagée est alors key_n.

1. On suppose qu'il faut un temps m pour résoudre une instance. Combien de temps faut-il à un attaquant pour trouver la clef partagée ?
2. Ce système est-il conforme aux standards de sécurité en cryptographie ?
3. On suppose que chaque instance est un problème RSA (un entier à factoriser) et que (id_n, key_n) sont les deux facteurs. Expliquer comment un attaquant peut tirer un avantage de cette construction.
4. (+ ouvert) Imaginer une construction proche de RSA qui évite cette attaque.

4 DM3

Devoir à rendre avant le 25 avril, soit au début du cours, soit par mail à quentin.deschamps@univ-lyon1.fr.

4.1 Réduction de Pollig-Hellman

Soit G un groupe d'ordre pq avec p et q premiers entre eux. Soit g un générateur de G et $h \in G$. En utilisant l'identité de Bezout montrer comment calculer le logarithme discret de h en complexité $O(\sqrt{\max\{p,q\}})$.

4.2 Fonction de hachage

1. Rappelez les trois propriétés que doit vérifier une fonction de hachage.
2. Soit f la fonction $x \to x^2 \mod N$. Quelle propriétés vérifie f ?
   Soit $g : \{0,1\}^* \to \{0,1\}^n$ que l'on suppose résistante à la collision. Soit $h : \{0,1\}^* \to \{0,1\}^{n+1}$ définie par

   - $h(x) = 1|x$ si x est de longueur n.
   - $h(x) = 0|g(x)$ sinon

   Quelle propriétés vérifie h ?
3. Quels autres implications ou non-implications pouvez-vous trouver.
4. Soit $h : \{0,1\}^* \to \{0,1\}^n$. On suppose que pour un élément m aléatoire, la probabilité d'avoir une valeur donnée $h(m)$ est de $\frac{1}{2^n}$ (l'espace d'arrivée est équiprobable). Donner une attaque pour chaque propriété de h ainsi que sa complexité.