L3 informatique. Sécurité. Partie J.-F. COUCHOT.

Seule une fiche manuscrite recto-verso de format A4 est autorisée. Toutes les réponses doivent être justifiées. Sans justification, une réponse est considérée comme fausse.

1 Fonction de hachage (3 pts)

Ci dessous une traduction en français du résumé de l'article *Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017, August). The first collision for full SHA-1. In Annual International Cryptology Conference (pp. 570-596). Springer, Cham.*

> SHA-1 est une fonction de hachage cryptographique du NIST(1995) largement utilisée qui a été officiellement dépréciée par le NIST en 2011 en raison de lacunes fondamentales en matière de sécurité démontrées dans diverses analyses et attaques théoriques.
> Malgré sa dépréciation, SHA-1 reste largement utilisé en 2017 pour les signatures de documents et de certificats TLS, ainsi que dans de nombreux logiciels tels que le système de gestion des versions GIT [...]. L'une des principales raisons de la réticence de nombreux acteurs de l'industrie à remplacer SHA-1 par une alternative plus sûre est le fait que la découverte d'une collision réelle a paru irréalisable au cours des onze dernières années en raison de la grande complexité et du coût de calcul de l'attaque.
> Dans cet article, nous démontrons que les attaques par collision SHA-1 sont enfin devenues réalité en fournissant le premier exemple connu de collision. De plus, **le préfixe des messages de collision a été soigneusement choisi pour permettre à un attaquant de construire deux documents PDF avec des contenus visuels distincts arbitrairement choisis, mais avec la même empreinte SHA-1**. [...]

1. (1 pt) Parmi les propriétés que doit posséder une fonction de hachage cryptographique, laquelle est mise à mal par les travaux présentés ici ?

2. (2 pts) Le texte en gras montre que les auteurs ont aussi réussi à réfuter une autre propriété. Laquelle et pourquoi ? Quelles en seraient les conséquences pour la signature de documents PDF, par exemple.

2 Chiffrement affine (6 pts)

Afin de chiffrer un message, on utilise un chiffre affine appelé par la suite *CA*. Chaque lettre de l'alphabet est associée à un nombre entier comme indiqué dans le tableau ci dessous.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

On considère une lettre l à chiffrer et soit x son nombre associé. On calcule

$$y \equiv (7x + 5) \bmod 26$$

et on regarde à quelle lettre c cela correspond. C'est le chiffre associé à l. On souhaite par exemple chiffrer la lettre 'M', dont le nombre associé est $x = 12$. On évalue

$$7 \times 12 + 5 \equiv 89 \bmod 26 \equiv 11 \bmod 26.$$

Comme 11 correspond à la lettre 'L', la lettre 'M' serait ainsi chiffrée en 'L' selon *CA*.

1. (1 pt) Chiffrer la lettre 'L'.

2. (1,5 pt) Si $y \equiv (7x + 5) \bmod 26$, montrer qu'en calculant $15y + 3 \bmod 26$ on retrouve x.

3. (0,5 pt) Déchiffrer la lettre 'S'.

4. (1 pt) Quelles-sont les clefs de cet algorithme ?

5. (2 pts) Décrire comme vous feriez pour décrypter un message chiffré par CA, c'est-à-dire sans en connaître la/les clef(s). Serait-ce complexe à mettre en place ?

3 Analyse d'un algorithme asymétrique (10 pts)

On considère l'algorithme asymétrique suivant.

Alice veut envoyer un message à Bob.

1. Bob choisit deux nombres premiers p et q tels que $p < q$ et p et $q-1$ sont premiers entre-eux.
2. La clef publique de Bob est (n, p), avec $n = pq$. Elle est envoyée à Alice.
3. Bob calcule $p' \in \mathbb{N}$ tel que $pp' \equiv 1 \bmod q - 1$. Sa clef privée est la paire (p', q).
4. Alice chiffre un nombre $m \in \{1, ..., p-1\}$ en calculant $a \equiv m^p \bmod n$.
5. Bob déchiffre a en calculant $m' \equiv a^{p'} \bmod q$. Normalement m est égal à m'.

1. (1 pt) : Montrez que $p = 5$ et $q = 7$ sont de bons candidats pour cet algorithme.

2. (2 pts) : Générez la clef publique et montrer que clef privée de cet algorithme est (5,7).

3. (2 pts) Montrez qu'on peut chiffrer $m = 2$. Chiffrez m en a puis déchiffrez a.

4. (2 pts) Montrez qu'on peut retrouver la clef privée à partir de la clef publique. Que dire alors de cet algorithme ?

5. (3 pts) **Difficile :** Montrez que l'algorithme est correct, c'est-à-dire que $m' = m$ pour n'importe quel $m \in \{1, ..., p-1\}$.

4 Codes correcteurs d'erreurs (5 pts)

Donner le code d'une fonction java ou python qui prend en paramètre k et qui retourne H_k une matrice de contrôle pour un code de Hamming systématique.