Université Côte d'Azur — L3 Info, L3 MI, L3 ST
Cryptographie et calcul symbolique — 2023-24

TD n° 6

Signatures digitales
Fonctions de hachage cryptographiques

Exercice 1) La clef privée de Bob dans un système de signature RSA est : $(n, d) = (33, 7)$.

1. Pour *authentifier* ses messages, il doit publier sa clef publique qui est ici une *clef de vérification*. Déterminez cette clef publique (n, e).
2. Bob veut envoyer un message signé $M = 123456789$ dont l'empreinte est $h(M) = 30$. Pourriez-vous aider Bob à calculer la signature S pour cette empreinte de M ?
3. Alice reçoit le couple message/signature (M, S). La fonction de hachage utilisée étant connue, elle calcule l'empreinte $h(M)$ à partir de M. Aidez-la ensuite à vérifier l'authenticité du message signé.

Exercice 2) Pour signer avec El Gamal, Alice choisit un entier premier $p = 11$ et un générateur $\alpha = 2$ du groupe multiplicatif $\mathbb{Z}_p^*$. Elle se choisit pour clef privée $k = 8$, on a bien $1 < k < p$.

1. Quelle est la clef publique (p, α, β) qu'Alice va diffuser afin que l'on puisse vérifier sa signature ?
2. Alice souhaite signer son message $M = 5$ à l'aide du nombre aléatoire $r = 9$. Elle a pris soin que r et $p - 1$ soient premiers entre eux. Aidez Alice à calculer la signature qui va servir à authentifier son message.
3. Un tiers vérifie la validité de la signature d'Alice à partir du couple message/signature : $(M, (\gamma, \delta))$. Comment s'y prend-il ?

Exercice 3) Alice veut pouvoir signer ses messages avec le standard DSA. Elle choisit les paramètres $p = 47$ et $q = 23$, deux nombres premiers tels que $q \mid (p - 1)$. Elle choisit aussi un générateur $\alpha = 2$ d'un sous-groupe d'ordre q du groupe $\mathbb{Z}_p^*$. Enfin, elle prend pour clef privée $k = 7$. Elle diffuse alors sa clef publique $(p, q, \alpha, \beta) = (47, 23, 2, 34)$.

1. Voici les puissances successives $2^i \mod 47$ pour i variant de 0 à 22 :

   $$1, 2, 4, 8, 16, 32, 17, 34, 21, 42, 37, 27, 7, 14, 28, 9, 18, 36, 25, 3, 6, 12, 24$$

   Vérifiez que α est bien un générateur d'un sous-groupe d'ordre q de $\mathbb{Z}_p^*$.
2. Aidez Alice à signer son message $M = 33$ avec l'entier aléatoire éphémère $r = 19$ choisi tel que $0 < r < q$.
3. A présent, aidez Bob à vérifier la signature d'Alice à partir du couple $(M, (\gamma, \delta))$ reçu.

Exercice 4) Paradoxe des anniversaires Poursuivons l'exemple du cours avec $n = 365$. Calculez la probabilité qu'il y ait 2 personnes parmi k ayant la même date d'anniversaire (jour et mois) dans les 3 cas suivants :

1. $k = 9$
2. $k = 23$
3. $k = 60$

Exercice 5) Soit f une fonction de $\{0,1\}^m$ dans $\{0,1\}^m$, on propose la fonction de compression h suivante à itérer en vue de bâtir une fonction de hachage :

$$h : \{0,1\}^{2m} \to \{0,1\}^m$$

$$x = x_l\, x_r \mapsto f(x_l \oplus x_r)$$

1. Peut-on savoir si la fonction h est résistante à la préimage ?
2. Montrez que la fonction h n'est pas résistante à la 2$^{\text{nde}}$ préimage.
3. En déduire qu'elle n'est pas résistante aux collisions.

Exercice 6) Résistance aux collisions Montrez les relations existantes entre les 3 propriétés suivantes :

1. *Résistance à la préimage* : pour une empreinte donnée, il est difficile de trouver un message qui aurait cette empreinte ;
2. *Résistance à la seconde préimage* : pour un message donné, il est difficile de trouver un autre message distinct qui aurait la même empreinte ;
3. *Résistance aux collisions* : il est difficile de trouver deux messages distincts ayant la même empreinte.

Exercice 7) Fonction de hachage On considère la fonction de compression g prenant en entrée une lettre minuscule et une valeur initiale (IV) sous la forme d'un entier modulo 100. La sortie de cette fonction est obtenue par la suite d'opérations suivante :

1. on code numériquement la lettre ;
2. on ajoute le code numérique de la lettre à la valeur de chaînage (ou à IV pour initialiser) et on réduit modulo 100 ;
3. on multiplie le résultat précédent par 7 modulo 100 ;
4. on échange les chiffres du résultat (12 devient 21) ;
5. on ajoute au résultat précédent la valeur de chaînage modulo 100 pour obtenir la valeur de chaînage suivante.

Chaque lettre est codée numériquement par :

	0	1	2	3	4
+0	a	b	c	d	e
+5	f	g	h	i	j
+10	k	l	m	n	o
+15	p	q	r	s	t
+20	u	v	w	x	y
+25	z				

1. Calculez la valeur de $g(\texttt{'h'}, 17)$;
2. Expliquez comment on combine l'usage de la fonction de compression g pour obtenir la fonction de hachage h selon la construction de Merkle-Damgård. On ajoutera le traitement de longueur de la chaîne fournie en entrée à la fin comme si c'était le code d'une lettre supplémentaire, comme c'est l'habitude dans une telle construction ;
3. En utilisant le paradoxe des anniversaires, donnez le nombre de messages à considérer pour avoir plus d'une chance sur deux de trouver une collision ;
4. Alice et Bob partagent le secret commun $s = 20$. Alice reçoit un HMAC sous la forme du couple message/empreinte $(\texttt{'ok'}, 7)$ de Bob. Que peut-elle en déduire ? Vous pouvez utiliser le tableau suivant pour vous aider dans les calculs :

	'o'	'k'	
IV	20		
1. codage	14	10	2
2. addition2			
3. $\times 7$			
4. échange			
5. addition5			

5. Par un argument de dénombrement sur les mots d'exactement 2 lettres, estimez le nombre d'antécédents pour une empreinte fixée.