Sécurité des SI

TD2 (cryptographie)

Questions de cours :
Donnez une définition de la confidentialité, l'intégrité, l'authentification et la non répudiation
Quels sont les principaux ingrédients d'un système de chiffrement symétrique ?
Quels sont les objets secrets dans un système de chiffrement symétrique (asymétrique)?

Problèmes :
1) Iwan vous propose le protocole suivant pour confirmer que vous êtes tous les deux en possession de la même clé secrète.
Vous créez une chaîne C aléatoire de la longueur de la clé k. Vous lui envoyez M=C+k ('+' étant un XOR). Iwan retrouve la valeur C (C=M+k) et vous l'envoie. La clé k n'est jamais passée par le canal.
Etes-vous surpris que ce protocole soit utilisé chez cretin.fr ?

2) Soit n=11 et l'encodage suivant :

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10

On suppose qu'on connaît les texte clair/chiffré comme suit (? représente des caractères manquants)

plaintext: B I ?
ciphertext: J F A
où m*k1 + k0 mod 11 = c

a) Déterminez k0 et k1
b) Retrouvez le texte en clair

3) Pourquoi est-il intéressant de compresser avant de chiffrer?

4) Alice est Bob ont chacun une paire de clés (publique/privée). Ecrivez un protocole qui permette à Alice d'envoyer en confidentialité un message authentifié à Bob.

5) Comparaison entre DS (signature digitale) et MAC : On suppose que Oscar peut observer tous les messages entre Bob et Alice. Oscar ne connaît aucune clé autre que publique (dans le cas de DS). Dire si et comment DS (resp MAC) protège contre chaque attaque. La valeur Auth(x) avec un algo de DS ou MAC :

a) (Message integrity) Alice envoie un message x = « Transfer $1000 to Iwan » en clair et Auth(x) à Bob. Oscar intercepte le message et remplace Iwan par Oscar. Bob va-t-il le détecter ?
b) (Replay) Alice envoie un message x= « Transfer $1000 to Iwan » en clair et Auth(x) à Bob. Oscar observe le message et la signature et les renvoie 100 fois à Bob. Bob va-t-il détecter que les messages ne sont pas d'Alice ?
c) (Sender authentication with cheating third party) Oscar prétend avoir envoyé x avec un valide Auth(x) à Bob mais Alice prétend la même chose. Bob peut-il savoir qui dit la vérité ?
d) (Authentication with Bob cheating) Bob prétend avoir reçu un message x avec un valide Auth(x) de la part de Alice (« Transfer $10000 from Alice to Bob ») mais Alice prétend n'avoir rien envoyé. Alice peut-elle prouver que Bob ment ?

6) Soit H(m) une fonction de hachage « collision-resistant » qui prend en input un message de taille arbitraire et rend en output n bits. Est-il vrai que, pour tous messages distincts x et x', on a H(x) différent de H(x') ? Expliquez votre réponse.

7) Ce problème introduit une fonction de hachage qui, dans l'esprit, est proche de SHA mais opère sur des lettres au lieu de bits. La fonction s'appelle tth (toy tetragraph hash). A partir d'un message constitué d'une séquence de lettres, tth produit un haché de quatre lettres. Premièrement, tth divise le message en blocks de 16 lettres en ignorant les espaces, les ponctuations et les lettres capitales. Si le nombre de lettres du message n'est pas divisible par 16, on rajoute des zéros pour arriver à 16 (bourrage). Au départ, un vecteur T est initialisé à (0,0,0,0) et sert d'input à la fonction appelée fonction de compression pour calculer le premier block. La fonction de compression opère en deux tours. Tour 1 : Prendre le block de texte et le réarranger en un tableau 4x4, puis le transformer en un tableau de nombre (A=0, B=1, ….)

Par exemple pour ABCDEFGHIJKLMNOP, on obtient

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Ensuite, additionner chaque colonne modulo 26, et additionner le résultat dans T modulo 26. Dans notre exemple T= (24,2,6,10).
Tour 2 : en utilisant la matrice du tour 1, décaler la première ligne de 1 vers la gauche, la deuxième de 2, la troisième de 3 et inverser l'ordre de la quatrième. On obtient dans notre exemple :

B	C	D	A
G	H	E	F
L	I	J	K
P	O	N	M

1	2	3	0
6	7	4	5
11	8	9	10
15	14	13	12

Maintenant, additionner chaque colonne modulo 26 et additionner le résultat dans T. La nouvelle valeur est T=(5,7,9,11). Cette valeur sert d'input pour la fonction de compression qui traite du deuxième block. Lorsque tous les blocks ont été traités, T est converti en lettres. Dans l'exemple, on obtient : FHJL.
a) Calculez la fonction de hachage pour le texte « is it a good hash function ? »
b) Analysez les points faibles de tth et essayez de trouver deux textes de 16 lettres qui donnent le même haché.

8) Un utilisateur peut n'avoir qu'une seule paire de clef (publique/privée) pour chiffrer et signer. Il peut aussi avoir une paire pour chiffrer et une paire pour signer. Quels sont les avantages de cette dernière alternative ?