Travaux dirigés –TD
Cryptographie et services de sécurité

<u>Exercice 1</u> : Commerce électronique

Le protocole 3-D Secure de VISA permet aux internautes de payer d'une manière sécurisée sur Internet. L'entité connue sous le nom Access Control Server (ACS) dans ce protocole a pour but principal d'authentifier l'acheteur dans la transaction. Comme résultat du processus d'authentification, l'ACS envoie un message signé (M1) au commerçant qui le vérifie. Après des échanges interbancaires, le commerçant envoie à l'acheteur un message chiffré (M2) montrant le résultat de l'achat. Dans le cadre du processus de vérification de VISA, vérifier les transactions suivantes :

a) Le message M1 comporte les éléments de données suivants :

- Date: 20012010
- PAN: 1701001012211001

On suppose que l'algorithme de signature est RSA et la clé publique de l'ACS : Kp(ACS) = (e= 13 , n= 91). L'algorithme de hachage appliqué sur les données numériques fonctionne de la manière suivante : on divise les éléments de données en groupes de deux chiffres. Ensuite, on calcule la somme des groupes. Exemple: si le message est 4432, la somme résultante sera 76 car 44+32=76). La valeur de hachage du message complet M1 est calculée en additionnant les valeurs de hachage de chaque élément de données et en appliquant l'opération de modulo 91.

Vérifiez si 32 est la signature correcte du message M1.

b) Message M2 comprend les éléments suivants :
- Date: 17
- Prix: 18

Chiffrer le message M2. Prendre en compte les informations suivantes :
- Kp (la clé publique de commerçant) = (e = 32, n = 64)
- Kv (la clé de publique de l'acheteur) = (e = 13, n = 143)

c) Supposons que le message M2 contient un seul élément indiquant l'heure. Soit 92 le cryptogramme de M2 obtenu en utilisant la cryptographie asymétrique.

- De quel paramètre avez-vous besoin pour déchiffrer le message ? Comment-pouvez-vous l'obtenir ?
- Décrypter le texte.
- Expliquer brièvement, si vous considérez que le résultat du déchiffrement est raisonnable ou non.

Corrigé Exercice1

On calcule la somme 2 à 2 de la date et le PAN

H(M1)= 17+1+0+10+12+21+10+1+20+1+20+10 mod 91 = 123 mod 91 = 32
32 = 32^e mod n = 32^13 mod 91 = 32. La signature est valide

Déchiffrement de 92: il faut trouver d= ?
n=143, donc 1<p<11 qui est la racine de 143=> p=11 et q=13 alors phi=120
13d=1 mod120
13u+120v=1
120=13*9 +3
13=4*3 +1
4=1*4+0

Il faut remonter: 1= 13-4*3=1-4*(120-13*9)=1-4*120+36*13=37*13-4*120 => d=37
Decrypted = 92^37 mod 143 = 27.
27 n'est pas une heure de transaction (0<h<23)

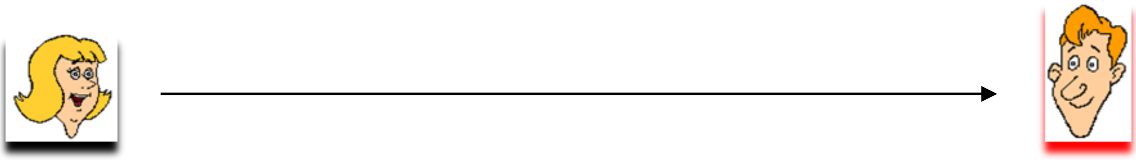
Exercice 2 : Services de sécurité

On suppose qu'Alice veut envoyer un message *M* à Bob. Pour ce faire, Alice et Bob peuvent potentiellement utiliser un certain nombre de méthodes cryptographiques, qui sont décrites dans le tableau suivant :

M	Message en clair (*plaintext*)
K_A K^{-1}_A	Clé publique d'Alice Clé privée d'Alice
K_B K^{-1}_B	Clé publique de Bob Clé privée de Bob
E_k	Chiffrement asymétrique RSA en utilisant la clé publique K
s_k	Clé de chiffrement symétrique (**s_k n'est pas partagée au préalable**)
AES_{sk}	Chiffrement à clé symétrique en utilisant AES-256 avec la clé s_k

$HMAC_{sk}$	*Keyed-Hash Message Authentication Code*
SHA	Fonction de hachage SHA-256
Sign	Signature numérique

On suppose que les clés publiques ont été distribuées en toute sécurité. Alice et Bob désirent avoir, dans leur communication, les propriétés suivantes : la confidentialité, l'intégrité, l'authentification et la non-répudiation. Rappelez ce qu'est une signature numérique, puis proposez une manière pour Alice d'envoyer son message afin d'assurer les propriétés de sécurité citées ci-dessus. Prenez en considération la présence d'Eve (attaque de MITM). **Vous justifierez votre solution en explicitant (rapidement) comment chaque propriété de sécurité est assurée**.



Alice Bob

Exemple d'un message échangé :

Si Alice souhaite chiffrer son message avec sa clé publique et l'envoyer avec un hash, elle transmettra par exemple : $E_{KA}(M)$, SHA(M).

Corrigé Exercice 2

a) Alice envoie à Bob : E_{KA} (M || Sign K^{-1}_{A} (SHA(M)))

   Le message est confidentiel, mais personne n'est capable de le déchiffrer même le destinataire. Alice est la seule qui est capable de le déchiffrer …..

b) Alice envoie à Bob : E_{KB} (M), Sign K^{-1}_{A} (SHA(M))

   Confidentialité, non-répudiation, intégrité et authentification.

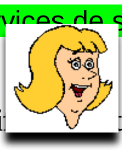
c) Alice génère une clé symétrique s_k et envoie à Bob : $E_{KB}(s_k)$, $E_{K^{-1}_{A}}$ (SHA(s_k)), AES_{sk}(M)

   Confidentialité de la clé + non-répudiation + authenticité, confidentialité du message

d) Alice génère deux clés symétriques s_{k1} et s_{k2} et envoie à Bob :

   $E_{KB}(s_{k1})$, $E_{KB}(s_{k2})$, AES_{sk1} (M), $HMAC_{sk2}$ (SHA(M)), SignK^{-1}_{A} (SHA(sk1)), SignK^{-1}_{A} (SHA(sk2))

   Les 4 services de sécurité

Exercice 3 : Chi  : RSA

a) Déterminer la clé publique et la clé privée pour p = 47 et q = 59. On prendra e = 17, justifiez la possibilité de ce choix.
b) Chiffrer la lettre B en système ASCII (66) avec la clé publique et vérifier que la clé privée permet bien de retrouver le message initial.

Corrigé Exercice 3

La clé publique est n=p*q= 47*59=2773
Pour calculer la clé privée d il faut trouver d telque e*d=1 mod j avec j=(p-1)(q-1)
J= (p-1) (q-1) = 46*58=2668 ; choisissons e=17, 17*d=1 mod 2668
2668 U + 17 V=1
2668=17*156 + 16
17=16*1+1

1= 17-16*1 = 17 – (2668*1-17*156)=17-2668 +17*156 = 17*157 +2668*1
Donc d=157

Si M=66
Pour chiffrer : $C=M^e$ mod n = 66^17 mod 2773 = 872

Pour déchiffrer M=C^d mod n = 872 ^ 157 mod 2773= 66

Exercice 4 : Chiffrement El Gamal

Soit p = 53; g = 2; y = 30 la clef publique ElGamal de Bob.

1. Chiffrer le message m = 42 (en calculant r et s) avec la clef publique de Bob.
2. On suppose que la clef secrète de Bob est 13. Vérifier le et déchiffrer le message (R = 22; S = 12). Déchiffrez le message chiffré dans la première question. Qu'en pensez – vous ?

Corrigé Exercice4

Chiffrement : On génère un secret aléatoire $k \in Z_{p-1}$
Pour chiffrer le message m (avec m < p)
On calcule E(m, k) = (r, s) tel que
$r = g^k \bmod p$
$s = m.y^k \bmod p$

Déchiffrement
Pour déchiffrer (r,s), on utilise la clé privée *a*
$D(r, s) = r^{p-a-1}.s \bmod p = m.g^{ak}g^{-ak} \bmod p = m.$
$r^{p-a-1}\cdot s=(g^k)^{p-a-1}\cdot m(g^a)^k$
$=m\cdot[(g^{p-1})^k(g^k)^{-a}]\cdot(g^k)^a$
$= m \cdot 1^k \cdot(g^k)^{-a}(g^k)^a$
$=m\cdot 1$ avec $(g^k)^{-a}(g^k)^a=1$
$= m.$

On suppose que k=11 ; un nombre aléatoire à générer par l'expéditeur.
Calculons r et s. $r = g^k$ mod p = 2^11 mod 53=34 et s= $m.y^k$ mod p = 42*30^11 mod 53 =12
Donc (r,s)=(34, 12)

Pour déchiffrer le message : m= r^{p-a-1}.s mod p = $22^{(53-13-1) \bmod 53}$ = 32^39 *12 = 42
Pour déchiffrer le message de la question1) m= r^{p-a-1}.s mod p = $34^{(53-13-1) \bmod 53}$ = 34^39 *12 mod 53 = 42
C'est le meme cryptogramme. Donc El gamal génère deux ciphers pour le même message à cause du nombre aléatoire utilisé au moment du chiffrement. C'est un chiffrement non déterministe.

Exercice 5 : Chaînes de certification

Alice reçoit le certificat de Bob signé par l'autorité de certification TrustSign. Malheureusement Alice ne connaît pas la clef publique de TrustSign. Il se trouve que cette clef (i.e., clef publique de TrustSign) est certifiée par l'autorité de certification VeriSign (dite racine) dont Alice a entièrement confiance.

a) Dessinez le graphe hiérarchique des différents certificats, en indiquant à chaque fois les clés authentifiées.
b) Dessinez le graphe de la chaîne de confiance qui en résulte. Comment Alice pourra-elle vérifier le certificat de Bob ?
c) Que pouvez-vous dire de la validité de la clef contenu dans le certificat de Bob ?