Travaux dirigés –TD
Cryptographie et services de sécurité

Exercice 1 : **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.

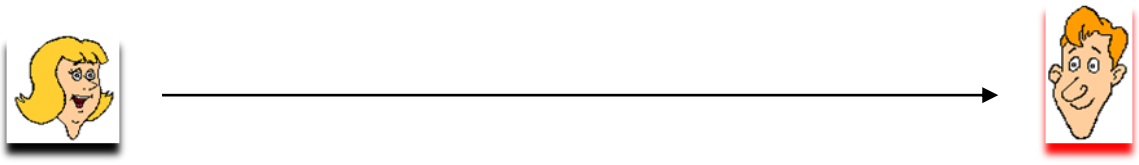
- De quel paramètre avez-vous besoin pour déchiffrer le message ? Comment-pouvez-vous l'obtenir ?
- Décrypter le texte.
- Expliquer brièvement, si vous considérez que le résultat du déchiffrement est raisonnable ou non.

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**.



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).

Exercice 3 : Chiffrement 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.

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. (On suppose k=11)
2. On suppose que la clef privée de Bob est a=13. Vérifier le et déchiffrer le message (r = 22; s = 12). Déchiffrez le message chiffré dans la première question. Qu'en pensez – vous ?

Rappel sur l'algorithme El Gamal:

Paramètres :

- p, un grand nombre premier
- g, un générateur de Z_p^*
- $a \in Z_{p-1}$, $y = g^a \bmod p$
- Clé Publique: (p, g, y), Clé privée : a

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

$D(r, s) = r^{p-a-1}.s \bmod p = m.g^{ak}g^{-ak} \bmod p = m.$

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 ?