Travaux dirigés –TD 1
Services de la sécurité

Partie 1 : Relations entre les attaques et les services

Exercice 1 :

Classer chacun des éléments suivants comme une violation de (A) confidentialité, (B) l'intégrité, (C) l'authentification, ou (D) la non-répudiation :

a) Alice lit le courrier électronique de Bob, qui est envoyé à Eve → A
b) Alice envoie un courrier électronique au nom de Bob à Eve → C
c) Alice transmet un e-mail à Bob et ne le reconnait pas → D
d) Alice modifie l'e-mail envoyé de Bob à Eve → B

Faire un petit rappel sur les services de securité avec les differents mécanismes

Exercice 2 :

Remplir le tableau suivant :

Service	Mécanisme(s)	Algorithme(s)	Type d'attaque
Confidentialité	chiffrement	DES, AES RC4	cryptanalyse MITM
Intégrité	hachage	MD5, SHA-1 SHA-256	chosen-prefix attack Collision attack
Authentification	Mot de passe Signature	RSA, EAP	Force brute

Exercice 3 : Robustesse des mots de passe

On suppose que le mot de passe utilisé pour s'authentifier en tant que *root* sur un serveur a une longueur de 6 octets. Tous les caractères alphanumériques majuscules et minuscules peuvent être utilisés dans ce mot de passe. Combien de temps une telle attaque par *Brute Force* dure-t-elle si l'ordinateur utilisé pour réaliser l'attaque

a) Prend une dixième de seconde pour vérifier un mot de passe ?
b) Prend une microseconde pour vérifier un mot de passe ?
c) Comparez vos réponses au cas où les mots de passe ont une longueur 8 octets

* Pour faire des tests en ligne : http://password-checker.online-domain-tools.com/
http://lastbit.com/pswcalc.asp

a) il y a 62 caractères alphanumériques, on a donc 62^6.
$62^6 = 56800235584$ mots de passe. $t = \frac{62^6}{365 \times 24 \times 60 \times 60 \times 10} = 180$ ans

b) $t = \frac{62^6}{60 \times 60 \times 10^6} = 15.8$ heures

Partie 2 : Services de sécurité

Exercice 4 :

1. La signature numérique, assure :
   a. Intégrité
   b. Authentification
   c. Contrôle d'accès
   d. Intégrité et Authentification

2. Une signature numérique du message M consiste à chiffrer le hash de M avec :
   a. La clé publique de l'expéditeur
   b La clé publique du destinataire
   c. La clé privée du destinataire
   -> d. La clé privée de l'expéditeur

3. Vous pouvez récupérer un message M avec la procédure suivante
   a. Chiffrer M avec la clé publique d'Alice et déchiffrer avec la clé privée d'Alice
   b. Chiffrer M avec la clé privée de Bob et déchiffrer avec la clé publique de Bob
   c. Chiffrer M avec la clé publique de Bob et déchiffrer avec la clé privée d'Alice
   d. (a) et (b)
   e. (b) ou (c)

Exercice 5 :

Choisissez la bonne réponse et justifiez.

a) Vrai ou Faux : en cryptographie asymétrique, même l'expéditeur (qui vient de chiffrer le message) ne sera plus en mesure de lire le message après son chiffrement avec la clé publique du récepteur.

b) Vrai ou Faux : dans l'algorithme RSA, pour un modulo *n* donné, un nombre premier supérieur à 2 peut être utilisé comme exposant public e. $pgcd(e, \phi(n)) = 1$

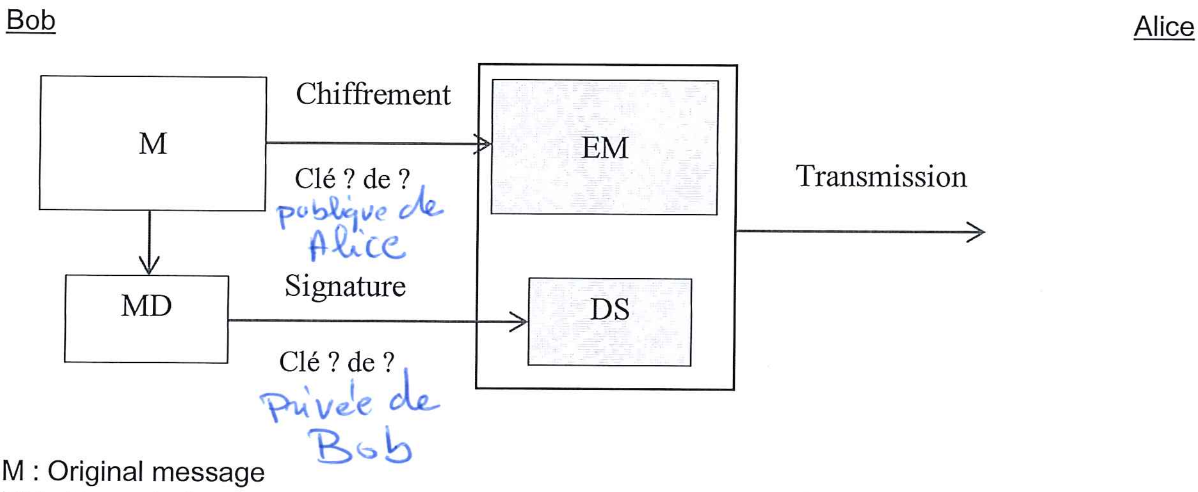
c) Vrai ou Faux : une des propriétés des algorithmes de la cryptographie à clé publique est que, s'ils sont appliqués correctement, ils fonctionnent généralement beaucoup plus rapidement que ceux de la cryptographie à clé symétrique.

d) Vrai ou Faux : l'un des principes de Kirchhoff dit que la sécurité d'un algorithme de cryptographie bien conçu ne devrait pas se baser sur le secret de l'algorithme lui-même, mais uniquement sur les clés secrètes qu'il utilise.

e) Vrai ou Faux : un HMAC (keyed-hash message authentication code) peut être utilisé pour vérifier simultanément l'intégrité de données et l'authenticité d'un message.

Exercice 6 :

La figure suivante représente le concept de la signature numérique en utilisant la technique de chiffrement à clé publique. Dans la première partie de la figure, Bob envoie à Alice le message chiffré ainsi que la signature numérique. Compléter la figure suivante et faire une autre figure qui montre la vérification (par Alice) de l'intégrité de données et l'authentification de Bob.



M : Original message
EM : Encrypted message
MD : Message Digest
DS : Digital Signature

$M = D_{K_{s}\text{-}Alice}(EM)$, $h(M) = MD1$

$MD2 = D_{K_{publique}\text{-}Bob}(DS)$

si $MD1 = MD2$

$\Rightarrow$ Message authentique

Partie 3 : Rappels arithmétiques et mécanismes de base

Exercice 7 :

Calcul de l'inverse de 18 mod 35

a. 4
b. -17
c. 36
d. 2

D'après le theoreme de Bezout : $18u + 35v = 1$ (v est l'inverse de 18[35])

$35 = 18 \times 1 + 17$

$18 = 17 \times 1 + 1$

$1 = 18 - 17 \times 1 = 18 - (35 - 18 \times 1) = 18 - 35 + 18 \times 1 = -35 + 2 \times 18$

$\Rightarrow$ l'inverse de 18[35] = 2.

Exercice 8 :

Le pgcd de a = 600 et b = 124 est

e. 3
f. 6
g. 4
h. 1

Theoreme de Bezout : $PGCD(600, 24) = 600u + 124v$

$600 = 124 \times 4 + 104$

$124 = 104 \times 1 + 20$

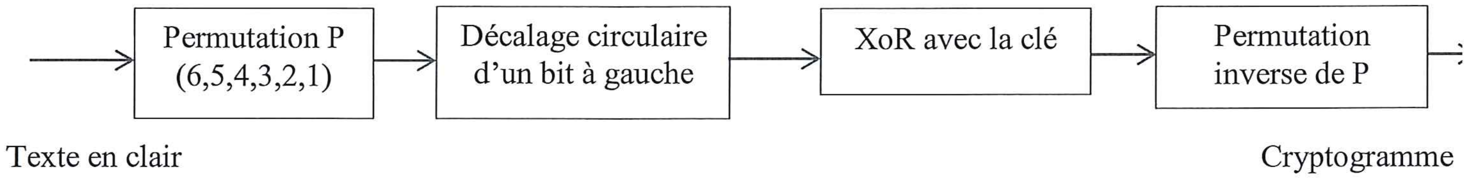
$104 = 20 \times 5 + 4$

$20 = 4 \times 5 + 0$

$PGCD(600, 124) = 4$

Exercice 9 : Chiffrement

On veut chiffrer la matrice 1 0 1 1 0 1 en utilisant la séquence suivante d'opérations. Si la clé est 0 1 0 0 1 0, quel sera le texte chiffré ?



plain text = 101101

permutation = 101101

decalage : 011011

XoR : 011011 ⊕ 010010 = 001001 , P^{-1} = 100100

Partie 4 : Algorithmiques

Exercice 10 : Attaque contre l'échange de clés par l'algorithme Diffie-Hellman

Alice et Bob utilisent l'algorithme de Diffie-Hellman pour échanger une clé secrète. Eve intercepte les valeurs suivantes : p = 283, g = 12, A = 77 et B = 196. A= g^a mod p et B = g^b mod p

a) Quelles sont les étapes à suivre par Eve pour trouver la clé secrète ?
b) Calculez la valeur de cette clé.
c) Donner une recommandation pour empêcher ce type d'interception.

a) Eve doit calculer le logarithme discret de A ou de B
si Eve trouve(a), alors $K = B^a$ mod , $K = A^b \bmod p$

b) a est un nombre aléatoire entre 1 et p-1 , $a \in \{1, 2, 3, \ldots 282\}$

$A = g^a \bmod p$

$12^1 \bmod 283 = 12$

$12^2 \bmod 283 = 144$

$12^3 \bmod 283 = 30$

$12^4 \bmod 283 = 77$ donc $K = 196^4 \bmod 283 = 90$

c) - (a, b) de très grande taille (100 digits)
- Signature numerique.

Exercice 11 : Chiffrement RSA

Alice publie sa clé publique n = 187 et e = 7.

a) Encoder le message m = 15 avec la clé publique d'Alice
b) En utilisant le fait que φ (n) = 160, retrouver la factorisation de n, puis la clé privée d'Alice

a) $C = m^e \bmod n = 15^7 \bmod 187 = 93$

b) $n = p \cdot q$ et $\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$

$p + q = n - \phi(n) + 1 = 187 - 160 + 1 = 28$

$x^2 - (p+q)\,x + pq = x^2 - 28x + 187 = 0$

$\Delta = b^2 - 4ac = 36$, $p = \frac{28-6}{2} = 11$ et $q = \frac{28+6}{2} = 17$

clé privée : $e \cdot d = 1 \bmod \phi(n) \Rightarrow 7 \cdot d = 1 \bmod 160$

d'après le theoreme de Bezout : $d = 23$.

Verifications : $M = C^d \bmod n = 93^{23} \bmod 187 = 15$.

Exercice 12 : Chiffrement/Attaques RSA

Dans le cadre de l'échange des paramètres publics de RSA entre Alice et Bob, on suppose qu'un pirate a vu passer modulo n = 1073 et e = 73. Le couple (n,e) est la clé publique du chiffrement, alors que le couple (n,d) est sa clé privée.

a) Le pirate peut-il calculer la clé privée d'Alice ?
b) Le pirate a sniffé le réseau et a trouvé le texte chiffré : 423 en HEX. Quel est le message échangé entre Alice et Bob ?

a) Oui c'est possible. on cherche les nombres premiers entre 2 et $\sqrt{1073}$

$\Rightarrow 2, 3, 5, 7, \ldots, 31$, $1073 = 29 \times 37 \Rightarrow p = 37$ et $q = 29$

$e \cdot d = 1 \bmod \phi(n) \Rightarrow 73 \cdot d = 1 \bmod 1008$

alors $73u + 1008v = 1$ d'après Bezout :

$1008 = 73 \times 13 + 59$

$73 = 59 \times 1 + 14$

$59 = 14 \times 4 + 3$

$14 = 3 \cdot 4 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \times 2 + 0$

$\boxed{d = 649}$

clé publique : $\boxed{73, 1073}$

clé privée : $\boxed{(649, 1073)}$

b) $(423)_{Hex} = (1059)_{10}$

$M = C^d \bmod n = (1059)^{649} \bmod 1073 = 97$ c'est la lettre (a) en ASCII

Exercice 13 : Chiffrement/Attaques RSA

Bob et Bernard ont pour clé publique RSA respectivement (n, e1) et (n, e2) avec e1 et e2 premiers entre eux. Alice envoie le même message *m* crypté par les clés publiques RSA de Bob et Bernard en c1 et c2. Expliquer comment Eve, qui intercepte les deux messages cryptés et qui connait les clés publiques de Bob et Bernard, peut retrouver le message *m*. Application numérique : m=2, n=21, e1=5, e2=13.

$$\text{Alice} \xrightarrow{C_1 = M^{e_1} \bmod n} \text{Bob}$$

$$\text{Alice} \xrightarrow{C_2 = M^{e_2} \bmod n} \text{Bernard}$$

EVE

$$C_1^u \times C_2^v = (M^{e_1})^u \times (M^{e_2})^v = M^{e_1 u + e_2 v} = M$$

$$e_1 u + e_2 v = 1$$

$n = 21$, $e_1 = 5$, $e_2 = 13$ et $M = 2$

$$\left.\begin{aligned} C_1 &= 2^5 \bmod 21 = 32 \bmod 21 = 11 \\ C_2 &= 2^{13} \bmod 21 = 8192 \bmod 21 = 8 \end{aligned}\right\}$$

$e_1 u + e_2 v = 1 \Rightarrow 5u + 13v = 1$

$$\left.\begin{aligned} 13 &= 5 \times 2 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}\right\} \begin{aligned} 1 &= 3 - 2 \times 1 = 3 - (5 - 3 \times 1) \times 1 = 3 - 5 \times 1 + 3 \times 1 \\ &= 2 \times 3 - 5 \times 1 \\ &= 2(13 - 5 \times 2) - 5 \times 1 = 2 \times 13 - 5 \times 5 \end{aligned}$$

$\Rightarrow u = -5$ et $v = 2$.

$$C_1^u \times C_2^v = (2^5)^{-5} \times (2^{13})^2 [21] = 2^{-25} \times 2^{26} [21] = 2^1 [21] = 2$$

donc $\boxed{m = 2}$