Travaux dirigés –TD
Services de la sécurité

Exercice 1 : Rappels

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
b) Alice envoie un courrier électronique au nom de Bob à Eve
c) Alice transmet un e-mail à Bob et ne le reconnait pas
d) Alice modifie l'e-mail envoyé de Bob à Eve

Exercice 2 : services de sécurité

Remplir le tableau suivant :

Service	Mécanisme(s)	Algorithme(s)	Type d'attaque
Confidentialité			
Intégrité			
Authentification			

Exercice 3 : Robustesse des mots de passe

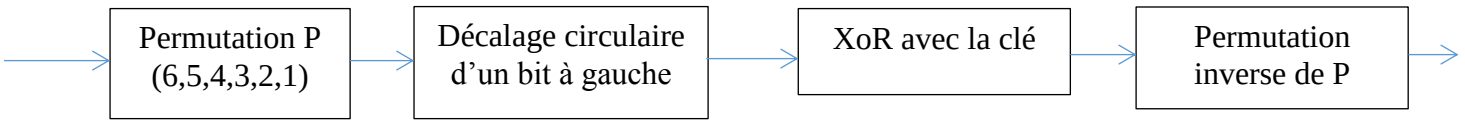
On suppose que le mot de passe utilisé pour s'authentifier en tant que *root* sur un serveur a une longueur de 6 octets. Tous les caractères alphanumériques majuscules et minuscules peuvent être utilisés dans ce mot de passe. Combien de temps une telle attaque par *Brute Force* dure-t-elle si l'ordinateur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

Exercice 4 : 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 ?



Texte en clair Cryptogramme

Exercice 5 : Chiffrement de Feistel

Un réseau ou chiffrement de Feistel est subdivisé en plusieurs étages (tours). Un chiffrement de Feistel est un chiffrement itéré qui utilise à chaque étage le même schéma pour chiffrer un bloc. Le message est découpé en blocs qui subissent une suite de transformations. On définit le schéma de Feistel Ψ lié à une fonction *f* (appelée la fonction de confusion) de la manière suivante :

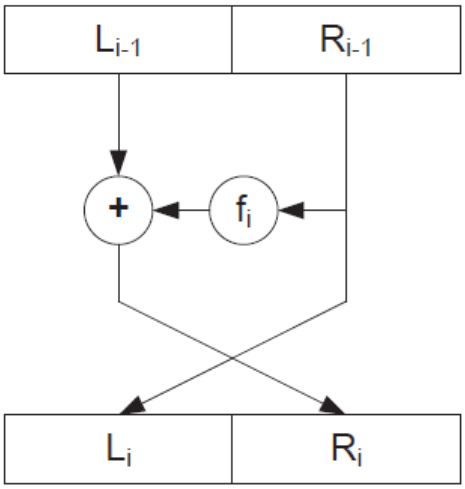


Figure 1. Schéma de Feistel

DES (*Data Encryption Standard*) est un schéma à 16 tours et Triple DES est un schéma 48 tours. On suppose dans cet exercice qu'on un schéma de Feistel à trois tours. Considérons le message à six bits 101110. Le message est découpé en deux parties de trois bits $L_0 = 101$ et $R_0 = 110$ (L pour *Left* et R pour *Right*). Les trois fonctions *f1*, *f2* et *f3* constituent la clé de chiffrement.

f_1 :				f_2 :				f_3 :			
	000	→	110		000	→	010		000	→	111
	001	→	100		001	→	011		001	→	010
	010	→	111		010	→	110		010	→	110
	011	→	000		011	→	111		011	→	110
	100	→	110		100	→	000		100	→	000
	101	→	010		101	→	101		101	→	101
	110	→	001		110	→	110		110	→	100
	111	→	101		111	→	110		111	→	001

Chiffrement : $L_1 = R_0$, $R1 = L_0 \oplus f(R_0)$
Déchiffrement : $R_0 = L1$, $L_0 = R_1 \oplus f(R_0)$

R_0	L_0
1 0 1	1 1 0

Quel est le message final après les trois tours de Feistel ?

Exercice 6 : Rappels Mathématiques

Calculer l'inverse de 18 mod 35
a) 4 b) -17 c) 36 d) 2

Le pgcd de a = 600 et b = 124 est : a) 3 b) 6 c)4 d) 1

Exercice 7 : 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. $A= g^a \bmod p$ et $B = g^b \bmod p$

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.

Exercice 8 : cryptographie asymétrique

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)

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.

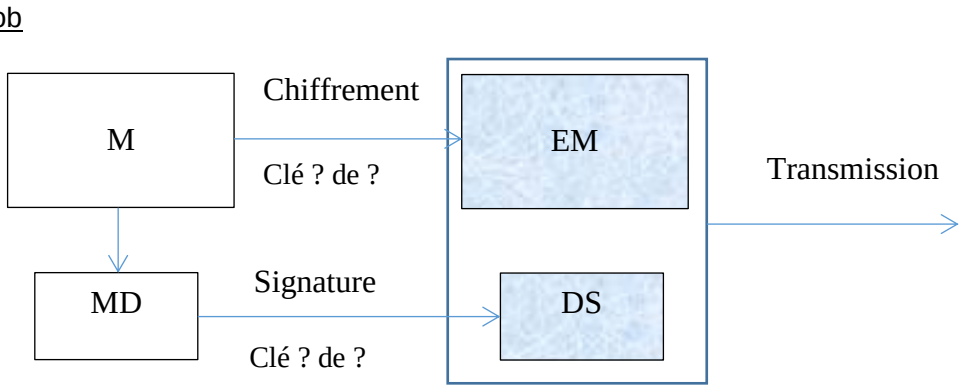
b) Vrai ou Faux : dans l'algorithme RSA, pour un modulo *n* donné, un nombre premier supérieur à 2 peut être utilisé comme exposant publique e.

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.

Exercice 9 : scénario cryptographie asymétrique

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

Exercice 10 : 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

Exercice 11 : 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 ?

Exercice 12 : 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.

Exercice supplémentaire : Casser une clé symétrique par la force brute

La puissance d'une machine est le nombre d'instructions qu'elle exécute par unité de temps. Cette puissance est exprimée en MIPS (Million d'instructions par seconde) qui est l'unité de mesure des processeurs. La puissance de la machine utilisée est environ 60 000 MIPS (cas d'un Intel *Core 2 Extreme QX9770* 59,455 MIPS at 3.2 GHz). Un algorithme optimisé est utilisé pour tester une clé de 128 bits de l'algorithme AES. Cet algorithme utilise environ 1200 instructions élémentaires pour tester une clé.

On dispose le *ciphertext* et le *plaintext* et on désire retrouver la clé par force brute (c.-à-d. tester toutes les possibilités). Combien y a-t-il de clés possibles ? En combien de temps une machine *Intel Core 2 Extreme QX9770* teste-t-elle une clé ? Combien faut-il attendre pour décrypter le *ciphertext* si on dispose une seule machine ?