TD1

Mécanismes cryptographique de la sécurité

Exercice 1 :

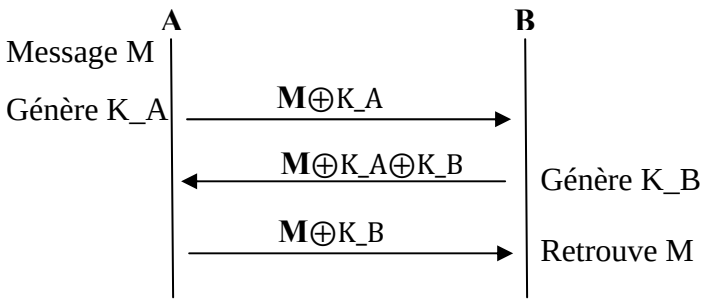
Soit un système de communication à N nœuds où les messages échangés entre les nœuds peuvent être facilement écoutés. Quel est le nombre de clés à maintenir par chaque nœud pour assurer une communication secrète entre chaque paire de nœuds :

a. Pour un système à clés symétrique ?
b. Pour un système à clé asymétrique ?

Exercice 2 :

Soit **M** un message et **K** une clé aussi longue que **K**. On note **C=M⊕K** le message **M chiffré avec K.** Si m[i] est le i^{ème} bit du message m et k[i] est le i^{ème} bit de la clé K, alors le i^{ème} bit de M⊕K est égal à (M[i] ⊕ K[i]))

1) Montrez que le "ou exclusif ⊕ " est une technique de chiffrement symétrique.
2) Est-il pratique de stocker des clés symétriques aussi longues que les messages à chiffrer?
3) Soit le protocole suivant qui exploite le "ou exclusif ⊕ " pour le chiffrement d'un message M. Quand A veut envoyer un message M à B, il génère une clé K_A aussi longue que M. B génère aussi une clé K_B aussi longue que M.
   c. Comment B peut-il déterminer la taille de la clé K_B ?
   d. Comment A peut-il déterminer M⊕K_B à partir de M⊕K_A⊕K_B ?
   e. Comment B retrouve t-il M ?
   f. Si tous les messages échangés peuvent être écoutés, ce protocole permet-il la confidentialité.

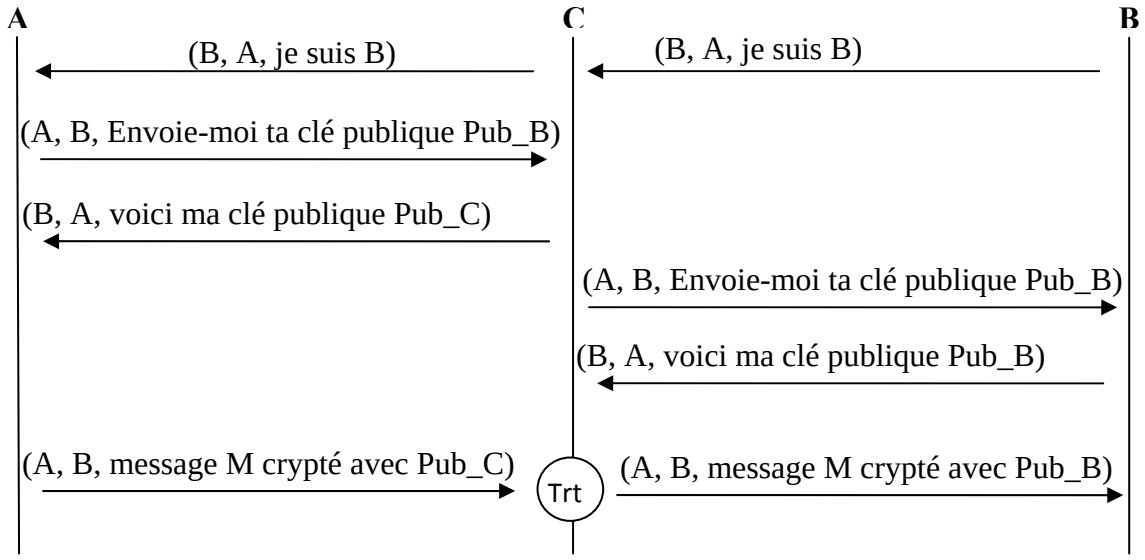


Rappel : $A \oplus A = 0$; $A \oplus 0 = A$;

Exercice 3 :

Soit l'échange de messages suivant entre 3 entités A, B et C (un intrus) utilisant un système de chiffrement asymétrique. Nous utilisons le format suivant (source, destination, message)

1) Quel est le traitement **Trt** effectué par C.
2) A et B se rendent-ils compte de l'existence de l'intrus C
3) Proposer une solution permettant de remédier à cette attaque



Exercice 4 : cryptographie symétrique

Soit **M** un message divisé en blocs $\{x_1,x_2,x_3,\ldots x_p\}$chacun de taille **n** bits et soit **K** une clé de même taille que les blocs (n bits). Soit $\{c_1,c_2,c_3,\ldots c_p\}$les cryptogrammes des blocs obtenus en appliquant la clé K aux blocs. Le chiffrement des blocs se fait selon le schéma suivant:

C_0= IV (valeur initiale) ; pour i de 1 à p, $c_j=E_K(C_{j-1}\oplus x_j)$

1) La fonction E_K est inversible et son inverse est **D_K**. Montrer que l'opération de déchiffrement est **$x_j=C_{j-1}\oplus D_K(C_j)$** (rappel : A⊕**A=0 ; A⊕0=A,** A⊕**B=** B⊕**A)**
2) Peut-on chiffrer un bloc quelconque du message M sans chiffrer les blocs qui le précèdent ? Expliquer ?
3) Peut-on déchiffrer un bloc quelconque c_i sans déchiffrer les blocs qui le précèdent ? Expliquer ?
4) Peut-on déchiffrer un bloc **c_j** en l'absence des autres blocs chiffrés ? Expliquer ?
5) Prenons le cas où **$E_K(x)=D_K(x)=K\oplus x$.** Supposons qu'un attaquant a pu récupérer deux blocs consécutifs (x_{j-1},x_j) ainsi que leurs cryptogrammes correspondants (c_{j-1},c_j). Montrer que cet attaquant peut en déduire la clé de chiffrement K.
6) Soient A et B deux entités utilisant le procédé de chiffrement décrit dans cet exercice. La clé K doit être échangée d'une façon **sécurisé et authentifié**. Pour cela A et B font appel au chiffrement asymétrique. A calcule la clé K, la chiffre pour obtenir KC et l'envoi à B.
    a. Avec quelle clé A doit chiffrer K ?
    b. Avec quelle clé B déchiffre KC ?
    c. Expliquer pourquoi cette méthode n'est pas authentifiée et proposer une solution ?

Exercice 5 : chiffrement RSA

Question 1 : Effectuer le chiffrement et le déchiffrement en utilisant l'algorithme RSA pour les valeurs suivantes:

Les deux nombres premiers p = 3 et q = 11

e = 7

Le message M = 5

Question 2 : Soit un système à clé publique utilisant le RSA, vous interceptez le texte chiffré C=10 envoyé par un utilisateur dont la clé publique est e = 5 et n = 35.

Que vaut M ?

Quelle est la clé privée de cet utilisateur ?

TD2 : corection

Mécanismes cryptographique de la sécurité

Exercice 1 :

Soit un système de communication à N nœuds où les messages échangés entre les nœuds peuvent être facilement écoutés. Quel est le nombre de clés à maintenir par chaque nœud pour assurer une communication secrète entre chaque paire de nœuds :

g. Pour un système à clés symétrique ? ➔ **(N-1) clés**
h. Pour un système à clé asymétrique ? ➔ **2 clés : sa clé privée et sa clé publique**

Exercice 2 :

Soit **M** un message et **K** une clé aussi longue que **M**. On note **C=M⊕K** le message **M chiffré avec K.** Si m[i] est le i^{ème} bit du message m et k[i] est le i^{ème} bit de la clé K, alors le i^{ème} bit de M⊕K est égal à (M[i] ⊕ K[i]))

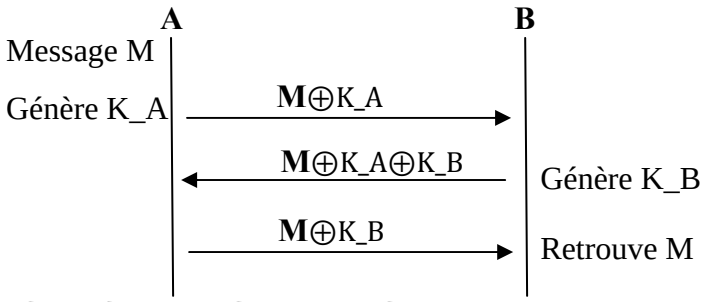
4) Montrez que le "ou exclusif ⊕ " est une technique de chiffrement symétrique.

➔ **On chiffre et on déchiffre avec la même clé K : C=M⊕K → C⊕K= M⊕K ⊕K=M**

5) Est-il pratique de stocker des clés symétriques aussi longues que les messages à chiffrer**?**

➔ **C'est inadéquat car il faut changer la clé pour chaque message et il faut la transmettre au destinataire dans un canal sécurisé.**

6) Soit le protocole suivant qui exploite le "ou exclusif ⊕ " pour le chiffrement d'un message M. Quand A veut envoyer un message M à B, il génère une clé K_A aussi longue que M. B génère aussi une clé K_B aussi longue que M.
   i. Comment B peut-il déterminer la taille de la clé K_B ?
      ➔ **même taille que M⊕K_A**
   j. Comment A peut-il déterminer M⊕K_B à partir de M⊕K_A⊕K_B ?
      ➔ **M⊕K_A⊕K_B ⊕K_A= M⊕K_B**
   k. Comment B retrouve t-il M ?
      ➔**M⊕K_B⊕K_B=M**
   l. Si tous les messages échangés peuvent être écoutés, ce protocole permet-il la confidentialité.
      ➔ **non, un ou exclusif entre les trois message donnera M**



Rappel : $A \oplus A = 0$; $A \oplus 0 = A$;

Exercice 3 :

Soit l'échange de messages suivant entre 3 entités A, B et C (un intrus) utilisant un système de chiffrement asymétrique. Nous utilisons le format suivant (source, destination, message)

4) Quel est le traitement **Trt** effectué par C.

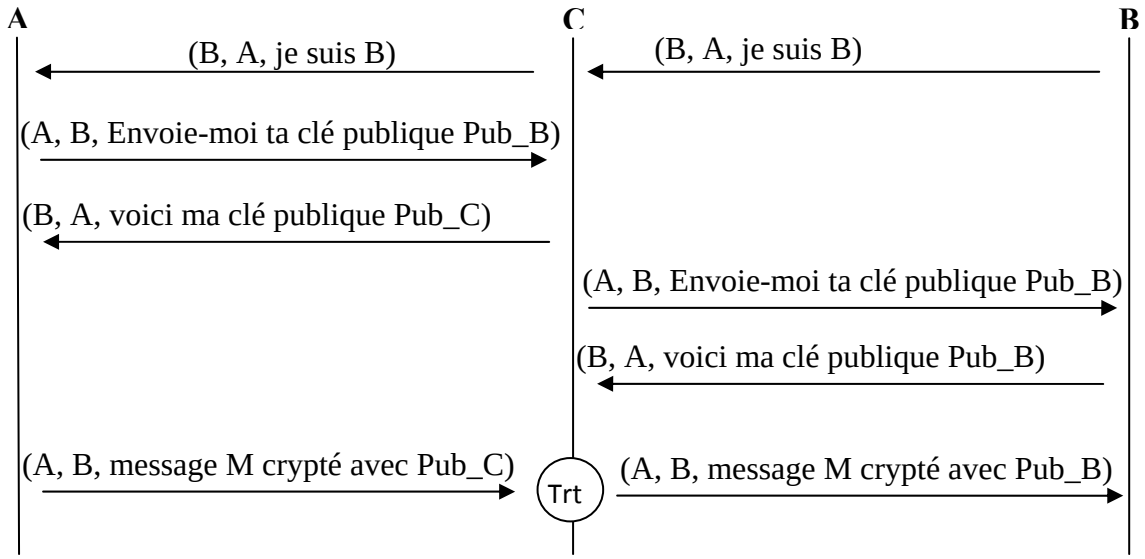
➔ **déchiffrement avec Pub_C puis chiffrement avec Pub_B**

5) A et B se rendent-ils compte de l'existence de l'intrus C

➔ **non**

6) Proposer une solution permettant de remédier à cette attaque

➔ **utiliser l'authentification par certificat qui assure l'appartenance d'une clé publique à une entité**



Exercice 4:

Soit **M** un message divisé en blocs $\{x_1,x_2,x_3,\ldots x_p\}$chacun de taille **n** bits et soit **K** une clé de même taille que les blocs (n bits). Soit $\{c_1,c_2,c_3,\ldots c_p\}$les cryptogrammes des blocs obtenus en appliquant la clé K aux blocs. Le chiffrement des blocs se fait selon le schéma suivant:

C_0= IV (valeur initiale) ; pour i de 1 à p, $c_j=E_K(C_{j-1}\oplus x_j)$

1) La fonction E_K est inversible et son inverse est **D_K**. Montrer que l'opération de déchiffrement est **$x_j=C_{j-1}\oplus D_K(C_j)$** (rappel : A⊕**A=0 ; A⊕0=A,** A⊕**B=** B⊕**A)**

$c_j=E_K(C_{j-1}\oplus x_j)$ ➔ $D_K(c_j)= D_K(E_K(C_{j-1}\oplus x_j))$

➔ **$D_K(c_j)= C_{j-1}\oplus x_j$**

➔ **$C_{j-1}\oplus D_K(c_j)= C_{j-1}\oplus C_{j-1}\oplus x_j$**

➔ **$C_{j-1}\oplus D_K(c_j)= x_j$**

2) Peut-on chiffrer un bloc quelconque du message M sans chiffrer les blocs qui le précèdent ? Expliquer ?
   ➔ **Non, selon la formule $x_j=C_{j-1}\oplus D_K(C_j)$, le chiffrement de x_j nécessite C_{j-1}**

3) Peut-on déchiffrer un bloc quelconque c_i sans déchiffrer les blocs qui le précèdent ? Expliquer ?
   ➔ **Oui, x_j ne dépend pas de x_{j-1}**

4) Peut-on déchiffrer un bloc $\mathbf{c_j}$ en l'absence des autres blocs chiffrés ? Expliquer ?
   ➔ **Non, selon la formule $x_j=C_{j-1}\oplus D_K(C_j)$, le déchiffrement de c_j nécessite C_{j-1}**

5) Prenons le cas où $\mathbf{E_K(x)=D_K(x)=K\oplus x}$. Supposons qu'un attaquant a pu récupérer deux blocs consécutifs (x_{j-1},x_j) ainsi que leurs cryptogrammes correspondants (c_{j-1},c_j). Montrer que cet attaquant peut en déduire la clé de chiffrement K.
   Dans ce cas : $c_j=K\oplus C_{j-1}\oplus x_j$ ➔ $K= c_j\oplus C_{j-1}\oplus x_j$

6) Soient A et B deux entités utilisant le procédé de chiffrement décrit dans cet exercice. La clé K doit être échangée d'une façon **sécurisé et authentifié**. Pour cela A et B font appel au chiffrement asymétrique. A calcule la clé K, la chiffre pour obtenir KC et l'envoi à B.
   a. Avec quelle clé A doit chiffrer K ? ➔ **avec la clé publique de B**
   b. Avec quelle clé B déchiffre KC ? ➔**avec sa clé privée**
   c. Expliquer pourquoi cette méthode n'est pas authentifiée et proposer une solution ?
      ➔ **Rien ne garantit l'appartenance de la clé publique de B à B.**

      Solution : certification de la clé publique de B.

Exercice 5 : chiffrement RSA

Question 1 : Effectuer le chiffrement et le déchiffrement en utilisant l'algorithme RSA pour les valeurs suivantes:

Les deux nombres premiers p = 3 et q = 11 ; e = 7 ; Le message M = 5

➔ **$N=pq=3*11=33$ et $\varphi=(p-1)(q-1)=2*10=20$**

➔ **$e.d=1 \bmod \varphi$ ➔ $7*d=1 \bmod 20$ ➔$d=3$**

Chiffrement : $C=M^e \bmod N=5^7 \bmod 33 = 14$

Déchiffrement : $M= C^d \bmod N$ ➔ $M=C^3 \bmod 33=14^3 \bmod 33 =5$

Question 2 : Soit un système à clé publique utilisant le RSA, vous interceptez le texte chiffré C=10 envoyé par un utilisateur dont la clé publique est e = 5 et n = 35. Que vaut M ? Quelle est la clé privée de cet utilisateur ?

➔ **$N=35$ ➔ $p*q=35$ ➔ $p=5$ et $q= 7$ ou $p=7$ et $q=5$ ➔ $\varphi=(p-1)(q-1)=6*4=24$**

➔ **$e.d=1 \bmod \varphi$ ➔ $5*d=1 \bmod 24$ ➔$d=5$**

➔ **$M= C^d \bmod N$ ➔ $M= 10^5 \bmod 35 =5$**