

TD1

Mécanismes cryptographique de la sécurité

Exercice 1 :

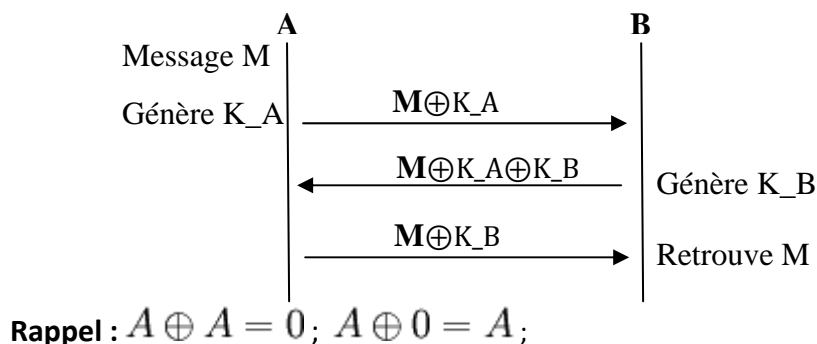
Soit un système de communication à N nœuds où les messages échangés entre les nœuds peuvent être facilement écoutés. Quel est le nombre de clés à maintenir par chaque nœud pour assurer une communication secrète entre chaque paire de nœuds :

- Pour un système à clés symétrique ?
- Pour un système à clé asymétrique ?

Exercice 2 :

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

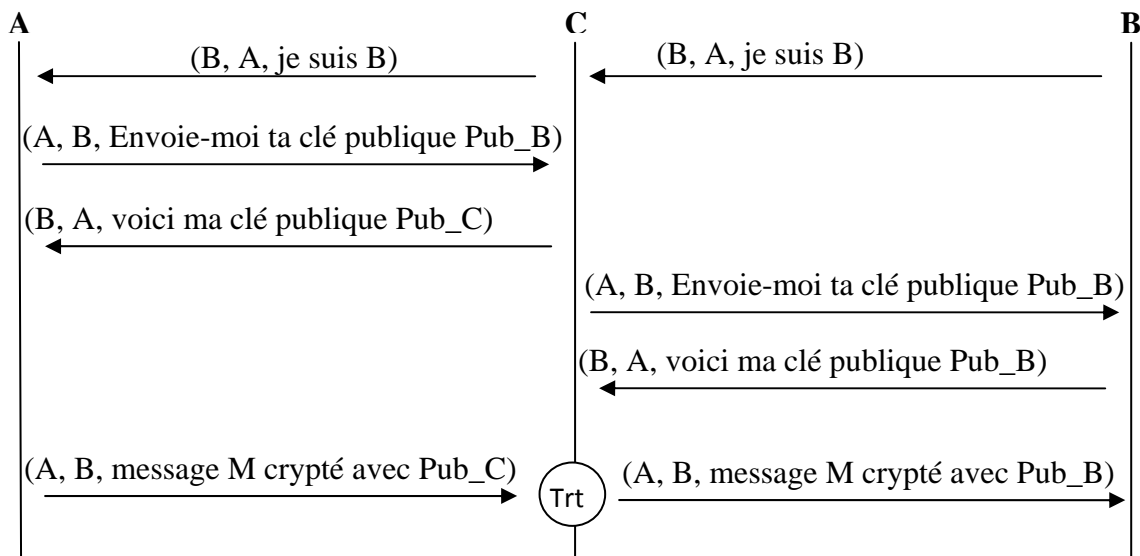
- Montrez que le "ou exclusif \oplus " est une technique de chiffrement symétrique.
- Est-il pratique de stocker des clés symétriques aussi longues que les messages à chiffrer?
- Soit le protocole suivant qui exploite le "ou exclusif \oplus " pour le chiffrement d'un message M . Quand A veut envoyer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



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 $\{x_1, x_2, x_3, \dots, x_p\}$ chacun de taille **n** bits et soit **K** une clé de même taille que les blocs (n bits). Soit $\{c_1, c_2, c_3, \dots, c_p\}$ 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 , $c_i = E_K(C_{i-1} \oplus x_i)$

- 1) La fonction E_K est inversible et son inverse est D_K . Montrer que l'opération de déchiffrement est $x_i = C_{i-1} \oplus D_K(C_i)$ (rappel : $A \oplus A = 0$; $A \oplus 0 = A$, $A \oplus B = B \oplus A$)
- 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_i 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 ?