

## TD2

### Mécanismes cryptographique de la sécurité

#### Exercice 1 :

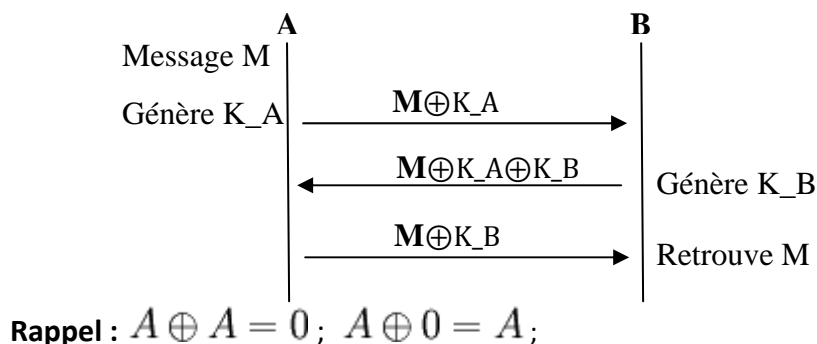
Soit un système de communication à  $N$  nœuds où les messages échangés entre les nœuds peuvent être facilement écoutés. Quel est le nombre de clés à maintenir par chaque nœud pour assurer une communication secrète entre chaque paire de nœuds :

- 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

