Université de khenchela
Faculté des sciences et Technologies L3 ISIL

TD 3 :Cryptographie moderne

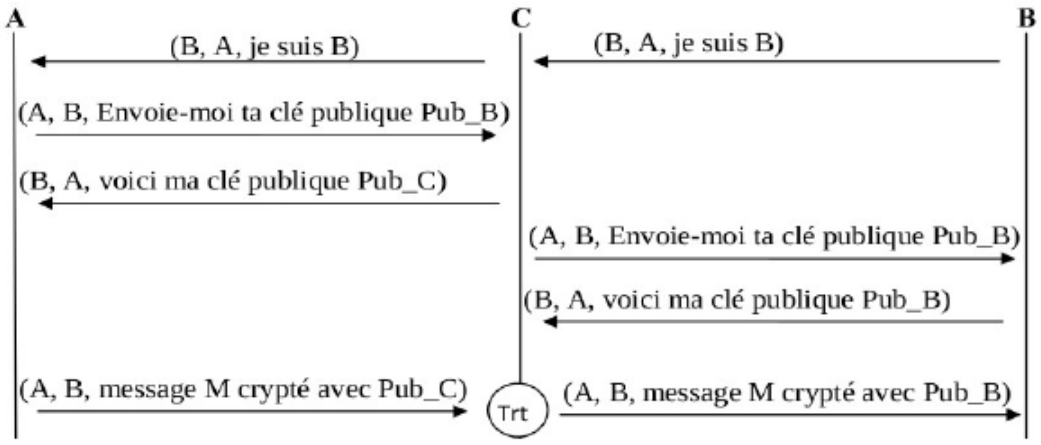
1 Exercice

Soit un système de communication à N noeuds où les messages échangés entre les noeuds peuvent être facilement écoutés.

1. Quel est le nombre de clés à maintenir par chaque noeud pour assurer une communication sécurisée entre chaque paire de noeuds :
   (a) Pour un système à clés symétrique ?
   (b) Pour un système à clés asymétrique ?
2. En déduire le nombre de clés du système pour chaque cas

2 Exercice

La figure suivante présente l'échange de messages entre 3 entités A, B et C (un intrus) utilisant un système de chiffrement asymétrique. Nous utilisons le format des messages 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