Cours IRC, TD: Cryptologie et Sécurité

Grenoble INP Ensimag - 1ère Année

1 Chiffrements symétrique et asymétrique

Un groupe de n étudiants souhaite utiliser un système cryptographique afin de pouvoir s'échanger des messages confidentiels. On entend par là que chaque message ne doit être lisible que par son destinataire (évidemment l'émetteur connaîtra aussi le message) et que chaque étudiant peut s'adresser à n'importe quel autre étudiant du groupe.

Question 1 *On utilise un chiffrement symétrique. Combien de clefs secrètes K_i un étudiant doit-il stocker ? Combien de clefs sont nécessaires en tout ? Faire un diagramme temporel représentant un échange de message entre deux étudiants.*

Question 2 *En utilisant un chiffrement asymétrique, combien de couples (Ke,Kd) de clefs publique/privée sont nécessaires ? Combien de clefs doit stocker chaque étudiant ? Faire un diagramme temporel de l'envoi d'un message ainsi chiffré entre deux étudiants.*
Est-ce que ce système est fiable ? Sinon, quelle faiblesse possède-t-il ?

Question 3 *Les étudiants n'ont pas assez de place pour stocker toutes les clefs de leurs camarades. L'un d'eux propose la solution suivante : chacun ne conserve que son propre couple de clef privée/publique ; lorsque deux étudiants veulent communiquer, ils s'échangent leurs clefs publiques afin de chiffrer la communication.*
Est-ce que ce système est fiable ? Sinon, quelle faiblesse possède-t-il ?

Supposons que les élèves font confiance à leur professeur (hypothèse réaliste), et que celui-ci possède un couple de clefs publique/privée pour une fonction asymétrique. Afin de résoudre le problème suivant, le professeur propose d'utiliser sa paire de clefs pour signer chacune des clefs publiques des étudiants.

Question 4 *Comment un étudiant peut-il être sûr de la clef publique qu'il a reçue d'un de ses camarades ? En déduire un système permettant aux étudiants de communiquer de manière sécurisée. Faire un diagramme temporel d'un échange de message entre deux étudiants. Combien de clefs doivent être stockées par chaque étudiant ?*

2 Stockage de mot de passe

Il est possible de se connecter à un serveur comme telesun grâce à une authentification par mot de passe. Les mots de passe, au nombre de n (nombre d'utilisateurs du système, ou plus exactement de mdp différents), sont composés de t caractères (codés sur 8 bits). Pour des raisons de sécurité, les mots de passe ne sont pas stockés en clair sur telesun. En effet, en cas de compromission de telesun par un hacker, tout les mots de passe des étudiants et des enseignants seraient révélés.
Ils sont en fait stockés sous forme d'*empreinte* (*hash*) dans un fichier "shadow". Le hash est le résultat d'une fonction de hachage cryptographique (MD5, SHA-512...) h :

$$h \ : \ 0,1* \rightarrow 0,1^s \tag{1}$$

$$m \rightarrow h(m) \tag{2}$$

Il faut noter que h n'est pas injective. Il est donc théoriquement possible d'obtenir la même empreinte avec plusieurs mots de passe différents. L'intérêt réside dans le fait que l'on considère qu'il est impossible (ou très difficile) de retrouver m à partir de $h(m)$ (attaques de pré-image). Au lieu de stocker le mot de passe *pwd*, on stocke le hash du mot de passe $h(pwd)$. Le fichier shadow a alors la forme suivante :

utilisateur1 : h(pwd1)
utilisateur2 : h(pwd2)
...

Lorsqu'un utilisateur rentre son mot de passe, telesun calcule le hash de la valeur entrée au clavier et le compare avec le hash stocké dans le fichier shadow. Telesun autorise l'accès si et seulement si les deux valeurs correspondent.
On suppose qu'un attaquant a réussi à obtenir le contenu du fichier shadow. Il cherche à trouver un mot de passe d'utilisateur.

Question 5 *En essayant tous les mots de passe possibles (attaque par force brute), combien d'essais doit on faire pour obtenir au moins un mot de passe de la liste d'utilisateurs ? On supposera que $s > 8t$ (en pratique les mots de passe dépassent rarement 8 caractères soit 64 bits, alors que s vaut de 128 bits dans le cas de MD5 à 512 bits dans le cas de SHA-512). Faire l'application numérique avec $t = 8$ (valeur minimale pour les systèmes UNIX) et $n = 200$.*

Question 6 *Quel autre type d'attaque visant à récupérer les mots de passe pourriez-vous imaginer ?*

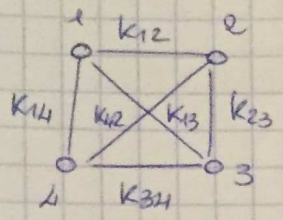
2.1 Complément d'information

Pour augmenter la sécurité du système, on utilise un grain de sel pour calculer le hash des mots de passe. Un grain de sel différent est choisi pour chaque utilisateur. le hash stocké dans le fichier shadow est alors le hash calculé à partir de la concaténation du grain de sel et du mot de passe. Ainsi le fichier shadow est de la forme :

utilisateur1,sel1 : h(sel1|pwd1)
utilisateur2,sel2 : h(sel2|pwd2)
utilisateur3,sel3 : h(sel3|pwd3)
...

TD NF1

Q1)



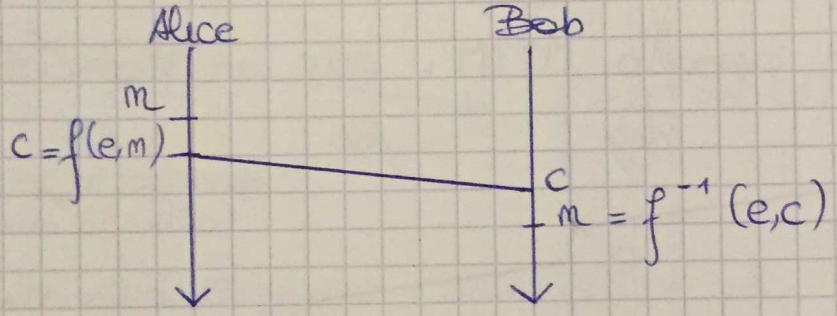
pour un ensemble de n étudiant. Chaque étudiant détient (n-1) clés

Et ce que chaque étudiant a une clé commune avec le précédent

Le système comprend $(n-1)+(n-2)+(n-3)+$ — etc....

Soit $\sum_{i=1}^{n} i = \frac{n(n-1)}{2}$ clés

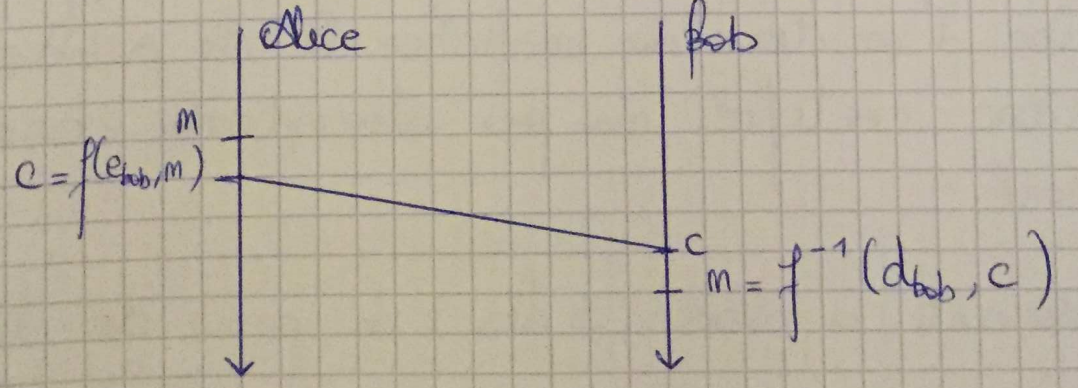
↳ Quadratique, ça augmente très rapidement



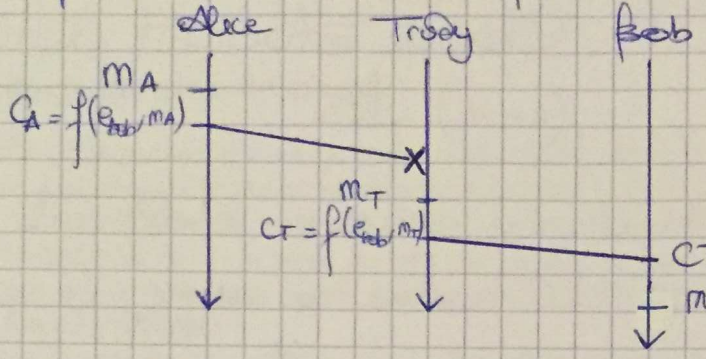
Le problème de la clé symétrique est qu'il faut à priori l'envoyer : Danger

Q2) En usant d'un chiffrement asymétrique, chaque étudiant doit avoir $\underbrace{n-1}_{\text{clé publ autre}} + \underbrace{2}_{\text{clé perso (privée + publ)}} = n+1$ clés

En tout il y a $2n$ clés : linéaire donc bien

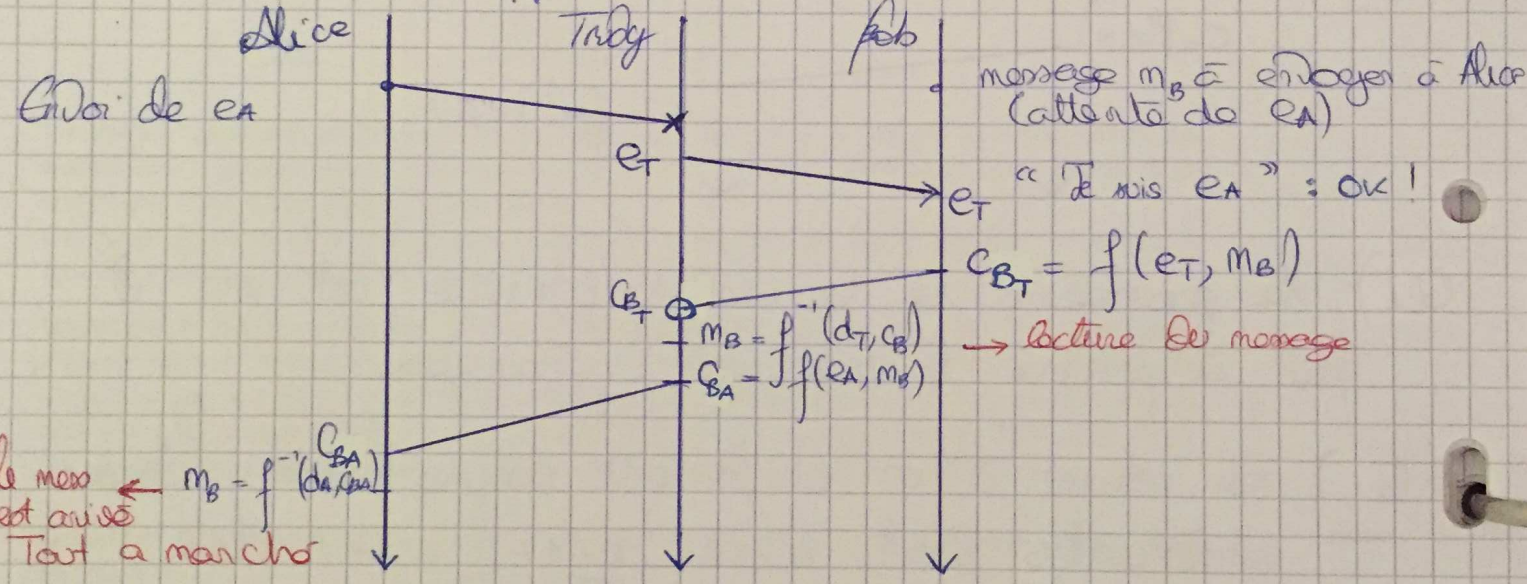


Le système est assez fiable mais la clé étant publique, il y a possibilité d'usurpation d'identité



Q3) Le fait que la clé public soit échangé lors du dialogue permet une capture et lecture d'un message

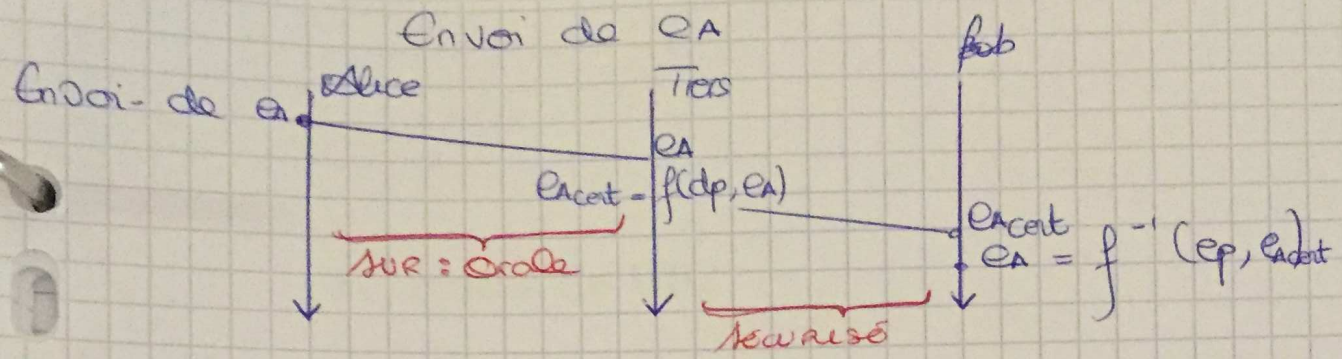
C'est ce qu'on appelle MITM : man in the middle.



Q4) Ce qu'il serait bien c'est que quand Bob reçoit la clé publique il y ait une certification On use alors d'un tiers de confiance de clé publique diffusé et donc certifié car pas interceptable comme précédemment

Chaque étudiant a alors 3 clés : la paire de clé puis la clé du tiers

De plus le tiers crypte avec sa clé privée, donc le message ne peut être usurpé car il serait décrypté et ne voudrait rien dire



Néanmoins dans un souci d'efficacité (rapidité) on préfère utiliser du symétrique

Alors, comment échanger les clés ?

Alice — g, p connue — Bob

$x = \text{random}()$ — $y = \text{random}()$

$e = g^x \bmod(p)$ → $f = g^y \bmod(p)$ (e reçu)

(f reçu) ←

Ainsi la clé commune aux deux est $K = e^y = f^x = g^{xy} \bmod$

Si il y a interception au milieu, vu que x, y sont inconnus, K n'est pas interceptable