Introduction à la sécurité et à la cryptographie
Examen – 1ère session

Jérémie Detrey
Jeremie.Detrey@loria.fr

29 mars 2016

Durée : 2 heures.
Les notes (transparents de cours, sujets de TD et TP, notes personnelles) **sont autorisées**.
Par contre, calculatrices, téléphones portables, ordinateurs ou autres **ne sont pas autorisés**.
Les exercices sont **indépendants**, vous pouvez donc les traiter dans l'ordre que vous souhaitez.
Le barème est donné à titre indicatif.
Détaillez et justifiez vos réponses.

1 Secure Shell (SSH) (5 points)

On peut décrire sommairement le protocole SSH par les étapes suivantes :

1. Établissement d'un canal confidentiel :
   (a) Sur requête du client, le serveur envoie sa clé publique PK en clair au client. Ce dernier la conserve en mémoire s'il ne la possède pas, ou la compare à la version qu'il a en mémoire s'il l'a déjà enregistrée. En cas de différence, le client prévient l'utilisateur qu'un risque de compromission du serveur existe.
   (b) Le client tire au hasard une clé de session et l'envoie au serveur en la chiffrant avec PK, la clé publique du serveur.
   (c) Le serveur déchiffre la clé de session. À partir de ce moment, le client et le serveur partagent une clé secrète commune qui va servir à la communication ultérieure.
2. Authentification du client. Elle peut se faire de plusieurs manières :
   — par mot de passe,
   — par défi-réponse.

Question 1. Expliquez en quoi le type de chiffrement utilisé pour protéger les communications est un chiffrement à clé secrète et non un chiffrement à clé publique. Expliquez ce choix.

Question 2. En supposant que toutes les communications de l'étape « établissement d'un canal confidentiel » sont authentifiées, expliquez pourquoi toutes les communications suivantes sont authentifiées et confidentielles.

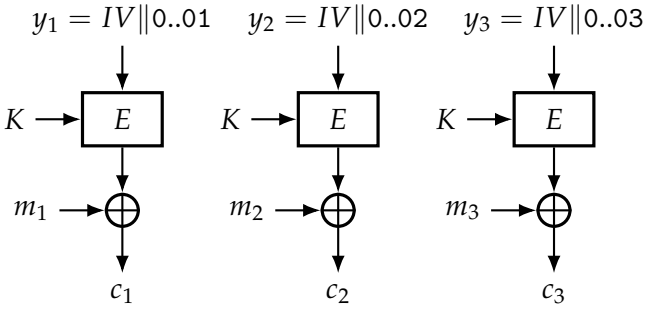
Question 3. Si la première connexion à un serveur n'est pas authentifiée, expliquez comment un attaquant actif peut se faire passer pour le serveur et quelles peuvent en être les conséquences.

Question 4. Pourquoi le client doit-il prévenir l'utilisateur en cas de modification de la clé publique du serveur ?

2 Modes et vecteur d'initialisation (5 points)

Nous considérons dans cet exercice un chiffrement par bloc E paramétré par une clé secrète K. Notons n la taille (en bits) des blocs en question.

Nous nous intéressons tout d'abord au cas du mode CTR (*Counter*), dont nous rappelons ici la définition. Étant donné un vecteur d'initialisation IV de $n - 64$ bits, nous notons $y_i = IV \| i$, pour tout $0 < i < 2^{64}$, la concaténation de cet IV avec l'entier i, représenté sur 64 bits. Le chiffrement de m_i, le $i^{\text{ème}}$ bloc du message en clair, est alors donné par la formule $c_i = m_i \oplus E_K(y_i)$, pour tout $0 < i < 2^{64}$, comme représenté sur le schéma suivant :



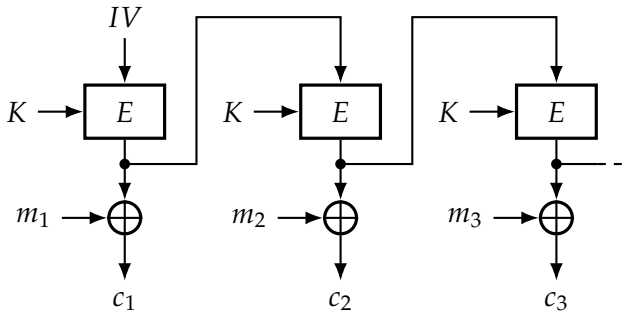
Question 1. Donnez le schéma de déchiffrement, ainsi que la formule correspondante pour calculer chaque bloc m_i en fonction de la clé K, du vecteur d'initialisation IV et du bloc chiffré c_i.

Question 2. Expliquez en quoi le mode CTR se rapproche d'un chiffrement par flot. De quels paramètres dépend le masque appliqué au message ?

Supposons alors qu'un·e utilisateur·trice décide d'utiliser toujours le même vecteur d'initialisation IV pour chiffrer plusieurs messages. Supposons de surcroît que vous, l'attaquant·e, disposiez d'un couple clair / chiffré (M, C) ; on parle alors d'attaque à *clair connu*.

Question 3. Pouvez-vous utiliser la connaissance de M et C afin de décrypter (sans connaître la clé, bien sûr) d'autres messages chiffrés avec la même clé K et le même vecteur d'initialisation IV ? Si oui, comment faites-vous ?

Considérons alors le mode OFB (*Output Feedback*) suivant :



Question 4. Donnez la formule de chiffrement, ainsi que la formule et le schéma de déchiffrement de ce mode.

Question 5. Est-ce qu'une attaque à clair connu est possible sur le mode OFB si un même vecteur d'initialisation IV est utilisé pour tous les messages ?

3 Double DES (10 points)

Considérons un mécanisme de chiffrement par bloc E paramétré par une clé de ℓ bits. On suppose que l'attaquant dispose d'un bloc en clair m et du bloc chiffré correspondant $c = E_k(m)$, et qu'il souhaite retrouver la clé secrète k.
Si l'on suppose de plus qu'il n'existe pas de faiblesse structurelle spécifique au chiffrement E, la seule attaque possible est la *force brute* qui consiste à tester toutes les clés possibles (c'est-à-dire l'ensemble des mots de ℓ bits) jusqu'à retrouver k, qui vérifiera bien l'équation $c = E_k(m)$.

Dans cet exercice, nous prendrons le cas de $E = \text{DES}$, pour lequel nous avons $\ell = 56$ bits.

Question 1. Quelle taille fait l'ensemble des clés possibles ? Quel est le coût de l'attaque ?

Question 2. En supposant qu'un ordinateur actuel soit capable d'effectuer un milliard d'essais par seconde, donnez l'ordre de grandeur du temps que prendrait cette attaque sur un tel ordinateur. Même question sur 10, puis 100 ordinateurs. Concluez sur la sécurité de DES.
Astuce : pour rappel, $10^3 \approx 2^{10}$, et une année contient environ 2^{25} secondes.

Afin d'augmenter la sécurité de DES, on propose d'utiliser *Double-DES* (ou 2DES), qui utilise des clés de taille double (112 bits, donc). Dans 2DES, une clé est ainsi la concaténation $k_1 \| k_2$ de deux clés k_1 et k_2 de 56 bits chacune. Le chiffrement d'un bloc en clair m est alors défini comme

$$c = \text{2DES}_{k_1\|k_2}(m) = \text{DES}_{k_2}(\text{DES}_{k_1}(m)),$$

c'est-à-dire que m est d'abord chiffré par DES avec la clé k_1, puis le résultat est alors chiffré par DES avec la clé k_2.

Question 3. Comment s'effectue le déchiffrement (lorsque l'on connaît la clé) ?
Remarque : vous pourrez noter DES_x^{-1} le déchiffrement DES avec la clé x.

Question 4. Quel est le coût d'une attaque par force brute sur 2DES ? Concluez sur la faisabilité d'une telle attaque.

Il est cependant possible de faire mieux : l'attaque *meet-in-the-middle*. Celle-ci repose sur l'observation suivante :

Question 5. Étant donnés deux blocs m et $c = \text{2DES}_{k_1\|k_2}(m)$, montrez qu'il existe deux clés x et y de 56 bits chacune telles que $\text{DES}_y^{-1}(c) = \text{DES}_x(m)$. Quelles sont les valeurs de x et y ?

Cette attaque requiert que, dans un premier temps, l'attaquant·e précalcule et stocke dans une grande table l'ensemble des couples $(\text{DES}_x(m), x)$, pour tout x dans l'ensemble des clés DES possibles, c'est-à-dire dans l'ensemble des mots de 56 bits.

Question 6. Combien coûte ce précalcul ? Sachant de plus qu'un bloc DES fait 64 bits, quel volume de stockage est nécessaire pour représenter cette table ? Est-ce complètement hors de portée ?

Il suffit alors à l'attaquant·e de retrouver, par force brute, la clé y pour laquelle le bloc $\text{DES}_y^{-1}(c)$ est présent dans la table.

Question 7. Comment finir l'attaque et retrouver la clé $k_1 \| k_2$?

Question 8. Concluez sur le coût total de l'attaque *meet-in-the-middle* et sur sa faisabilité.

En fait, plutôt que Double-DES, on propose d'utiliser *Triple-DES* (ou 3DES), qui fonctionne avec trois clés de 56 bits :

$$c = \text{3DES}_{k_1\|k_2\|k_3}(m) = \text{DES}_{k_3}(\text{DES}_{k_2}^{-1}(\text{DES}_{k_1}(m)))$$

Question 9. Quel est le coût d'une attaque *meet-in-the-middle* sur 3DES ? Peut-on utiliser 3DES dans la pratique ?