TD Cryptographie

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 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. On suppose pour cela que chaque étudiant a stocké la clef publique du professeur. Si nécessaire, on pourra supposer que le professeur dispose au départ de toutes les clés 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.*

2 Authentification et signatures

Nous avions vu en cours deux approches pour assurer l'intégrité d'un message m envoyé de A à B, selon qu'on dispose d'un secret partagé, ou d'un couple de clés asymétriques :

1. Message Authentication Code (MAC) : A envoie $\{m; H(m + s)\}$, où s est un nombre secret connu par A et B ;

2. Digital signature (DS) : A envoie $\{m; \{H(m)\}_{Kd(A)}\}$, où $Kd(A)$ est la clé privée de A.

La fonction $H(.)$ est, une fonction de hachage cryptographique connue universellement.

Questions (veuillez donner une brève explication de 1-3 phrases) ;

Question 5 *Pour le cas MAC, pourquoi est-il insuffisant que A envoie simplement* $\{m; H(m)\}$ *?*

Question 6 *Pour le cas DS, A pourrait-elle aussi envoyer* $\{m; \{H(m)\}_{Ke(A)}\}$ *pour assurer l'intégrité ?*

Question 7 *Lors d'une dispute juridique, B veut prouver à un tiers (p.ex., un tribunal) que A est l'auteur d'un document donné (p.ex., un contrat). Avec DS, comment B peut-il le prouver ?*

Question 8 *Même question avec MAC.*