Université de Sherbrooke - Département d'informatique
IFT606 – Sécurité et Cryptographie
Dave Touchette, professeur

Devoir 3
Date de remise : Dimanche 26 février à 23h59

Effectuez ce devoir en équipe de 3 ou 4 personnes. Utilisez TurninWeb, le système de soumission de travaux du Département d'informatique, pour soumettre votre travail. Soumettez un seul fichier pdf.

Contexte

Nous voulons qu'Alice et Bob puissent communiquer de façon sécurisée, disons Alice veut envoyer un message m à Bob de sorte à ce que la transmission de m soit faite de manière confidentielle, intègre et authentifié.
Ils communiquent sur un réseau non-sécurisé, et donc, en particulier, il est possible qu'un adversaire puisse:

- lire toutes les communications transmises,
- modifier les communications,
- tenter de se faire passer pour Alice.

Ils veulent utiliser les systèmes cryptographiques suivants :

- $\Pi_{CPriv} = (Gen_{CPriv}, E_{CPriv}, D_{CPriv})$, un système de chiffrement à clés privées sécuritaire,
- $\Pi_{MAC} = (Gen_{MAC}, MAC, Verif_{MAC})$, un système d'authentification à clés privées sécuritaire,
- $\Pi_{CPub} = (Gen_{CPub}, E_{CPub}, D_{CPub})$, un système de chiffrement à clés publiques sécuritaire,
- $\Pi_{Sign} = (Gen_{Sign}, Sign, Verif_{Sign})$, un système de signatures digitales sécuritaire,
- $\Pi_{KE} = (\Pi_A^i, \Pi_B^i)$, un système d'échange de clés interactif sécuritaire.

Alice et Bob ont tous deux confiance en Charlie pour émettre des certificats de confiance, et Alice et Bob connaissent tous deux la clé public pk_C de Charlie. Alice a reçu un certificat $cert_{C\to A}$ de Charlie et Bob a reçu un certificat $cert_{C\to B}$ de Charlie.

1. **Protocole ''handshake''**

En utilisant les systèmes cryptographiques $\Pi_{CPriv}, \Pi_{MAC}, \Pi_{CPub}, \Pi_{Sign}, \Pi_{KE}$ ainsi que les certificats $cert_{C\to A}$ et $cert_{C\to B}$ et la clé publique de Charlie pk_C, donner le pseudo-code d'un protocole qui permet à Alice et Bob d'établir une clé privée partagée k avec les propriétés suivantes:

- robuste: si les messages transmis de Alice vers Bob et de Bob vers Alice ne sont pas modifiés lors de leur transmission, Alice et Bob n'abandonnent pas le protocole et produisent tous les deux la même clé k en sortie de protocole,
- secret: seulement Alice et Bob peuvent calculer de l'information sur k à la fin du protocole,
- intègre: si Alice et Bob n'abandonnent pas le protocole, ils produisent tous les deux la même clé k,
- authentifié: Alice peut être certaine que c'est bien Bob qui a communiqué avec elle pour établir cette clé, et vice-versa.

-Argumenter pourquoi votre protocole satisfait ces propriétés.
-Que contiennent $cert_{C\to A}$ et $cert_{C\to B}$?
-Comment a été générée pk_C ?

2. **Protocol ‘’record layer’’**

Vous pouvez maintenant supposer qu'Alice et Bob partagent une clé privée k qui est secrète, intègre et authentifié.
Si vous désirez faire des suppositions sur k, prière de les noter ici.
On souhaite un protocole qui permet à Alice d'envoyer le message m à Bob avec les propriétés suivantes:

- robuste: si les messages transmis de Alice vers Bob et de Bob vers Alice ne sont pas modifiés lors de leur transmission, Alice et Bob n'abandonnent pas le protocole et Bob produit bien le message m qu'Alice lui envoyait en sortie de protocole,
- confidentialité: seulement Alice et Bob peuvent calculer de l'information sur m à la fin du protocole,
- intègre: si Alice et Bob n'abandonnent pas le protocole, Bob produit bien le message m d'Alice en sortie,
- authentifié: Bob peut être certain que m provient bien d'Alice.

Argumenter en un court paragraphe comment utiliser une telle clé secrète k pour transmettre un message m d’Alice vers Bob. Vous pouvez donner une description très haut niveau de ce qui a déjà été fait au devoir 1.