8INF135: SÉCURITÉ DES RÉSEAUX ET DU WEB

TP1 : Authentification des messages et tiers de confiance
Travail en équipe de 2 ou 3
À remettre le vendredi 2 novembre 2018 à 18h

1.Objectifs

- Comprendre et assimiler les différents concepts de la cryptographie symétrique:
  - Les algorithmes de chiffrement et de déchiffrement par bloc;
  - Les modes d'opération lors du chiffrement par bloc;
- Comprendre et assimiler la base de l'authentification de message:
  - Fonction de hachage;
  - Code MAC;
- Se rappeler des notions de programmation d'application client-serveur.
- Comprendre les problématiques reliées aux tiers de confiance et à la distribution de clés.

2. Mise en contexte

Paranoïaque de nature, Bernard ne fait pas confiance aux infrastructures de sécurité utilisées sur l'internet. Or, il doit recevoir d'importants messages d'Agnès tout en étant certain que les messages viennent bien d'elle. En terme de communication Internet, il ne fait confiance qu'à Clément. Bernard vous demande de l'aider à sécuriser ces communications entre lui et Agnès en utilisant Clément.

Ces besoins sont les suivants:

- Agnès et Bernard ne se connaissent pas. À priori, ils ne peuvent pas se faire confiance;
- Agnès et Bernard connaissent tous deux Clément, avec qui ils partagent chacun une clé privée différente pour chacun;
- Lorsque Bernard reçoit un message d'Agnès, il doit être certain que le message provient bien d'Agnès;
- Pour son application, Bernard n'a besoin que d'Intégrité. La confidentialité est secondaire.
- La performance n'est pas nécessaire.

Il vous demande de lui programmer **en C++** les différents outils dont il aura besoin pour sa communication.

3. Travail à effectuer

Pour le travail, vous aurez à implémenter et à utiliser les différents outils permettant à Bernard de recevoir des informations d'Agnès:

Algorithme de chiffrement symétrique:

- Implémenter un algorithme de chiffrement par bloc (Algorithme de Vigenère au minimum).
- Utiliser un mode d'opération du chiffrement (CBC ou CTR).
- Une taille de clé d'au moins quatre caractères;
- Le message est de taille variable (au moins de la taille de clé).

Authentification des messages:

- Programmer Algorithme d'authentification des messages:
- Algorithme MAC au choix;
- Mettre en place une fonction de hachage simple;

Fonctionnalité Client/serveur:

- Être en mesure de faire des échanges de message texte entre un client (Agnès ou Bernard) et un serveur (Bernard ou Clément).

Application:

- Comment Bernard peut-il authentifier Agnès de façon sécuritaire?
- Utiliser les outils implémentés pour mettre en place les fonctionnalités, dont Bernard, à besoin:
    - Trois processus (Agnès, Bernard et Clément);
    - Une interface utilisateur minimale pour chaque processus (Interface Console);
    - Les processus doivent afficher les traces des communications:
        - Les messages reçus et envoyés;
        - Les entrées et sorties résultats des algorithmes;

Bonus:

- Intégrer la génération aléatoirement des clés de chiffrement (1 point);
- Assurer la confidentialité du message (une clé différente doit être utilisée) (2 points);
- Implémenter un algorithme de chiffrement utilisant un réseau de Feistel (4 points);

Note:

- Je vous suggère fortement de travail vos messages en base64. Vous pouvez facilement trouver du code sur Internet pour faire la conversion.
- Si vous utilisez du code fourni sur Internet, assurez-vous de bien indiquer la provenance et l'auteur, autrement, il s'agit de plagiat.

4. Livrables

Vous devez me faire parvenir via Moodle les éléments suivants:

- Un document texte contenant :
    - Une page de garde contenant vos noms, prénoms et codes permanents;
    - Un schéma expliquant le fonctionnement de vos communications entre Agnès, Bernard et Clément.
    - Les particularités de votre devoir (compilation, initialisation des composantes, utilisation de l'interface, les algorithmes particuliers, etc.);
- Le code source documenté et lisible. **N'envoyez que les fichiers .h et .cpp.**

Barème de correction	
Algorithme de chiffrement symétrique **Réseau de Feistel** **Mode d'opération**	/4
Authentification des messages **Fonction de Hachage** **Algorithme MAC**	/4
Fonctionnalité Client/serveur	/2
Application **Schéma de fonctionnement** **Interface utilisateur et affichage** **Fonctionnement général**	/10
Lisibilité et documentation	/-2
Bonus	/7
Total	/20
Commentaires	