UNIVERSITÉ DE SHERBROOKE

DÉPARTEMENT D'INFORMATIQUE

IFT 606

Devoir 1 — Hiver 2018

Cryptographie et sécurité

19 février 2018

Remise du devoir

— Le devoir est à remettre le 12 mars 2017 à l'adresse suivante : mohammed.ouenzar@gmail.com.

— La qualité du français et celle des références scientifiques sont évaluées.

— L'implémentation des tests fonctionnels donnera des points bonus.

— Les programmes développés devraient être accompagnés d'un fichier *readme.txt* expliquant leur l'utilisation.

Wi-Fi (*7pts*)

L'évolution de la sécurité des réseaux sans-fil est liée principalement aux algorithmes de chiffrement utilisés lors de la connexion d'un utilisateur. L'article *A Survey of Wireless Security* résume l'évolution de la sécurité dans les réseaux de ce type.

1. En lisant l'article, expliquer **en détail** le fonctionnement de chacun des trois algorithmes (*3,5pts*).
2. En lisant l'article, expliquer **en détail** les points faibles (attaques possibles) des implémentations des trois algorithmes (*3,5pts*).
3. (optionnelle-points-bonus) En utilisant la suite *Aircrack-ng*, essayez de trouver le mot de passe qui vous permettra d'accéder au réseau *Dinf-ift606-tpxa* [1] (expliquer étape par étape le fonctionnement des commandes) (*2pts*)*)*.

Chiffrement et signature (*7pts*)

L'utilisation de la boite à outils *OpenSSL* est recommandée pour répondre aux questions suivantes.

1. Générer une paire de clés RSA d'une taille de 2048 bits protégée par un mot de passe (*1pts*).
2. Créez un fichier ne contenant que la partie publique de votre clé RSA (*1pts*).
3. Chiffrer la partie privée générée à l'aide de l'algorithme *des3* (*1pts*).
4. Assumons que votre partenaire a une clé publique que vous pouvez échanger (*2pts*).
   — Chiffrer à un fichier contenant le message suivant : "OpenSSL is really cool!!!" et envoyez lui le cryptogramme obtenu.
   — Déchiffrer le fichier reçu et vérifier que résultat correspond au message chiffré.
5. Signer le fichier et vérifier la signature (*2pts*).

[1] . le réseau Dinf-ift606-tpxa est détectable au sous-sol du département d'informatique.

RSA (*10pts*)

1. En utilisant python, implémenter l'algorithme *RSA*. Votre programme devra proposer trois fonctionnalités :
   — generer_cles() : cle_privee, cle_public
   — chiffrer(cle_public,message) : message_chiffré
   — dechiffrer(message _chiffré) : message

Diffie-Hellman (DH) (*6pts*)

En lisant l'article *Diffie-Hellman Key Exchange : A Non-mathematician's explanation*, donner une explication détaillée du fonctionnement de l'algorithme DH.