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

**Devoir 2**
**Date de remise : Jeudi 9 février à 23h59**

Effectuez ce devoir en équipe de 3 ou 4 personnes. Utilisez TurninWeb pour soumettre votre travail. Soumettez un seul fichier pdf, contenant le code source nécessaire comme texte dans le corps de votre devoir.

## 1. **Échange de clé à la Diffie-Hellman**

Vous allez implémenter une version allégée du protocole d'échange de clé interactif de Diffie-Hellman.

Soit le protocole suivant:

1- Alice pige un nombre aléatoire x $\in_R [2^{32}] = \{1,2,\dots,2^{32}-1,2^{32}\}$ de 32 bits, calcule $h_A = 3^x \bmod 2^{63}$, et envoie $h_A$ à Bob.
2- Bob pige un nombre aléatoire $y \in_R [2^{32}]$ de 32 bits, calcule $h_B = 3^y \bmod 2^{63}$, et envoie $h_B$ à Alice.
3- Alice, après réception de $h_B$, output la clé $k_A = h_B^x \bmod 2^{63}$.
4- Bob, après réception de $h_A$, output la clé $k_B = h_A^y \bmod 2^{63}$.

Les parties 1 et 3 du protocole correspondent au code de Alice, et les parties 2 et 4 au code de Bob.

Écrivez le code pour ces 4 algorithmes en langage C, python ou Java. N'oubliez pas de vous assurer que votre protocole soit calculatoirement efficace.. en particulier, rappelez-vous comment performer l'exponentiation modulaire efficacement !

Dans ce qui suit, une personne jouera Alice, une jouera Bob, et une Eve.

(a) Essayer de rouler le protocole ici-haut entre Alice et Bob avec les messages passant entre les mains de Eve, qui peut voir les messages mais ne les modifie pas. Essayer ensuite de le rouler avec Eve qui agit comme un homme-dans-le-milieu, comme pour l'attaque vue en cours contre le protocole de Diffie-Hellman. Donner les traces de l'exécution pour chacun des cas : quelles sont les ''transcripts'' et ''outputs'' locaux des trois participantes et participants, Alice, Bob et Eve ?

(b) Du point de vue d'Alice et de Bob, si ils ne peuvent pas communiquer directement, est-ce qu'il y a une différence entre leurs vues locales dans ces 2 cas ?

(c) Si vous comparer maintenant les outputs $k_A$ et $k_B$ d'Alice et de Bob, respectivement, est-ce que $k_A = k_B$ dans les deux cas ?

(d) Dans la notation des notes de cours (voir révision IKE), quelles sont les $\Pi_A^i$, $\Pi_B^i$ ?

2. **Hypothèse RSA**

Soit la sortie (143, 11, 13) d'un algorithme GenModulus(1111) pour RSA.

(a) Quels sont N, p et q ici ?
(b) Quel est ϕ(N), la taille de $Z_{143}^*$ ?
(c) Si on prend e = 7 comme exposant RSA, quelle serait l'exposant inverse d correspondant que l'algorithme GenRSA(1111) produirait en sortie ?
(d) Pour un schéma de chiffrement public ''textbook'' RSA, quelles seraient les clés publiques et secrètes, pk et sk, correspondantes ? Et similairement pour un schéma de signature digitale ''textbook'' RSA ?

3. **Signatures ''textbook'' RSA**

Soit $\Pi_{sign-t-RSA}$ = (Gen2, Sign2, Verif2), le schéma de signature digitale ''textbook'' RSA (vous pouvez supposer pour les besoins du devoir que N est au plus 8 ou 16 bits, et que les messages sont valides).

(a) Écrivez le code pour les deux algorithmes Sign2 et Verif2, en langage C, python ou Java.

Dans ce qui suit, une personne jouera Alice, une jouera Bob, et une Eve.

(b) En supposant que Alice produit la sortie de Gen2 tel que à la question 2 et distribue publiquement pk, répétez le scénario suivant trois fois, une fois chacune pour chacun des messages suivants : m = 3, m = 5, m = 7. Alice génère la signature σ = E1(pk, m), et envoie (m, σ) à Alice en passant par Eve, qui peut modifier les messages; elle modifiera le message de la troisième exécution mais pas celle des deux premières. Bob reçoit (m, σ) et produit un bit de vérification v. Donner les traces de chacune des trois exécutions : quelles sont m, sk et σ du côté d'Alice, m, pk et σ du côté de Eve, et m, pk, σ et v du côté de Bob.
(c) Si Eve veut maintenant envoyer un message $m_e$ de son choix à Bob, est-ce qu'elle pourra réussir avec une bonne probabilité de succès ? Justifiez votre réponse.