Université de Sherbrooke - Département d'informatique
IFT814 – Cryptographie
Dave Touchette, professeur

**Devoir 2**
**Date de remise : Mercredi 11 octobre à 23h59**

Effectuez ce devoir en équipe d'au plus 4 personnes. Soumettez un seul fichier pdf, contenant le code source nécessaire comme texte dans le corps de votre devoir.

## 1. **MAC insécure**

Soit $\Pi_{MAC}$ = (Gen, MAC, Verif), le schéma MAC suivant, pour messages de longueur 32 bits. Gen génère 32 bits de clé k pigés uniformément au hasard. MAC génère le tag suivant : MAC(k,m) = m $\oplus$ $k$. L'algorithme de vérification compare le tag reçu avec celui correspondant au message reçu et la clé privée k, et dit si oui (1) ou non (0) ils sont égaux.

Écrivez le code pour les trois algorithmes Gen, MAC et Verif, en langage C, python ou Java.

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

(a) Répéter le scénario suivant trois fois de manière indépendante. Alice et Bob génèrent secrètement une clé k. Pour les messages $m_1 = 0^{32}, m_2 = 1^{32}, m_3 = 0^{16}1^{16}$, Alice génère le tag $t_i$ correspondant et envoie la paire $(m_i, t_i)$ à Bob en passant par Eve, qui peut modifier les messages. Bob reçoit et produit un bit de vérification $v_i$. Donner les traces de chacune des trois exécutions : quelles sont m, k et t du côté d'Alice, m et t du côté de Eve, et m, k, t et v du côté de Bob.

(b) Pour chacune de ces trois exécutions, est-ce que Eve peut réussir avec bonne probabilité à envoyer un message modifié à Bob tout en faisant accepter le test de vérification à Bob ? Et à la fin de chacune de ces répétitions, 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 vos réponses

(c) Soit la fonction $F: \{0,1\}^n \, x \, \{0,1\}^n \rightarrow \{0,1\}^n$, $F(k,x) = f_k(x) = x \oplus$ k. Est-ce que $F(k,.)$ est pseudo-aléatoire ? Justifiez votre réponse.

## 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 $\phi$(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 ?