Université de Sherbrooke - Département d'informatique
IFT814 – Cryptographie
Martin Fiset, chargé de cours

**Devoir 2**
**Date de remise : Vendredi 10 octobre à 23h59**

Soumettez un seul fichier pdf, contenant le code source nécessaire comme texte dans le corps de votre devoir. Ce devoir compte pour 12% de la note finale.

---

## 1. Analyse d'un MAC Défaillant

Soit $\Pi_{MAC}$ = (Gen, MAC, Verif), le schéma MAC suivant, pour messages de longueur 64 bits.

**Gen** génère une clé k de 64 bits choisis uniformément au hasard. **MAC** génère le tag suivant : MAC(k, m) = $(m \oplus k) \bmod 2^{32}$, où le résultat est tronqué à 32 bits. L'**algorithme de vérification** compare le tag reçu avec celui correspondant au message reçu et la clé privée k, et retourne 1 (accepté) ou 0 (rejeté).

Implémentez les trois algorithmes Gen, Mac et Vérif en langage C, Python, Java ou le langage de votre choix.

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

(a) Répétez le scénario suivant quatre fois de manière indépendante. Alice et Bob génèrent secrètement une clé k. Pour les messages $m_1 = 0^{64}$, $m_2 = 2^{64-1}$(le bit de poids fort à 1, les autres à 0), $m_3 = 0^{32}1^{32}$, $m_4$= alternance de 101010…10, Alice génère le tag $t_i$ Correspondant et envoie la paire ($m_i$, $t_i$) à Bob en passant par Eve, qui peut observer et modifier les messages. Bob reçoit et produit un bit de vérification $v_i$.

Donnez les traces de chacune des quatre exécutions : quelles sont m, k et t du côté d'Alice, m et t observés par Eve, et m, k, t et v du côté de Bob.

(b) Pour chacune de ces quatre exécutions, analysez si Eve peut réussir avec une bonne probabilité à :

- Modifier un message en transit tout en préservant la validité du Tag ;
- Après avoir observé plusieurs paires ($m_i$, $t_i$), forger un nouveau message $m_e$ de son choix avec un tag valide

Justifiez mathématiquement vos réponses en expliquant les failles exploitables.

(c) Considérez maintenant la fonction $F : \{0,1\}^n \; x \; \{0,1\}^n \; \rightarrow \{0,1\}^{n-16}$, $F(k,x) = f_k(x) = (x \oplus k) \bmod 2^{n-16}$. Démontrez formellement si $F(k,.)$ constitue une famille de fonctions pseudo-aléatoires ou non. Si elle n'est pas pseudo-aléatoire, construisez un distingueur* efficace.

*Distingueur : Il s'agit d'un algorithme réel, comme le chiffrement avec une clé secrète ou un système idéal comme un oracle (voir notre définition dans le glossaire à la fin des présentations PowerPoint).

---

2. **Cryptosystème RSA et extensions**

Soit la sortie (221, 13, 17) d'un algorithme GenModulus(2048) pour RSA.

(a) Identifiez N, p et q. Vérifiez que p et q sont effectivement premiers

(b) Calculez $\varphi(N)$, la taille du groupe multiplicatif $Z^*_{221}$

(c) Si on choisit e= 11 comme exposant de chiffrement RSA :

- Vérifiez que PGCD(e, $\varphi(N)$) = 1
- Calculez l'exposant de déchiffrement d correspondant que RenRSA(2048) produirait
- Montrez vos calculs utilisant l'algorithme d'Euclide étendu

(d) Pour les schémas suivants, donnez les clés publiques et privées (pk, sk) :

- Chiffrement RSA « texbook »
- Signature RSA « textbook »
- Chiffrement RSA-OAEP (Optimal Asymmetrical Encryption Padding (PKCS#1) et décrivez conceptuellement les différences avec « textbook »

(e) Analyse de sécurité ;

- Si un adversaire intercepte un message chiffré $c = m^e \bmod N$, et connaît que le message original m appartient à un ensemble de 1000 messages possibles, décrivez une attaque par dictionnaire efficace.
- Proposez une contre-mesure pour prévenir cette attaque

(f) Extension au cas multi-premier

- Supposez que N = p*q*r ou p, q et r sont trois nombre premiers distincts
- Exprimez $\varphi(N)$ en fonction de p, q et r
- Si p= 7, q= 11 et r =13, Calculez N et $\varphi(N)$
- Commentez les implications sur la sécurité comparée au RSA standard à deux facteurs.

---

**Notes importantes**

- Assurez-vous que votre code est bien commenté et lisible pour la question 1
- Incluez des exemples d'exécution pour chaque algorithme
- Discutez des limites de vos implémentations et des améliorations possibles