Université de Sherbrooke - Département d'informatique
IFT814 – Cryptographie

Devoir 1
Date de remise : Mercredi 27 septembre 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.

Vous allez implémenter et étudier trois schémas de chiffrement (à longueur fixe) et les utiliser pour transmettre le message suivant :

m = ''ceciestlemessageclairadechiffrer''.

C'est donc un message de longueur 32 sur un alphabet de 26 symboles possibles, a-z.

1. **Chiffre de César**

Soit Π_{Cesar1} = (Gen1, E1, D1), le schéma de chiffrement de César (avec décalage variable selon la clé k) pour messages de longueur 32 sur alphabet a-z de 26 symboles.
Écrivez le code pour les trois algorithmes Gen1, E1 et D1, en langage C, Java ou Python.

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 le message m ici-haut, Alice génère le cryptogramme c = E1(k,m), et envoie c à Bob en passant par Eve (qui ne modifie pas le cryptogramme c). Bob déchiffre c pour obtenir le message m. Donner les traces de chacune des trois exécutions : quelles sont m, k et c du côté d'Alice, c du côté de Eve, et c, k et m du côté de Bob.

(b) Pour chacune de ces trois exécutions, est-ce que Eve peut déchiffrer le message m avec l'information qu'elle voit ? Si oui, comment, et si non, pourquoi.

2. **Masque jetable**

Soit Π_{OTP} = (Gen2, E2, D2), le schéma de chiffrement masque jetable pour messages de longueur 32*16 = 512 bits, sur alphabet {0,1} de 2 symboles.
Écrivez le code pour les trois algorithmes Gen2, E2 et D2 en langage C, Java ou Python.
Montrer comment utiliser ce schéma de chiffrement pour transmettre le message m ici-haut.
La méthode de conversion utilisée entre l'alphabet a-z vers des bits est laissée à votre discrétion.

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 le message m ici-haut, Alice génère le cryptogramme c, et envoie c à Bob en passant par Eve (qui ne modifie pas le cryptogramme c). Bob déchiffre c pour obtenir le

message m. Donner les traces de chacune des trois exécutions : quelles sont m (sur alphabet a-z ainsi qu'en bits), k et c du côté d'Alice, c du côté de Eve, et c, k et m du côté de Bob.

(b) Pour chacune de ces trois exécutions, est-ce que Eve peut déchiffrer le message m avec l'information qu'elle voit ? Si oui, comment, et si non, pourquoi.

3. **Chiffre de César modifié**

Soit Π_{Cesar3} = (Gen3, E3, D3), une variation sur le schéma de chiffrement de César pour messages de longueur 32 sur alphabet a-z de 26 symboles. La modification est la suivante : plutôt que de générer une clé k de longueur 1, l'algorithme de génération de clé Gen3 génère une clé k de longueur 32 pigée uniformément au hasard (ou suffisamment près selon ce qui est facilement faisable dans le langage utilisé !) parmi toutes les clés de cette longueur sur alphabet a-z de 26 symboles. Les algorithmes E3 et D3 fonctionne ensuite comme pour un chiffrement de César de longueur 1 pour chacun des symboles du message m et de la clé k, respectivement.
Écrivez le code pour les trois algorithmes Gen3, E3 et D3 en langage C, Java ou Python.

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 le message m ici-haut, Alice génère le cryptogramme c, et envoie c à Bob en passant par Eve (qui ne modifie pas le cryptogramme c). Bob déchiffre c pour obtenir le message m. Donner les traces de chacune des trois exécutions : quelles sont m, k et c du côté d'Alice, c du côté de Eve, et c, k et m du côté de Bob.

(b) Pour chacune de ces trois exécutions, est-ce que Eve peut déchiffrer le message m avec l'information qu'elle voit ? Si oui, comment, et si non, pourquoi. Comparer la sécurité de ce schéma avec celle des schémas aux questions 1 et 2.

(c) Faites trois nouvelles exécutions, mais maintenant Eve fait un décalage de 9 lettres sur le troisième symbole de c et de 18 lettres sur le quatrième symbole de c dans chacune de ces exécutions. Comparez le message que Bob déchiffre à celui que Alice a envoyé. Que se passe-t-il? Est-ce que Bob détectera quelque chose ?