Université de Sherbrooke - Département d'informatique

IFT814 – Cryptographie

Devoir 1

Date de remise : Vendredi 26 septembre 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.

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 avec double décalage

Soit $\Pi_{César1}$ = (Gen1, E1, D1), le schéma de chiffrement de César avec double décalage pour messages de longueur 32 sur alphabet a-z de 26 symboles.

Principe : Ce schéma utilise deux clés k1 et k2. Les caractères en positions paires (0, 2, 4, ...) sont chiffrés avec k1, et les caractères en positions impaires (1, 3, 5, ...) sont chiffrés avec k2.

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 = (k1, k2). Pour le message m ci-dessus, Alice génère le cryptogramme c = E1(k_n,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_n= (k1, k2) et c du côté d'Alice, c du côté d'Eve, et c, k et m du côté de Bob.

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

---

2. Masque jetable

Soit Π_{OTP} = (Gen2, E2, D2), le schéma de chiffrement masque jetable pour messages de longueur 32*5 = 160 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 ci-dessus. Utilisez un encodage de 5 bits par caractère (a=00000, b=00001, ..., z=11001).

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 ci-dessus, 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 d'Eve, et c, k et m du côté de Bob.

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

---

3. Chiffre de substitution monoalphabétique

Soit Π_{Sub} = (Gen3, E3, D3), le schéma de chiffrement par substitution monoalphabétique pour messages de longueur 32 sur alphabet a-z de 26 symboles.

Principe : La clé k est une permutation complète de l'alphabet (bijection* de {a,b,...,z} vers {a,b,...,z}). Chaque lettre du message est remplacée par sa correspondante selon la permutation.

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 ci-dessus, 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 d'Eve, et c, k et m du côté de Bob.

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

*Bijection : C'est une correspondance un-à-un entre deux ensembles. Pour le chiffre de substitution monoalphabétique. Les propriétés essentielles sont :

injective : chaque lettre en claire correspond à une seule lettre chiffrée

Surjective : Chaque lettre de l'alphabet est utilisée dans le chiffrement

Réversible : On peut toujours retrouver la lettre originale

Questions bonus (20 points supplémentaires)

Bonus 1 : Attaque par analyse de fréquences (10 points)

Eve a intercepté le message chiffré suivant, généré avec un chiffre de substitution monoalphabétique :

c_bonus =
"KQCAWYQVKFVNCQCUKTQVCKQOWBNKLOLZQJTBWYVAZCQTBOQBFZYABKQF"

Ce message a été chiffré à partir d'un texte en français. Utilisez l'analyse de fréquences pour tenter de le déchiffrer.

Fréquences attendues en français (approximatives) :

- E: 12%, A: 9%, I: 8%, S: 7%, N: 7%, R: 6%, T: 6%, O: 5%, L: 5%, U: 4%

(a) Calculez les fréquences des lettres dans le cryptogramme c_bonus.

(b) Proposez une correspondance entre les lettres du cryptogramme et l'alphabet clair en vous basant sur les fréquences.

(c) Déchiffrez le message et vérifiez si le résultat a du sens en français.

(d) Si nécessaire, ajustez votre correspondance et répétez le processus.

Bonus 2 : Analyse comparative de sécurité (10 points)

(a) Classez les trois schémas étudiés (César double décalage, OTP, substitution monoalphabétique) par ordre de sécurité croissant. Justifiez votre réponse.

(b) Pour chaque schéma, calculez la taille de l'espace des clés et évaluez la faisabilité d'une attaque par force brute avec les moyens de calcul actuels.

(c) Discutez des avantages et inconvénients pratiques de chaque schéma (facilité d'implémentation, distribution des clés, résistance aux erreurs de transmission, etc.).

Notes importantes

- Assurez-vous que votre code est bien commenté et lisible
- Incluez des exemples d'exécution pour chaque algorithme
- Pour les questions bonus, documentez clairement votre démarche
- Discutez des limites de vos implémentations et des améliorations possibles