a@

Semestre 2 **Licence 3 en ingénierie Informatique** Cours Sécurité des Réseaux.

TD2 : Algorithmes et Protocoles Cryptographiques

Chiffrement moderne

Exercice 1 : ECB

On considère un cryptosystème ECB qui applique un mode opératoire à des blocs de 4 bits par décalage de deux positions vers la droite de chaque bit du bloc.
La fonction de décalage à droite d'un bit noté $E = x_{i \gg y}$ où le bit x_i est décalé de y positions vers la droite est définie sur un bloc comme suit :
$E(b_0b_1b_2b_3) \rightarrow b_{0\gg 2}\ b_{1\gg 2}\ b_{2\gg 2}\ b_{3\gg 2}$ (Décalage circulaire)
Soit le plaintext ou texte claire M = 11001010111011

1- Sachant que | est l'opérateur de concaténation qui permet de regrouper des bits ou des blocs, décrire mathématiquement ou avec un pseudo-code:
   a. Le chiffrement d'un bit
   b. Le chiffrement d'un bloc
   c. Le fonctionnement de ECB.
2- En partant de la gauche vers la droite, décomposer le texte claire en blocs de taille appropriée. Faire du bourrage avec des zéros pour avoir des blocs de même taille
3- Appliquer le mode ECB sur M et donner le texte chiffré C.
4- Appliquer le déchiffrement et vérifier avec le message original
5- Si on considère un texte clair formé par les mêmes blocs 1110, cette redondance est-elle propagée dans le texte chiffré ?
6- Si l'ordre des blocs du texte chiffré est modifié, le décryptage de chaque bloc sera-t-il possible ?
7- Si M est le salaire de A et M'=11000010111100 le salaire de B. A perçoit son salaire et reçoit C=E(M) et C'=E(M'), peut-il connaitre l'ordre de grandeur du salaire de B.
8- Si le salaire M' de B est 1010111011001, A reçoit C=E(M) et C'=E(M'), peut-il connaitre le salaire de B sachant que les deux messages sont constitués des mêmes blocs dans ordre différent.
9- Si on remplace les bits par des lettres et que chaque quartet de lettre a une fréquence différente selon la langue, comme par exemple « tion » est plus fréquent « rxkt », la fréquence d'apparition des blocs chiffrés peut-il permettre de retrouver le texte claire si on dispose du tableau de fréquence ?
10- Pour un algorithme de chiffrement sûr, chaque bit d'un texte chiffré provient d'une transformation complexe de tous les bits du bloc de texte en clair correspondant et de tous les bits de la clé. Ainsi une erreur d'un bit dans le texte chiffré ou dans la clé utilisée implique qu'en moyenne 50% du texte en clair récupéré sont faux. Si pendant la transmission des données, il y a un 1 bit qui se transforme en 0, à quel pourcentage le texte en clair obtenu par déchiffrement de ce bloc sera correct ?

Exercice 2 : CBC

On considère un cryptosystème CBC qui applique un mode opératoire par permutation de bit sur des blocs de 4 bits. On donne un vecteur d'initialisation IV=1001

La fonction de permutation E est définie sur un bloc comme suit : $E\ (b_1b_2b_3b_4) \rightarrow b_3b_2b_4b_1$.
Soit le plaintext ou texte claire M = 1100101011101 1

1- Sachant que | est l'opérateur de concaténation qui permet de regrouper des bits ou des blocs, décrire mathématiquement ou avec un pseudo-code le fonctionnement de CBC ?
2- En partant de la gauche vers la droite, décomposer le texte claire en blocs de taille appropriée. Faire du bourrage avec des zéros pour avoir des blocs de même taille
3- Appliquer le mode CBC sur M et donner le texte chiffré C.
4- Appliquer le déchiffrement et vérifier avec le message original
5- Si on considère un texte clair formé par les mêmes blocs 1110, cette redondance est-elle propagée dans le texte chiffré ?
6- Si l'ordre des blocs du texte chiffré est modifié, le déchiffrement de chaque bloc sera-t-il possible ?

7- Si M est le salaire de A et M'=11000010111100 le salaire de B. A percoit son salaire et reçoit C=E(M) et C'=E(M'), peut-il connaitre l'ordre de grandeur du salaire de B.
8- Si le salaire de B M'est 1010111011001, A reçoit C=E(M) et C'=E(M'), peut-il connaitre le salaire de B.
9- Si on remplace les bit par des lettre et que chaque quartet de lettre a une fréquence différente selon la langue, comme par exemple « tion » est plus fréquent « rxkt », la fréquence d'apparition des blocs chiffrés peut-il permettre de retrouver le texte claire si on dispose du tableau de fréquence ?
10- Pour un algorithme de chiffrement sûr, chaque bit d'un texte chiffré provient d'une transformation complexe de tous les bits du bloc de texte en clair correspondant et de tous les bits de la clé. Ainsi une erreur d'un bit dans le texte chiffré ou dans la clé utilisée implique qu'en moyenne 50 pour cent du texte en clair récupéré sont faux. Si pendant la transmission des données, il y a un 1 se transforme en 0, a quel pourcentage le texte en clair obtenu par déchiffrement de ce bloc sera correct ?

Protocoles d'échanges

Exercice 3 : échange de clé

Quatre personnes A, B,C et D participent à une tontine, A est le coordonnateur, il se charge de collecter les montants cotisés par B,C et D qu'ils envoient par code via un système de transfert d'argent. A la réception, A procède au tirage et envoie par code via un système de transfert d'argent la somme au gagnant. Les codes transmis sont confidentiels et la provenance des messages échangés doit être vérifiée. Pour se faire, ils utilisent des algorithmes de chiffrements symétriques et asymétriques. Chacun d'eux génère une paire de clés (publique et privé, respectivement KpuA et KprA pour A) et distribue une des clés aux autres. La clé symétrique (KsA pour A) est générée au besoin.
1-Quelle clé est distribuée ?
2-A la fin du mois, A diffuse un message pour demander de verser les cotisations. Proposer une méthode qu'il peut appliquer pour que les autres puissent vérifier que la diffusion est bien évidemment de A.
3- B souhaite envoyer le code confidentiel de son montant déjà transférer à A, quelle clé doit il utiliser ?
4- Après réception de l'ensemble des transferts de B,C et D, A réuni le montant et doit transmettre le code de retrait au gagnant C et attendre un accusé de réception. Il le chiffre alors avec la la clé KsA et l'envoie à C. Ce protocole est il correcte ? Proposer au moins deux solutions alternatives ?

Exercice 4 : Propriétés de sécurité
Soit le protocole de needham-schroeder
Analyser et trouver les propriétés (services ou objectifs de sécurité) que comporte ce protocole.
A ⟶ B : {Na.A}Kb.
B ⟶ A : {Na.Nb}Ka.
A ⟶ B : {Nb}Kb//
2. Analyser les protocoles suivant et dire

- si la donnée s est secrète et
- si A et B s'authentifient mutuellement ou authentifie mutuellement leur message
- si les données échangées sont fraîches

1. A ⟶ B : A,s
2. A ⟶ B : {A,s}Kb, avec Kb publique et Kb-1 est privée
3. A ⟶ B : A, {s} Ka-1
4. A ⟶ B : {A, {s} Ka-1} Kb
5. A :génère un nombre fraîche Na
   A ⟶ B : {A, B, Na} Kb
   B ⟶ A : {A, B, Na, s} Ka.
   A ⟶ B : {A, B, Na} Kab
   B ⟶ A : {A, B, Na, s} Kab