UQAC
Département d'informatique et de mathématique
Université du Québec à Chicoutimi

Travail pratique #1

But du travail pratique

Le but de ce travail pratique est de vous familiariser avec

- Les algorithmes de chiffrement symétriques
- Les algorithmes de chiffrement asymétriques
- La comparaison des algorithmes
- Les signatures numériques

Instructions

- Répondez à toutes les questions le mieux possible.
- Montrez toutes les étapes et calculs.
- Écrivez vos réponses de manière claire.

Partie 1 – Évaluation de l'Encryption AES

Pour cette partie, vous utiliserez l'information suivante :

- Le texte en clair (plaintext) : **`00112233445566778899AABBCCDDEEFF`**
- La clé de ronde initiale **:** **`000102030405060708090A0B0C0D0E0F`**

Vous devez réaliser la ronde initiale et la première itération de l'algorithme AES-128.

N.B : dans les calculs avec les matrices AES, les numéros de lignes et de colonnes débutent à l'index 0

Pour la première itération, l'entrée sera la chaîne **`000102030405060708090A0B0C0D0E0F`** et vous aurez à calculer SubBytes, ShiftRows, ~~MixColumns~~ et AddRoundKey.

1. Opération SubBytes

Pour cette opération, vous utiliserez la S-box suivante :

```
S-box = [
    63, 7C, 77, 7B, F2, 6B, 6F, C5, 30, 01, 67, 2B, FE, D7, AB, 76,
    CA, 82, C9, 7D, FA, 59, 47, F0, AD, D4, A2, AF, 9C, A4, 72, C0,
    B7, FD, 93, 26, 36, 3F, F7, CC, 34, A5, E5, F1, 71, D8, 31, 15,
    04, C7, 23, C3, 18, 96, 05, 9A, 07, 12, 80, E2, EB, 27, B2, 75,
    09, 83, 2C, 1A, 1B, 6E, 5A, A0, 52, 3B, D6, B3, 29, E3, 2F, 84,
    53, D1, 00, ED, 20, FC, B1, 5B, 6A, CB, BE, 39, 4A, 4C, 58, CF,
    D0, EF, AA, FB, 43, 4D, 33, 85, 45, F9, 02, 7F, 50, 3C, 9F, A8,
    51, A3, 40, 8F, 92, 9D, 38, F5, BC, B6, DA, 21, 10, FF, F3, D2,
    CD, 0C, 13, EC, 5F, 97, 44, 17, C4, A7, 7E, 3D, 64, 5D, 19, 73,
    60, 81, 4F, DC, 22, 2A, 90, 88, 46, EE, B8, 14, DE, 5E, 0B, DB,
    E0, 32, 3A, 0A, 49, 06, 24, 5C, C2, D3, AC, 62, 91, 95, E4, 79,
    E7, C8, 37, 6D, 8D, D5, 4E, A9, 6C, 56, F4, EA, 65, 7A, AE, 08,
    BA, 78, 25, 2E, 1C, A6, B4, C6, E8, DD, 74, 1F, 4B, BD, 8B, 8A,
    70, 3E, B5, 66, 48, 03, F6, 0E, 61, 35, 57, B9, 86, C1, 1D, 9E,
    E1, F8, 98, 11, 69, D9, 8E, 94, 9B, 1E, 87, E9, CE, 55, 28, DF,
    8C, A1, 89, 0D, BF, E6, 42, 68, 41, 99, 2D, 0F, B0, 54, BB, 16
]
```

Et l'entrée suivante : **`000102030405060708090A0B0CAA0E3F`**

À titre d'indice, la **première** colonne de votre matrice résultante devrait ressembler à ceci :

```
63
F2
30
FE
```

2. Opération ShiftRows

À cette étape, les octets dans les trois dernières lignes de l'état sont décalés vers la gauche par des décalages différents :

- La première ligne n'est pas décalée.
- La deuxième ligne est décalée vers la gauche d'un octet.
- La troisième ligne est décalée vers la gauche de deux octets.
- La quatrième ligne est décalée vers la gauche de trois octets.

3. Opération MixColumns

L'opération MixColumns est complexe à calculer manuellement; on va donc pas aller jusque-là. On effectue un calcul complexe de multiplication de matrices dans le corps de Galois (GF(2^8)) qui transforme chaque colonne de la matrice d'état (provenant de ShiftRows) à travers une matrice fixe, introduisant une diffusion et assurant une force cryptographique.

Vous pouvez consulter de multiples ressources en ligne pour en apprendre davantage.

https://en.wikipedia.org/wiki/Finite_field_arithmetic

Le résultat après l'opération MixColumns est :

```
6F 4B 45 36
EF CB 60 46
13 38 7D 50
5E 70 5F E9
```

4. Opération AddRoundKey

Effectuez l'opération AddRoundKey avec la clé de ronde **`2B7E151628AED2A6ABF7158809CF4F3C`** pour obtenir la matrice finale

5. Réflexion

Expliquez l'importance des opérations ShiftRows et MixColumns dans l'algorithme AES. Comment contribuent-elles à la sécurité et aux propriétés de diffusion du processus d'encryption ?

Partie 2 – Algorithme RSA

1. Expliquez les principes de base de la cryptographie RSA. Incluez les rôles de la clé publique et de la clé privée, ainsi que la manière dont elles sont générées.
2. Alice veut envoyer un message confidentiel à Bob en utilisant RSA. La clé publique de Bob est (e, N) = (17, 3233), où N est le modulo. Alice chiffre son message M en utilisant la clé publique de Bob. Si son message M est 123, calculez le texte chiffré C.
3. Bob reçoit le texte chiffré C = 2753 d'Alice. En utilisant sa clé privée (d, N) = (2753, 3233), déchiffrez le message pour obtenir le texte en clair d'origine.
4. Alice génère sa paire de clés RSA. Elle choisit deux nombres premiers, p = 61 et q = 53. Calculez les valeurs de N, φ(N) et l'exposant public (e) pour sa paire de clés.
5. Décrivez une application du monde réel ou un cas d'utilisation où la cryptographie RSA est couramment utilisée. Discutez des avantages spécifiques en termes de sécurité fournis par RSA dans ce contexte.

Partie 3 – Analyse et application des signatures numériques

Imaginez une entreprise de développement de logiciels qui crée et distribue un programme antivirus populaire. L'entreprise publie régulièrement des mises à jour logicielles pour faire face aux menaces émergentes et améliorer les capacités du programme. Les utilisateurs peuvent télécharger ces mises à jour depuis le site officiel de l'entreprise.

1. Décrivez comment les signatures numériques peuvent être appliquées pour garantir l'intégrité et l'authenticité des mises à jour logicielles.
2. Discutez du rôle des clés publiques et privées dans ce scénario.
3. Analysez les risques potentiels et les conséquences si les signatures numériques n'étaient pas utilisées pour vérifier l'authenticité et l'intégrité des mises à jour logicielles.
   Considérez l'impact sur la confiance des utilisateurs, la réputation de l'entreprise et la sécurité globale du programme antivirus.

Document à remettre

Vous devrez remettre le document GabaritReponse.docx (en version docx ou PDF) comprenant les réponses aux parties 1, 2 et 3 avec le plus de détails possibles dans vos réponses.

Une réponse sans explications de calculs ou sans détails ne vaut pas de points.

Date de remise

Le vendredi 1er mars 2023 via le Moodle du cours.