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.

Prénom et nom étudiant 1 : Marco Chan Witzel

Prénom et nom étudiant 2 : Godric Bouteloup

Partie 1 – Évaluation de l'Encryption AES

Ronde initiale

Le texte en clair :
00 11 22 33
44 55 66 77
88 99 AA BB
CC DD EE FF

La clé ronde initiale :
00 10 20 31
40 41 50 6E
08 18 12 A1
CC 4F 0D 00

On effectue une opération XOR entre chacune de ces valeurs pour obtenir la matrice résultante. (Exemple à la question 4)
On obtient donc :

00 01 02 02
04 14 36 19
80 81 B8 1A
00 92 E3 FF

1. *Opération SubBytes*

Pour effectuer l'opération SubBytes, on lit, pour chaque octet la position de la valeur à sélectionner dans la S-BOX. En effet, la première valeur d'un octet (les 4 premiers bits) nous indique la ligne et la seconde nous indique la colonne.

En partant de la matrice :

00 01 02 03
04 15 06 F7
08 09 0A 9B
0C AA 0E 3F

La première valeur ("00") correspond à la ligne 0 et à la colonne 0, ce qui nous donne la valeur 63. La deuxième valeur ("01") correspond à la ligne 0 et à la colonne 1, qui est la valeur 7C.

```
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
]
```

En appliquant la même étape pour chaque valeurs, on obtient finalement :

63 7C 77 7B
F2 59 6F 68
30 01 67 14
FE AC AB 75

2. ***Opération ShiftRows***

Comme précisé dans l'énoncé, on décale chaque ligne selon le nombre d'octet donné vers la gauche et on obtient :

63 7C 77 7B
59 6F 68 **F2**
67 14 **30 01**
75 **FE AC AB**

3. ***Opération MixColumns***

Ici le sujet ne nous demande pas de faire cette opérations nous avons donc juste mis le résultat.

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

4. ***Opération AddRoundKey***

Soit les deux matrices suivantes :

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

2B 7E 15 16
28 AE D2 A6
AB F7 15 88
09 CF 4F 3C

On effectue une opération XOR entre chacune de ces valeurs pour obtenir la matrice résultante.
À titre d'exemple, on peut détaillé 6F XOR 2B :
$(6F)_{16} = (0110\ 1111)_2$ et $(2B)_{16} = (0010\ 1011)_2$
-> $(0110\ 1111)_2$ XOR $(0010\ 1011)_2 = (0100\ 0100)_2 = (44)_{16}$

$(4B)_{16}$ XOR $(7E)_{16} = (35)_{16}$
$(45)_{16}$ XOR $(15)_{16} = (50)_{16}$
…
$(E9)_{16}$ XOR $(3C)_{16} = (D5)_{16}$

La matrice résultante est donc :

44 35 50 20
C7 65 B2 E0
B8 CF 68 D8
57 BF 10 D5

5. Réflexion

Ces deux opérations jouent un rôle essentiel dans la sécurité et aux propriétés de diffusion du processus de chiffrement à travers les divers objectifs de chacune d'elles.

En effet, l'opération ShiftRows ajoute de la confusion ainsi que de la complexité au chiffrement en modifiant l'ordre des bits.

L'opération MixColumns, deuxième étape de diffusion, est une opération linéaire qui fait intervenir de multiples bits dans le codage d'un seul rendant ainsi le déchiffrement plus complexe si l'on ne connaît pas la clé.

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.*

La cryptographie RSA pour Rivest-Shamir-Adleman est un algorithme très répandu intervenant dans deux principes, le chiffrement et la signature numérique.
Celui-ci fonctionne à l'aide de deux clés, une publique et une privée, celles-ci sont générées à l'aide de calculs autour de deux nombres premiers.
Les étapes de calculs sont composées de la sélection de deux nombres premiers (généralement grands) puis de leur produit pour créer le module de chiffrement "**n"** (ou module RSA). Par la suite, on calcule la valeur indicatrice d'Euler selon :
$\varphi(n) = (p - 1)(q - 1)$
puis on choisit un entier naturel "**e**" premier avec $\varphi(n)$ et strictement inférieur à $\varphi(n)$ appelé

exposant de chiffrement. Enfin, on calcule "**d**" de par l'inverse modulaire de e pour la multiplication modulo φ(*n*) soit $d \equiv e^{-1} \pmod{\varphi(n)}$.
Ainsi, on obtient la clé publique de par le couple (e,n) et la clé privée : d.

En ce qui concerne le rôle de ces clés, la clé publique permet de chiffrer les données ou de vérifier les signatures tandis que la clé privée permet de déchiffrer les données ou de générer des signatures.

Le chiffrement RSA marche donc avec la clé publique selon $C = M^e \bmod n$ avec M le message et C le message chiffré.
Le déchiffrement fonctionne avec la clé privée, on a $M = C^d \bmod n$.

La signature RSA dépend de la formule suivante $S = M^d \bmod n$.
Enfin, pour vérifier une signature, on regarde si M est égal à $S^e \bmod n$.

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*.

On applique donc la formule expliquée précédemment en simplifiant notre valeur de M^e :
$C = M^e \bmod n$
$C = (123)^{17} \bmod 3233$
C = 123×(123)^16mod3233
C = 123×(123^2)^8mod3233
C = 123×(15129)^8mod3233
C = 123×(2197)^8mod3233
C = 123×(2197^2)^4mod3233
C = 123×(4826809)^4mod3233
C = 123×(3173)^4mod3233
C = 123×(3173^2)^2mod3233
C = 123×(367)^2mod3233
C = 123×134689mod3233
C = 855

Le texte chiffré C de M = 123 est donc C = 855.

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.*

On applique donc la formule du déchiffrement :
$M = C^d \bmod n$.
M = 2753^2753mod3233
M = 2753×(2753^2752)mod3233
M = 2753×(2753^2752)mod3233
M = 2753×((2753^2)^1376)mod3233
M = 2753×(7579009^1376)mod3233
M = 2753×(857^1376)mod3233
M = 2753×((857^2)^688)mod3233
M = 2753×(734449^688)mod3233
M = 2753×(558^688)mod3233
M = 2753×((558^2)^344)mod3233
M = 2753×(996^344)mod3233
M = 2753×((996^2)^172)mod3233
M = 2753×(2718^172)mod3233
M = 2753×((2718^2)^86)mod3233
M = 2753×(119^86)mod3233
M = 2753×((119^2)^43)mod3233
M = 2753×(1229^43)mod3233
M = 2753×1229×(1229^42)mod3233
M = 2753×1229×((1229^2)^21)mod3233
M = 2753×1229×(630^21)mod3233
M = 2753×1229×630×(630^20)mod3233
M = 2753×1229×630×((630^2)^10)mod3233
M = 2753×1229×630×(2474^10)mod3233
M = 2753×1229×630×((2474^2)^5)mod3233
M = 2753×1229×630×(607^5)mod3233
M = 2753×1229×630×607×(607^4)mod3233
M = 2753×1229×630×607×((607^2)^2)mod3233
M = 2753×1229×630×607×(3120^2)mod3233
M = 2753×1229×630×607×3070mod3233
M = 952

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.*

Dans un premier temps on doit choisir deux nombres premiers distincts, *p* et *q*. On calcule ensuite leur produit *N = p * q*, appelé *module de chiffrement. Dans notre situation : N = 61 * 53 = 3233*.

On calcule par la suite le valeur de l'indicatrice d'Euler en n : *φ(n) = (p - 1)(q - 1).*
Qui nous donne *φ(n) = (61 - 1)(53 - 1) = 3120.*

On choisit e, un entier premier tel que e est strictement inférieur à φ(*n*) et premier avec φ(*n*)
e = 3119 car PGCD(3119,3120) = 1 donc premiers entre eux.
De plus, 3119 < 3120
Donc, pour la paire de clés RSA d'Alice :

- Valeur de N : 3233
- Valeur de φ(n) : 3120
- Exposant public e : 3119

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.*

Dans le monde réel, nous pouvons citer diverses utilisations de la cryptographie RSA tel que dans les réseaux privés virtuels (VPN), les navigateurs Web et les services de messageries.
Nous pouvons développer davantage la partie concernant le Web. En effet, lors de la visite d'un site web sécurisé contenant "https://" dans l'url, la connexion à ce site est réalisée à l'aide du protocole SSL/TLS. La cryptographie RSA est utilisée dans ce processus :

- Lors de la connexion d'un client au serveur, celui-ci envoie son certificat SSL/TLS contenant la clé publique. Le client l'utilise pour pouvoir générer une clé de session, celle-ci est ensuite envoyée au serveur qui la déchiffre à l'aide de sa clé privée. Cette clé de session est donc commune et sécurisée.
- Une fois la connexion sécurisée, l'ensemble des données sécurisées entre client et serveur sont chiffrées selon la clé de session. Cela protège des attaques man-in-the-middle (MITM) et garantit l'intégrité des données.

En ce qui concerne les avantages en termes de sécurité, RSA permet la protection de la clé privée qui n'est jamais exposée sur le réseau réduisant le risque de vol puis de déchiffrement de données.
Cette cryptographie offre aussi l'avantage d'avoir une authentification forte ainsi qu'un chiffrement asymétrique.

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.

Les signatures numériques nous assurent à la fois l'authenticité et l'intégrité des mises à jour logicielles.
En effet, si un attaquant modifie le message en cours de route, la signature ne sera pas considérée comme valide lors de la vérification. Voici comment ce processus se déroule :

Étape 1 : Création de la Clé Privée

- L'entreprise crée une clé privée sécurisée pour signer ses mises à jour. Cette clé est utilisée pour générer des signatures numériques uniques pour chaque mise à jour logicielle.

Étape 2 : Calcul de la Signature

Avant de publier la mise à jour, l'entreprise calcule la signature : $s = m^d \bmod N$, où d est la clé privée, m est le message (la mise à jour logicielle), et (e ,N) est la clé publique.

Étape 3 : Publication de la Mise à Jour et de la Signature

L'entreprise publie la mise à jour sur son site officiel, accompagnée de sa signature numérique.

Étape 4 : Vérification par l'Utilisateur

L'utilisateur télécharge la mise à jour et la signature depuis le site officiel de l'entreprise. Ensuite, l'utilisateur vérifie la signature en effectuant le calcul suivant : $m' = s^e \bmod N$. Si m' est égal à m, alors la signature est considérée comme valide. Sinon, cela signifie que le message a été modifié en cours de route.

Garantie d'Intégrité et d'Authenticité

En concluant cette vérification, l'utilisateur peut avoir confiance que la mise à jour téléchargée provient bien de l'entreprise légitime, car la signature numérique correspond à la clé publique connue de l'entreprise.
De plus, l'intégrité de la mise à jour est garantie, car toute altération du message entraînerait une signature incorrecte lors de la vérification.

Ainsi, grâce aux signatures numériques, les utilisateurs peuvent être assurés que les mises à jour logicielles qu'ils téléchargent sont à la fois authentiques (vérifiées par la clé publique de l'entreprise) et intègres (toute modification serait détectée par la vérification de la signature).
Cela renforce la confiance des utilisateurs dans les mises à jour et protège leurs systèmes contre les attaques potentielles.

2. Discutez du rôle des clés publiques et privées dans ce scénario.

Dans ce scénario les deux types de clés jouent des rôles cruciaux dans le processus de sécurité.

La clé privée permet de générer des signatures numériques uniques, étant en possession de l'entreprise uniquement, elle garantit que seule l'entreprise peut générer des signatures.
La clé publique est quant à elle distribuée publiquement par l'entreprise, elle permet aux utilisateurs de vérifier la signature lorsqu'ils téléchargent une mise à jour. Elle déchiffre la

signature, si celui-ci est valide, cela signifie que la signature provient bien de l'entreprise (authenticité).

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.

Si les signatures numériques ne sont pas utilisées pour vérifier l'authenticité et l'intégrité des mises à jour logicielles, un individu malveillant pourrait altérer ces mises à jour en y introduisant des malwares ou des logiciels malveillants.

Si les utilisateurs découvrent que leurs mises à jour ne sont pas sécurisées et qu'elles pourraient être altérées, cela entraînerait une perte de confiance chez les utilisateurs, pouvant même conduire à une désertion des utilisateurs vis-à-vis de l'entreprise. De plus, lorsque des utilisateurs peu confiants en parlent à d'autres, la réputation de l'entreprise serait sérieusement affectée. Les utilisateurs pourraient considérer l'entreprise comme peu fiable, ce qui pourrait impacter ses ventes et sa croissance future.

Cette situation créerait une atmosphère de méfiance généralisée, où les utilisateurs hésiteraient à télécharger les mises à jour par crainte qu'elles ne soient pas authentiques, entraînant ainsi une perte de clients pour l'entreprise.

En conclusion, l'absence d'utilisation de signatures numériques pour vérifier l'authenticité et l'intégrité des mises à jour logicielles présente des risques sérieux pour les utilisateurs, l'entreprise et la sécurité globale des systèmes.
Cela pourrait entraîner des conséquences désastreuses en termes de pertes de données, de réputation, de confiance des utilisateurs et de sécurité des systèmes.