IUT DE COLMAR

R401 – Infrastructure de sécurité

Année 2022-23

TP1 - Chiffrement et PKI

martin baumgaertner

7 juin 2023

Table des matières

1 Chiffrement

1.1 Permutation

1.1.1 Question 1

Le message déchiffré que j'obtiens est `MAITRE CORBEAU SUR UN ARBRE PERCHEX`
Voici ce que j'ai fait pour obtenir ce message :

1. J'ai créé une liste des lettres de l'alphabet, dans l'ordre.
2. J'ai créé une deuxième liste, contenant les nombres 1 à 6.
3. J'ai apparié les lettres et les chiffres des deux listes, dans l'ordre spécifié dans la clé.
4. J'ai utilisé les chiffres pour créer une nouvelle séquence de lettres, en remplaçant chaque lettre du message d'origine par la lettre qui lui correspond dans la nouvelle séquence.
5. J'ai supprimé tous les espaces de la chaîne obtenue.

1.2 Substitution

1.2.1 Question 2

Voici le message que j'ai trouvé `UN SECRET`

1.3 Diffie-Hellman

1.3.1 Question 3

J'ai obtenu `K = 117`

1.4 Chiffrement symétrique AES

1.4.1 Question 5

Voici le résultat que l'on obtient en base64 :

```
U2FsdGVkX1+QhnAugHjdc6bhMEMibXxWGQSE6ZKN56o=,
```

L'option "-nosalt" lors d'une commande openssl permet de ne pas rajouter de valeur aléatoire au code avant son hachage. En effet "salt" rajoute une valeur aléatoire pour renforcer le code/mot de passe.

2 PKI

2.1 Création du Certificat Racine (ou CA) et de sa clé privée.

CA signigie **C**ertificate **A**uthority. C'est une entité qui émet des certificats numériques.

2.2 Lecture du certificat

Ci-dessous, un tableau avec les différents **champs** et **fonctions** du certificat.

Champ	**Fonction**
Version	Version du certificat
Serial Number	Numéro de série du certificat
Signature Algorithm	Algorithme de signature
Issuer	Entité qui a signé le certificat
Validity	Période de validité du certificat
Subject	Entité à qui le certificat est destiné
Subject Public Key Info	Informations sur la clé publique
X509v3 extensions	Extensions du certificat

2.3 Contenu du CSR

CSR signifie **C**ertificate **S**igning **R**equest. C'est une requête de signature de certificat.
Voici ci-dessous un tableau listant les **champs** et **fonctions** du CSR.

Champ	**Fonction**
Version	Version du CSR
Subject	Entité à qui le certificat est destiné
Subject Public Key Info	Informations sur la clé publique
X509v3 extensions	Extensions du certificat

2.4 Création de la liste de révocation

CRL signifie **C**ertificate **R**evocation **L**ist. C'est une liste de révocation de certificats.