Introduction à la sécurité informatique - cryptologie
TP2 : cryptographie

Ce sujet est la suite de la fiche de TP numéro 1.

1 Cryptographie symétrique

Exercice 6 : Chiffrement XOR

Le but de cet exercice est de décrypter deux fichiers chiffrés à l'aide d'un **chiffrement XOR** : `encrypted_file_simple` et `encrypted_file_hard`.

Exercice 7 : Mauvaise implémentation de Vernam

Le service disponible à l'adresse `51.195.253.124`, port `4321`, exécute l'algorithme suivant :

```
new_conn, client = ma_socket.accept()
message_secret = "XXXXXXXXXXXXXXXXXXXXXXXXX"
pad = ""
while len(pad) < len(message_secret):
  while True:
    lettre = random.choice(string.ascii_uppercase)
    if lettre != 'A':
      break
  pad = pad + lettre

message_chiffre = vigenere(message_secret, pad, vigenere_table)
new_conn.sendall(bytes(message_chiffre + '\n', 'utf-8'))
new_conn.close()
```

Retrouvez la valeur de la variable `message_secret`.

Exercice 8 : Padding oracle

Vous avez intercepté un message chiffré dans le fichier `cbc_ciphertext`. Vous savez que ce message a été chiffré en utilisant AES-128 en mode CBC et la méthode de padding PKCS#7.

Le service disponible à l'adresse `51.195.253.124`, port `11111`, vous permet de **déchiffrer n'importe quel message en utilisant la clé secrète AES**, en revanche, le serveur vous donne simplement un message indiquant si oui ou non le déchiffrement a pu aboutir.

En utilisant cet oracle de déchiffrement, réalisez une attaque de type **padding oracle** pour déchiffrer le message.

2 Cryptographie asymétrique

Exercice 9 : Mise en pratique avec `openssl`

Les questions de cet exercice doivent être réalisées en utilisant l'outil `openssl`. Vous pouvez trouver de la documentation sur son utilisation sur Internet.

- Générez une clé RSA de 2048 bits,
- Toujours à l'aide de l'outil, affichez les valeurs de p, q, d, n et e,
- Utilisez cette clé pour chiffrer et déchiffrer un message de votre choix,
- Répétez cette procédure pour un fichier au lieu d'un message.

3 Canaux auxiliaires

Exercice 10 : Question de timing

Trouvez le bon mot de passe pour vous authentifier à l'adresse `51.195.253.124`, port `22222`.