CRYPTOGRAPHIE
TP N°2

Objectif du TP : *Nous allons nous intéresser à quelques méthodes simples de cryptographie "moderne". Ces méthodes seront : chiffrement par One Time Pad, chiffrement symétrique ECB, chiffrement asymétrique RSA.*

ENONCE :

Utilisez le code source fourni avec ce TP sur le site !

Exercice 1 : Le One Time Pad.
Votre premier programme va lire le contenu d'un fichier, générer un OneTimePad de la bonne taille, appliquer le chiffrement, sauver le OneTimePad et le contenu chiffré dans des fichiers séparés.

Le second programme va lire le fichier chiffré, lire le fichier contenant le OneTimePad, déchiffrer et sauver le contenu du message déchiffré dans un autre fichier.

Exercice 2 : Chiffrement symétrique ECB et algo XOR
Cette méthode consiste a définir une clef de taille fixe, puis a découper le fichier en blocs de la taille de la clef. La méthode de chiffrement est un XOR simple entre chaque bloc et la clef.
Vous ferez trois programmes :
- Le premier génère une clef de taille N (8 octets semble correct) et la sauve dans un fichier.
- Le second chiffre le contenu d'un fichier avec cette clef et sauve un fichier chiffré
- Le troisième déchiffre le contenu du fichier chiffré et sauve le résultat dans un fichier.

Si votre méthode de chiffrement est utilisée pour coder des documents HTML, cette méthode a une faille vue en TD. Mettez ceci en pratique pour déchiffrer (comme pourrait le faire Eve) en supposant que tout fichier html commence avec les caractères "<html><head>".

Conclusion ?

Exercice 3 : Chiffrement asymétrique RSA
Les fichiers "RSA.java" et testRSA.java" disponibles sur le sites mettent en oeuvre un chiffrement RSA.

- Regardez attentivement ces fichiers pour comprendre chaque ligne de code, et comprendre comment sont générées les clefs, comment sont fait le chiffrement et le déchiffrement.

Vous allez ensuite vous inspirez de ces fichiers pour faire trois programmes :
- Le premier génère un couple de clef publiques/privées pour une taille de clef de 1024 (correspond au nombre de chiffres approximatif du module). Il devra sauver la clef publique et la clef privée dans des fichiers séparés.
- Le second chiffre le contenu d'un fichier avec la clef publique sauve le fichier chiffré
- Le troisième déchiffre le contenu du fichier chiffré avec la clef privée et sauve le résultat dans un fichier.