TP 3 : Cryptanalyse

Le fichier `\\labinfo\dfs\cours\CRYSE\TPs\TP3\cryptes.zip` contient 7 fichiers. Voici, dans le désordre, une description du contenu de ces fichiers :

- Un texte français crypté selon la méthode de César (décalage de *n* lettres). Avant le cryptage, le fichier a été traité de la manière suivante : suppression de tous les accents, des chiffres, des espaces, des ponctuations et passage en majuscule (le texte ne contient donc que les 26 lettre de l'alphabet en majuscule).
- Un texte français crypté selon la méthode de Vigenère. La fichier a été prétraité comme pour César. La longueur de la clé est inférieure à 15 caractères.
- Un texte français encrypté en DES.
- Une date au format JJMMAA encryptée par RSA.

Pour corser un peu les choses, deux fichiers de "bruit" ont été rajoutés :

- Une suite aléatoire de lettres majuscules.
- Une suite aléatoire d'octets quelconques.

Enfin, le fichier `RSA-keys.txt` contient la clé publique utilisée pour le cryptage RSA.

Étape 1

Déterminer quel fichier correspond à quelle description ("Attaque distinctive").

Efforcez-vous de distinguer le plus grand nombre de fichiers possible sans essayer de les décrypter.

Lorsque vous pensez ne plus pouvoir raffiner votre connaissance sans passer au décryptage, passez à l'étape 2.

Étape 2

Mettre de côté les deux fichiers de "bruit". Pour les quatre autres, essayer de

- déterminer le texte en clair
- récupérer la clé.

Remarques

1. À la fin du TP, vous devriez avoir distingué tous les fichiers les uns des autres.
2. De plus, aurez probablement trouvé trois textes en clair et deux clés.
3. N'hésitez pas à récupérer/adapter le code que vous avez écrit dans les premiers TPs pour vous aider à résoudre celui-ci !