Projet Nigma : Deuxième soutenance

CrypTeam : LAPÔTRE Guillaume (lapotr_g)
GANIVET Justin (ganive_j)
LADEVIE Stéphane (ladevi_s)
GISLAIS Sébastien (gislai_s)

Table des matières

1 Introduction

2 Cryptographie

Cette fois-ci encore, nous avons respecté ce que nous avions prévu de présenter pour cette seconde soutenance. En effet nous avons implémenté l'algorithme DES (Data Encryption Standard). Contrairement au RSA présenté en première soutenance, le DES est un algorithme de chiffrement symétrique. Cela signifie que pour chiffrer ou déchiffrer un fichier on utilise la même clé. Ce type de chiffrement a ses avantages et inconvénients par rapport au chiffrement asymétrique. Son principal avantage est sa rapidité : il est 1000 fois plus rapide que le RSA ! Son principal inconvénient est le fait de ne possèder qu'une seule clé. Ainsi le problème principal est l'échange de cette clé entre les différents protagonistes qui veulent échanger des données chiffrées. En effet pour le RSA il suffisait de donner sa clé publique aux personnes désirant chiffrer des messages, ensuite ils renvoient les messages chiffrés et on peut les déchiffrer à l'aide de notre clé privé jamais échangé avec personne. Si l'on envoie notre clé DES au n'importe qui, il y a un risque qu'un pirate puisse intercepté la clé et donc s'en servir ensuite pour déchiffrer les messages confidentiels. Cepandant il y a une astuce permettant de contourner le problème : On chiffre la clé DES avec un chiffrement RSA !

Un petit exemple : Alice veut envoyer un message confidentiel à Bob. Bob crée donc un jeu de clé RSA puis envoie la clé publique à Alice. Alice crée sa clé DES, puis chiffre son message à envoyer avec cette clé. Finalement, elle envoie à Bob sa clé DES chiffrée avec la clé publique RSA ainsi que le message chiffré avec la clés DES. Bob reçoit donc les deux fichiers, avec sa clé privé RSA il déchiffrer le fichier de clé envoyé apr Alice, puis avec la clé DES qu'il vient de déchiffrer il peut déchiffrer le message d'Alice !

Le DES a été achevé en 1977, c'est donc un algorithme de chiffrement ancien. Sa sécurité n'est plus optimal, en effet un état peut casser une clé DES en quelque minutes maintenant. Cepandant nons pensons qu'il est intéressant de se pencher sur cet algorithme qui fût un des premiers algorithmes de chiffrement symétrique défini rigouresement.

2.1 Partie de Guillaume Lapôtre

2.2 Partie de Sébastien Gislais

3 Stéganographie

3.1 Partie de Justin Ganivet

3.2 Partie de Stéphane Ladevie

4 Conclusion

5 Annexe

5.1 Screenshot Cryptographie