13092 MOUFAKKIR Zineb

La cryptographie RSA

Nous envoyons chaque jour des dizaines d'informations secrètes sur internet. Qui peut nous assurer qu'ils sont en sécurité et que personne ne peut les atteindre? Dans ce contexte, le chiffrement RSA demeurent une partie indispensable de la sécurité informatique moderne.
Le cryptage est l'un des piliers les plus importants des enjeux de société surtout dans le monde actuel où une entreprise s'appuie de plus en plus sur son système d'information et où des messages très privés en provenance de réseaux informatiques sont transmis d'un appareil à un autre.

Une demande de confidentialité a été enregistrée pour ce MCOT.

Positionnement thématique (ETAPE 1)

MATHEMATIQUES (Algèbre), INFORMATIQUE (Informatique pratique).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
cryptographie	*cryptography*
chiffrement asymétrique	*asymmetric encryption*
clé privée	*private key*
clé publique	*public key*
nombres premiers	*prime numbers*

Bibliographie commentée

Le cryptage est historiquement l'une des premières applications de l'informatique. Ce domaine, qui était il y a encore quelques années, réservé aux militaires et aux grandes entreprises, concerne aujourd'hui tous ceux qui souhaitent transmettre des données protégées, qu'ils soient professionnels ou particuliers. Pour cela, il existe de nombreuses méthodes de cryptage, mais peu d'entre elles sont reconnues comme sûres. La méthode RSA fait depuis longtemps partie de cette catégorie. Le cryptage RSA, du nom de ses concepteurs, Ron Rivest, Adi Shamir et Leonard Adleman, est le premier algorithme de chiffrement asymétrique. Il a été découvert en 1977 au Massachusetts Institute of Technology. [1]

Un chiffrement asymétrique est un cryptage où l'algorithme de chiffrement n'est pas le même que celui de déchiffrement, et où les clés utilisées sont différentes. L'intérêt est énorme : il n'y a plus besoin de transmettre la clé à son destinataire, il suffit de publier librement les clés de cryptage. N'importe qui peut alors crypter un message,mais seul son destinataire, qui possède la clé de décodage, pourra le lire[2]. Le RSA est basé sur la théorie des nombres premiers, et sa robustesse tient du fait qu'il n'existe aucun algorithme de décomposition d'un nombre en facteurs premiers. Alors qu'il est facile de multiplier deux nombres premiers, il est très difficile de retrouver ces deux entiers si l'on en connaît le produit.

Ce projet est la réalisation d'une application en simulant une attaque sur le crypto-système RSA. Nous allons développer un petit programme d'espionnage sous quelques conditions.

Problématique retenue

malgré sa force qui garantit la confidentialité tout en protégeant la communication entre les personnes dans le monde virtuel. le message codé par le RSA risque toujours d'être déchiffrer après une attaque. Alors comment profiter de ces failles pour attaquer le RSA ?

Objectifs du TIPE

1-générer des clés privées et des clés publiques

2-démontrer par des calculs mathématiques comment attaquer le cryptage RSA .

3-réaliser une application en simulant une attaque sur le crypto-système

Références bibliographiques (ETAPE 1)

[1] Simon Singh : The code book

[2] *http://planeteisn.fr/crypto/cryptographie_ rsa.pdf*

[3] Dan Boneh : Twenty years of attacks on the RSA cryptosystem :
https://www.ams.org/notices/199902/boneh.pdf

DOT

[1] *j'ai pris tout d'abord connaissance sur le fonctionnement et les notions nécessaires du cryptage RSA et sa relation avec l'arithmétique*

[2] *J'ai traduit l'algorithme de cryptage en un exemple simple pour clarifier son fonctionnement*

[3] *Simulation de nombreuses attaques sur le RSA*

[4] *J'ai réalisé un programme en simulant une des attaques citées sur le crypto-système*