TD3 – Cryptographie

Chiffrement Asymétrique RSA

Télécharger l'archive TD3.zip sur enseignement.

Partie 1 : Chiffrement RSA

1) Étudier, compiler et tester le code de **test_size.c**

   Que fait ce programme?
2) Pourquoi utiliser le type **Huge** au lieu de **int** lors de l'utilisation de RSA?

   Quelles sont les valeurs minimales et maximales pour un **int** et un **Huge**?

   typedef unsigned long int Huge;
3) Que fait la fonction suivante?

```
static Huge modexp(Huge a, Huge b, Huge n) {
    Huge        y;
    y = 1;
    while (b != 0) {
        if (b & 1)
            y = (y * a) % n;
        a = (a * a) % n;
        b = b >> 1;
    }
    return y;
```

---

4) Ecrire une fonction en C qui prend en paramètres deux entiers **P** et **Q** et qui affiche la clé publique **(e,n)** et la clé privé **(d)** correspondants.
5) A l'aide de la fonction **modexp, é**crire une fonction **rsa_crypt** qui prend en paramètres une clé publique **(e,n)** et un message **M** à chiffrer (du type **Huge**) et qui renvoie le message chiffré avec l'algorithme RSA. Tester votre fonction avec les valeurs vues en cours (slide 28).
6) A l'aide de la fonction **modexp, é**crire une fonction **rsa_decrypt** qui prend en paramètre une clé privée **(d)** et un message **C** chiffré (du type **Huge**) et qui renvoie le message déchiffré avec l'algorithme RSA. Tester votre fonction avec les valeurs vues en cours (slide 28).

Partie 2 : Génération de clés RSA

1) Ecrire une fonction en C qui génère un paire de clefs RSA **((e,n),d)**.

   Pour cela vous aurez besoin d'écrire :

- Un générateur de nombre premiers (qui renvoi le plus grand nombre premier inférieur à une valeur N passée en paramètre)
- Une fonction gcd(x,y)

Partie 3 : Librairie de chiffrement

1) Compléter le code de la librairie en complétant les fonctions **rsa_crypt** et **rsa_decrypt**.

   Pour cela, vous utiliserez les fonctions **texttoint** et **inttotext** pour normaliser le message et le caractère **'$'** comme séparateur de bloc.

2) Inclure votre générateur de clé RSA dans la librairie.