

Barret Alexandre - Mizoules Vincent

Compte rendu - TP6

Usage

Pour lancer notre programme :

```
make && ./tp6
```

Pour nettoyer le projet

```
make clean  
make clear
```

Il est possible de désactiver l’affichage des informations de debug en commentant/décommentant le `define` présent au début du programme.

Réponses aux questions

1)

L’algo RSA repose sur 6 étapes :

- 1) Tout d’abord on génère deux entiers premiers avec la fonction ‘nextprime’
- 2) On calcule n et ϕ via des simples multiplications
- 3) On prend un nombre inférieur à ϕ impair via la fonction ‘gcd’
- 4) On calcule d tel que $ed \equiv 1 \pmod{\phi}$ via la fonction ‘invert’
- 5) Affichage des clés
- 6) Chiffrement / déchiffrement du message via la fonction ‘powm’

2)

Pour tester l’algorithme de chiffrement et déchiffrement sur des données aléatoires, nous avons écrit une fonction nommée `getRandomMessage` qui génère un message aléatoire de taille fixé par l’utilisateur.

Notre programme fonctionne bien !

3)

Les fonctions réécrites sont `custom_nextprime` et `custom_powm` correspondants respectivement aux fonctions `mpz_nextprime` et `mpz_powm`.

Elles sont utilisées dans notre programme principale et fonctionnent parfaitement.