

MiniRSA

Cahier des charges:

Réaliser en équipe, le développement d'un miniRSA en utilisant des concept de cryptographie asymétrique

- Générer des clés privée et publique
- Signer un message donnée
- Générer un certificat pour une clé publique
- Coder le test de Miller-Rabin

Grâce à ce projet j'ai découvert comment:

- Réaliser un message coder
- Signer un message
- Générer l'empreinte d'un message
- Gérer de grands entiers

Logiciel utilisé:

- Notebook python

Livrables:

```
Le message d'origine de Alice est 1435263726352725355365241625326643625185635625635624365265736
Empreinte:
28487066876335106005769088999416046006469128091404508879916493712454946167307606134005165643736
Empreinte Chiffré:
10891161699126934696117569456587297620755789507425202244476870388170193927376511625943079044935
Message + empreinte:
10891161699126934696117569456587297620755789507425202244476870388170193927376511625943079044935
Message déchiffré:
14352637263527253553652416253266436251856356256356243652657365535365381089116169912693469611756
Message : 1435263726352725355365241625326643625185635625635624365265736553536538
Empreinte du message chiffrée:
10891161699126934696117569456587297620755789507425202244476870388170193927376511625943079044935
Le message décrypté est 1435263726352725355365241625326643625185635625635624365265736553536538
```

Résultat du RSA