Criptografia

Curvas Elípticas

Lucas de Macedo Terças

Contents

Curvas Elípticas

Especifica

Cifragem

1. Solicitar ao usuário os parâmetros (p, d, e)
2. Disponibilizar a curva para outro programa
3. Definir o ponto q da curva
4. Definir o valor da variável k
5. Ler a mensagem clara de um arquivo txt
6. Gerar os pontos Pm a partir da mensagem clara
7. Criptografar os pontos Pm armazenando em um arquivo txt

Decifragem

1. Definir a chave privada e salvar em um arquivo
2. Gerar a chave pública e armazenar em um arquivo
3. Decifrar a mensagem cifrada e armazenar em um arquivo txt

Funcionamento

Cifragem

```
a = b
```