实验三 公钥密码实验报告

1. 实验目的
2. 熟悉多精度数学库gmp，详见实验二；
3. 掌握gmp的使用方法；
4. 掌握RSA加密和解密使用方法；
5. 掌握ECDSA数字签名使用方法；
6. 掌握RSA密码分析方法
7. 实验背景

（请根据密码学课堂学习内容自行填写）

1. 实验内容

1）读取文件plaintext.txt，完成以下加密任务：

随机生成一对RSA公钥pk和私钥sk，随机生成一个128比特的AES加密密钥k，用pk采用RSA加密k得到密文ek，用k采用AES加密文件plaintext.txt中的内容，采用CBC模式，得到密文et，最后把密文ek和et写到文件cipher-de.txt

2)随机生成一对ECDSA的公钥pk和私钥sk，利用sk采用ECDSA数字签名算法对文件plaintext.txt中的内容进行数字签名，哈希函数采用SH256，并把签名拼到plaintext的后面，一起写到文件plaintext-sig.txt

3)完成如下RSA密码分析任务：

详见文件：RSA密码分析.docx

1. 实验过程
2. 实验心得