|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | 实验项目  名 称 | 实验三 RSA非对称加密算法 | 成绩 |  |   **一、实验目的**  1)  了解非对称加密机制。  2)  理解 RSA 算法的加解密原理。  3)  能够使用 RSA 算法对数据进行加解密处理。  **二、实验内容**  用c++语言实现 RSA 加解密程序   1. **实验步骤**   1.为MAC系统配置GMP库（脚本在setup.sh中）  编译代码时，需要加“-lgmp”：  g++ -o rsa.o rsa.cpp -lgmp  2.随机生成大素数p，q:  先随机生成128位大整数(mpz\_urandomb)，再调用mpz\_nextprime，求此大整数的下一个素数，这样可以获得随机的大素数  3.生成n，ϕ(n):  n = p\*q, ϕ(n)=(p-1)\*(q-1)  **../Screen%20Shot%202018-05-23%20at%2012.29.58%20AM.png**  4.选择a，b：  1）a为65537  2）b为模ϕ(n)下a的逆（调用mpz\_invert函数）  ../Screen%20Shot%202018-05-23%20at%2012.32.01%20AM.png  5.（a，n）构成公钥，（b，n）构成私钥  6. 加解密函数：  用户输入的待加(解)密文本为 txt，选择的秘钥为key，使用mpz\_powm可以求出加（解）密的结果，函数如下：  **../Screen%20Shot%202018-05-23%20at%2012.33.54%20AM.png**  7.主函数循环：等待用户输入的待加(解)密文本，与秘钥的选择，选用相应的秘钥加解密，输出结果（按q可退出）  **四、实验结果及分析**  1. 某次运行程序，生成各个参数如下：  **../Screen%20Shot%202018-05-23%20at%2012.14.41%20AM.png**  2. 加密解密结果  ../Screen%20Shot%202018-05-23%20at%2012.14.51%20AM.png  如上图，“5201314”用一个秘钥加密后，再另一个秘钥解密可以得到“5201314”，说明结果是正确的。  **五、实验总结**  1.通过这个实验，进一步理解了RSA算法的原理和实现细节  2. 学习了GMP库的基本使用方法  **六、代码说明及实验环境：**  1.代码文件夹与本报告在同一文件中。  Github: <https://github.com/vampire321/rsa.git>  rsa.cpp: c++文件  rsa.o: 可执行文件  setup.sh: 配置gmp库脚本  2. 实验环境：  1）MAC OS，配置如下：    2）G++版本：Apple LLVM version 9.1.0 (clang-902.0.39.1)  3）GMP 版本：6.1.2 |
| **七、实验参考：**  1. 配置GMP库: <https://zybuluo.com/veightz/note/12742>  2. GMP说明文档: <https://gmplib.org/gmp-man-6.1.0.pdf>  3. C++ GMP库: <https://blog.csdn.net/lianzhouxiaowu/article/details/53669636> |