|  |
| --- |
| **Github账号：** |
| **个人博客关于密码学大作业的链接：**[密码学大作业\_DeeBaTO的博客-CSDN博客](https://blog.csdn.net/DeeBaTO/article/details/129343622?csdn_share_tail={"type":"blog","rType":"article","rId":"129343622","source":"DeeBaTO"}) |
| **题目：RSA大礼包** |
| **摘要：**  本次RSA大礼包大作业中，本人对于RSA的一系列使用数论以及格的攻击进行整理，以及对本次实验中提供的样本进行分析以及攻击，成功破译得到内容。  并且将代码托管于Github仓库，将文章发布于博客中。 |
| **题目描述**  有人制作了一个 RSA 加解密软件（采用的 RSA 体制的参数特点描述见密码背景部分）。已知该软件发送某个明文的所有参数和加密过程的全部数据（加密案例文件详见附件 3-1）。Alice 使用该软件发送了一个通关密语，且所有加密数据已经被截获，请问能否仅从加密数据恢复该通关密语及 RSA 体制参数？如能请给出原文和参数，如不能请给出已恢复部分并说明剩余部分不能恢复的理由？  即对给出的内容进行破解，并且分析是否参数选取不恰当，是否会被攻击成功。 |
| **过程**  将在后文进行详细描述。 |
| **总结**  我们在使用RSA的时候，需要注意是否参数选取不恰当，以及随机数生成器使得素数生成是否不安全。 |
| **参考文献**  [1] Dan Boneh et al. Twenty years of attacks on the rsa cryptosystem. Notices of the AMS, 46(2):203–213, 1999. 2.1  [2] Don Coppersmith. Finding a small root of a univariate modular equation. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 155–165. Springer, 1996.2.2.1  [3] Nicholas Howgrave-Graham. Finding small roots of univariate modular equations revisited. In IMA International Conference on Cryptography and Coding, pages 131–142. Springer, 1997. 2.3  [4] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefffficients. Mathematische annalen, 261(ARTICLE):515–534, 1982. 2.2.1  [5] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120–126, 1978. 2.1  [6] H. P. Williams. Integer and combinatorial optimization. Journal of the Operational Research Society, 41(2):177–178, 1990. 2.3  [7] [【大数分解】Pollard‘s p-1 method\_随缘懂点密码学的博客-CSDN博客](https://blog.csdn.net/qq_42667481/article/details/106729900) |