**RSA公钥密码体制的攻击**

1. **实验任务描述**

1.1符号说明

对任意一个比特正整数，设为其二进制表示，则称为的二进制比特串，为二进制比特串对应的整数。

1.2加密系统描述

某加密邮件系统的128比特密钥由RSA-2048加密保护。假设用户Alice给用户Bob发邮件，其加密过程如下：

1. 第一步：Alice随机产生128比特随机密钥，加密邮件得到密邮件;
2. 第二步：Alice选定Bob的公钥)，加密密钥：先按固定方式得到2048比特填充，然后计算

;

1. 第三步：用户Alice将（）发送给Bob。

该系统提供的RSA模数均由某固定随机序列（）的某段产生，生产方式如下：随机产生起点,从开始检测二进制比特串对应的1024比特整数的素性,不满足则将增加1再检测,直至为素数;同样,从位置开始检测,直到某个使得二进制比特串对应的1024比特整数为素数，则输出模数。加密指数为范围内的奇数。

1.3问题描述

假设已经掌握了多个用户的证书以及产生证书的起点。已知,请给出求取加密密钥的方法。

1.4实验要求

1）根据提供的证书相关数据条件，构建求解模型，求出加密密钥，共有6个用户数据；

2）描述整个分析和求解过程，特别是模型构建和求解算法的创新性。

1. **密码学背景及相关问题的研究进展**

大数分解是一个古老的数论问题，1977年麻省理工学院的Rivest、 Shamir和 Adleman利用这个问题的难解性成功地设计出了RSA公钥密码体制，至今广泛应用于网络与信息安全中。

整数分解方法的发展与公钥密码学的发展密切相关，从RSA公钥密码体制提出至今，整数分解问题不断取得突破，形成了许多有效的方法，总结起来可以分为两类：一类是特殊分解方法，对待分解整数的素因子有特殊要求，这类方法包括试除法、法、方法、SQUFOF类群方法及椭圆曲线方法等；另一类是基于组合同余的一般分解方法，对素因子没有特殊的要求，这一类方法包括连分数方法、二次筛法和数域筛法。目前计算复杂度最低的大整数分解方法是数域筛法，国际上用数域筛法进行大整数分解的记录是829比特。

但是在实际攻击RSA公钥密码体制时，还存在很多其它的方法，比如小加解密指数的RSA攻击方法、素因子部分泄露的RSA攻击方法等等。2013年9月，Bernstein等人利用求公因子和格技术，成功分解了台湾居民数字证书库中的184个1024比特大数，这是Coppersmith方法在实际RSA密码攻研中发挥关键作用的成功案例。

1. **参考文献**

[1] D.Coppersmith. Finding a small root of a univariate modular equation. In U. Maurer. Proceedings of Eurocrypt’96, Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, Berlin, 155-165, 1996 .

[2] D. Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In U. Maurer. Proceedings of Eurocrypt’96, Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, Berlin, 178-189, 1996.

[3] Jingguo Bi and Phong Q. Nguyen.Rounding LLL: Finding Faster Small Roots of Univariate Polynomial Congruences, 2013.

[4] J. Coron, J. Faugere, G.Renault, and R.Zeitoun. A variant of Coppersmith's Algorithm with Improved Complexity and Efficient Exhaustive Search, 2013.

[5] J. Hastad. On using RSA with low exponent in a public key network, Advances in Cryptology – CRYPTO’85, LNCS 218, Springer-Verlag, 408-408, 1986.

[6] D. Boneh and G.Durfee. Cryptanalysis of RSA with private key d less than N0.292. IEEE Trans. On Information.Theory, vol. 46(4), 1339-1349, 2000.

[7] D. Coppersmith. Small solutions to Polynomial Equations and Low Exponent Vulnerabilities. Journal of Cryptology, vol.10(4):223-260, 1997.

[8] J.Blomer and A. May. New partial key exposureattacks on RSA. Lecture Notes in Computer Science, vol. 2729, Springer-Verlag, Berlin, 27-43, 2003.

[9] Henri Cohen.A Course in Computational Algebraic Number Theory. Springer-Verlag GTM138.

[10] Brent R P. Recent Progress and Prospects for Integer Factorisation Algorithms.Computing and Combinatorics:6th Annal International Conference,COCOON 2000

1. **附件**

附件为数据文件，文件名为RSA-data.txt。文件中每行为一个用户数据，总共有六个用户的相关数据；每个用户已知六个参数，具体数据格式如下：

用户号 起点 起点 模数(hex) 加密指数 密文(hex)

其中hex表示十六进制数，无说明的为十进制数。