RSA 密码体系攻击

丁湛钊[a,b]

[a] *1901210628*
[b] *anciety@pku.edu.cn*

Abstract: RSA 密码体系是目前使用最为广泛的公私钥密码体系之一，在工业界中被大量的使用。自发明以来，对 RSA 的攻击研究就一直在进行当中，RSA 算法本身是安全的，但是不当的使用方法或是忽略了其使用中的一些细节就可能会导致 RSA 算法被攻破，使得许多工业中目前还在使用中的系统的安全性受到极大的影响。在本文中，我们将讨论 RSA 的一些攻击思路，通过这些思路了解到 RSA 算法使用中的一些细节的注意事项。

1. 引言

RSA 是 1977 年由 3 位学者提出的密码体系 [1]。RSA 密码体系提供了一种非对称加密的实现方案。在非对称加密中，密钥分为公钥和私钥两个部分，使用公钥加密的密文只能使用私钥进行解密。公钥和私钥的非对称性使得加密方和解密方可以处于非对称的地位。这样的非对称性提供了一些有价值的使用场景，例如在数字签名场景中进行使用 [2]，在数字签名的场景中，加密和解密对应了签名和验签，签名者对数据进行加密，验签者对数据进行解密，但是验签者不应当对数据具有加密的能力，否则验签者同时也可以进行签名，签名就可以被任意伪造，失去了有效性。为了保证签名的有效性，就需要加密和解密的双方具有不对称的地位，验签者无法进行签名。

非对称加密的特点使得公钥可以公开，在真实软件中，加密方有时无法保证其不可被攻击者观察到，例如在 Web 服务器中，前端的数据可以被攻击者轻松获取，如果使用对称加密，就无法保证密钥的安全性，从而使得整个加密系统失去作用，所以在真实软件中，非对称加密具有大量的使用场景。在这些非对称加密中，又以 RSA 密码体系为使用最为广泛的公钥加密方式之一。所以，RSA 的安全性自然的受到了关注。一旦 RSA 的安全性受到了威胁，就意味着对大量现有软件中的安全性的威胁，所以对 RSA

安全性的研究一直以来是密码学研究的一个重要方向。在本文中，我们将介绍 RSA 的原理，以及针对 RSA 密码体系的几种重要的攻击方式。

2. RSA 密码体系

2.1. 整数分解问题

整数分解问题是 RSA 密码体系所基于的数学困难问题。整数分解问题是数论中的一个问题，在数论中，如果一个整数 $n > 1$ 当该整数的因子只有 ± 1 和 $\pm n$ 时，该整数就被认为是一个**素数**，其他的整数则被称作**合数**。根据数论中的算术基本定理，每一个正整数都可以分解为唯一的有限个素数因子的乘积。但是，在算术基本定理中，并没有给出对这些因子的求解方法。对整数这些因子的运算过程，就被称作整数分解问题。[3] 这个问题目前还没有在多项式时间内可以进行运算的方法，所以被认为是一个数学困难问题。通用数域筛选法是目前已知的最快的在传统计算机上的整数分解算法，不过其复杂度依然与多项式运行速度差距极大。[4]。如果无法在多项式时间内解决，那么这个问题在传统计算机上运行速度的增长就是很快的，通过使用大的整数，就可以基本保证这个问题以目前的计算能力来说无法进行计算了。

2.2. RSA 密钥生成

RSA 的密钥生成过程分为几步。

1. 选择两个大小相近的不同的素数 p 和 q
2. 使用这两个素数计算出他们的乘积 $N = p \times q$
3. 计算整数 N 的卡迈克尔函数结果，即 $\lambda(N)$ 。由于 $N = p \times q$ ，所以可以得到 $\lambda(n) = LCM(\lambda(p), \lambda(q))$，另外，又因为 p 和 q 都是素数，此时 $\lambda(p) = \phi(p) = p - 1$ ，所以，$\lambda(N) = (p-1) \times (q-1)$。
4. 选择一个任意的 e 使得 $1 < e < \lambda(N)$ 同时满足 $gcd(e, \lambda(N)) = 1$。这个 e 的选择对大小的要求并不高，一般来说我们可以将 e 选择为 65537。
5. 最后，我们可以使用扩展欧几里得算法计算 $d \equiv e^{-1} (mod\ \lambda(N))$ ，也就在模 $\lambda(N)$ 意义下的 e 的逆元。

经过这些操作之后，我们将使用 d 作为私钥，将 N 和 e 一起作为公钥。

2.3. RSA 加密和解密过程

2.3.1. 加密过程

RSA 的加密过程需要使用到公钥。过程为计算 $c \equiv m^e (mod\ N)$，其中的 c 就是密文。如果攻击者获取到了密文 c，想要在没有私钥的情况下获取到明文，那么就需要知道去计算 d，也就是在模 $\lambda(N)$ 意义下的 e 的逆元。由于此时，e 的内容是已知的，所以问题就在于计算逆元的过程。计算逆元本身并不复杂，但是由于此时无法获取到 $\lambda(N)$，所以计算是很困难的。如果暴力的对 $\lambda(N)$ 进行猜解，就以为着需要知道整数 N 的分解方式，这样才可能快速的计算出 $\lambda(N)$，由于整数分解问题本身是数学困难问题，那么只要整数分解问题没有简单的计算方法，攻击者就没有办法去简单的求解到这个明文的值了。

2.3.2. 解密过程

在有私钥的情况下，解密过程是很简单的，通过 $c^d \equiv (m^e)^d \equiv m$ 就可以恢复出明文了。

3. RSA 密码体系的攻击方式

3.1. 共模数攻击（Common Modulus Attack）[5]

在错误的使用方式中，如果整数 N 在多个加密过程中被重复用于加密同一密钥，例如在两次加密中使用了 $< N, e_1 >$ 和 $< N, e_2 >$ 作为其公钥，同时满足 $gcd(e_1, e_2) = 1$，两次加密的结果分别为 $c_1 = m^{e_1}$ 和 $c_2 = m^{e_2}$ 那么就可以进行共模数攻击。由于 $gcd(e_1, e_2) = 1$，那么根据贝祖定理，$ae_1 + be_2 = 1$ 中的 a 和 b 有整数解，这个解可以通过扩展欧几里得算法获取。明文的计算方法如下:

$$c_1^a c_2^b = m^{e_1 a} m^{e_2 b} = m^{e_1 a + e_2 b} = m^1 = m \tag{1}$$

所以在 RSA 的使用中，模数 N 应当每次使用不同的值，而不能反复使用。

3.2. 费马分解攻击（Fermat Factoring Attack）[6]

在 RSA 密码体系中使用了 p 和 q 用于生成公钥的 N，在 p 和 q 满足特定条件时，可能导致 RSA 的安全性受到威胁。

设 $\Delta = p - q$，当 $\Delta < N^{\frac{1}{4}}$ 时，费马的分解方法可以有效的分解出 p 和 q，其复杂度为 $O(\frac{\Delta^2}{N^{\frac{1}{2}}})$。在这种攻击方法中，由于 $\Delta = p - q$ 的范围较小，通过找到除 $x = N + 1$ 以及 $y = N - 1$ 以外的 x 和 y 使得 x 和 y 满足

$4N = x^2 - y^2$ ，如果成立，我们就可以使 $p = \frac{1}{2}(x + y)$ 以及 $q = \frac{1}{2}(x - y)$ ，此时 $N = pq$ 成立。

设 $B = \lceil 2N^{\frac{1}{2}} \rceil$ ，查找 x 和 y 的方法就是通过不断尝试 B、$B + 1$ 以此类推，直到 $x^2 - 4N$ 为平方数。

在这个过程中，我们需要尝试的次数大约为 $x - 2N^{\frac{1}{2}} = p + q - 2N^{\frac{1}{2}}$，此时又由于 $\Delta^2 = (p + q)^2 - 4N = (p + q - 2N^{\frac{1}{2}})(p + q + 2N^{\frac{1}{2}})$ 那么，$p + q - 2N^{\frac{1}{2}}) < \frac{\Delta^2}{4N^{\frac{1}{2}}}$ 。

所以在 RSA 的使用中，素数 p 和 q 的选择需要满足一些特定的要求，除此以外，还有一些其他针对 p 和 q 的计算方法，例如 Pollard 的 $p - 1$ 攻击 [7]，在这个攻击中，要求 p 和 q 的选择中，$p - 1$ 或 $q - 1$ 不应当是平滑数，以及 William 的 $p + 1$ 攻击 [8] 要求 $p + 1$ 或 $q + 1$ 不应当是平滑数。

3.3. Håstad 的广播攻击（Håstad's broadcast attack）[6]

在 RSA 密码体系中，公钥包含两个部分 N 和 e 。e 的选择如果过小，可能会导致安全性受到威胁。

Håstad 的广播攻击指出，设 $N_1, ..., N_k$ 是互素的整数，且 $N_{min} = min_i\{N_i\}$，设 $g_i(x) \in \mathbb{Z}/N_i[x]$ 为 k 个最高次为 q 的多项式，假设明文 $m < N_{min}$，同时对 $i \in \{1, ..., k\}$ 有 $g_i(m) \equiv 0 \ (mod\ N_i)$，且 $q < k$，此时如果获取到所有的 $< N_i, g_i(x) >$ ，那么就可以恢复出明文。

我们将展示 Håstad 的广播攻击的一种简单形式，来展示 e 的选择在特定情况下对 RSA 安全性的影响。

假设 $e = 3$，多项式一共有 3 个，同时 $m < N_{min}$ ，一共有三个加密消息：

$$c_1 = m^3 \ (mod\ N_1)$$
$$c_2 = m^3 \ (mod\ N_2)$$
$$c_3 = m^3 \ (mod\ N_3)$$

此时，就可以使用中国剩余定理得到 $m^3 \equiv c \ (mod\ N_1N_2N_3)$，此时 $m^3 < N_{min} < N_1N_2N_3$，此时对 c 进行开三次方操作就可以得到 m 了。

对于更大的 e ，我们需要更多的多项式方程。所以，e 的选择会涉及到安全性，而要彻底防御这种攻击，还需要使用具有一定随机化的填充方案，例如使用 OAEP 填充方案等。[9]

3.4. Wiener 的攻击

在 RSA 中，私钥 d 如果选择不当也可能导致安全问题。例如 Wiener [10] 提到，在 $d < \frac{1}{3}N^{\frac{1}{4}}$ 时，那么在只知道公钥的情况下就可以对明文进行恢复。

首先，由于 $ed \equiv 1\ (mod\ \lambda(N))$，此时 $\lambda(N) = (p-1) \times (q-1)$，所以存在整数 k 使得 $ed = 1 + (p-1)(q-1) = 1 + k(N - p - q + 1)$。

通过计算 $|\frac{e}{N} - \frac{k}{d}| = |\frac{1}{dN} - \frac{k(p+q-1)}{dN}| = |\frac{k(p+q-1)}{dN}| < \frac{1}{2d^2}$，再根据连分数定理，$x = \frac{k}{d}$ 应该是 $\frac{e}{N}$ 的连分数展开的其中一个渐近。在这个时候，$\frac{e}{N}$ 只使用了公钥的内容，所以是已知的，$\frac{1}{k} < 1$，那么 $\lfloor \frac{e}{x} \rfloor = \lfloor \frac{ed}{k} \rfloor = \lfloor \frac{1}{k} + \lambda(N) \rfloor = \lambda(N)$。已知 $\lambda(N)$ 想要恢复到 p 和 q 就比较容易了，因为 $\lambda(N)$ 配合已知的 N 包含了 $p + q$ 的信息。

所以，通过这种攻击，说明 RSA 密钥中，对私钥的选取也需要符合一定的要求，不能太小，否则就会导致其安全性无法得到保证。

4. 发展

2017 年 K. Somsuk 等人提出了对费马分解攻击的一种改进方式，称为 SFFA-X 算法 [11]，在这个算法中将费马分解攻击中的一些不相关的整数信息忽略掉，提高了费马分解攻击的速度。Bunder 等人则是在这一年提出了利用连分数的一种新型的 RSA 攻击方式 [12]，在 Wiener 攻击的基础上做了一些改进，将 Wiener 攻击中对私钥指数 d 的大小范围进行了扩大。之后，在 2019 年，Susilo 等人再次对这个方法进行了改进，再一次扩大了可以恢复到私钥的私钥指数大小范围。另外，在 RSA 的一些变种形式被提出以后，针对 RSA 的变种的一些攻击形式也得到了发展。例如 Takayasu 等人提出了利用一种新型的格构造对 CRT-RSA 的一种攻击方式 [13]，Bunder 等人也提出了一种攻击方式可以对三种 RSA 的变种形式进行攻击 [14]。

5. 结论

我们对 RSA 密码体系中各个参数的其中一种攻击方式进行了介绍。通过这些攻击方式我们了解到，虽然 RSA 密码体系本身基于整数分解问题实现，整数分解问题是一个数学困难问题，其安全性有一定程度的保证，但是在 RSA 的密钥选择和参数选择以及填充方案上都需要非常小心，其中的任何一个环节都对 RSA 的安全性有一定的影响，不当的配置将会使得 RSA 密码体系的安全性大大下降。所以在使用 RSA 当中，我们需要小心的选取参数和填充方式，避免出现由于不当使用导致的安全性下降。

References

[1] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.

[2] *W. Diffie, M. Hellman, New directions in cryptography, IEEE transactions on Information Theory 22 (6) (1976) 644–654.*

[3] *P. L. Montgomery, A survey of modern integer factorization algorithms, CWI quarterly 7 (4) (1994) 337–366.*

[4] *T. Kleinjung, On polynomial selection for the general number field sieve, Mathematics of Computation 75 (256) (2006) 2037–2047.*

[5] *M. Mumtaz, L. Ping, Forty years of attacks on the rsa cryptosystem: A brief survey, Journal of Discrete Mathematical Sciences and Cryptography 22 (1) (2019) 9–29.*

[6] *B. De Weger, Cryptanalysis of rsa with small prime difference, Applicable Algebra in Engineering, Communication and Computing 13 (1) (2002) 17–28.*

[7] *J. M. Pollard, Theorems on factorization and primality testing, in: Mathematical Proceedings of the Cambridge Philosophical Society, Vol. 76, Cambridge University Press, 1974, pp. 521–528.*

[8] *H. C. Williams, A $p + 1$ method of factoring, Mathematics of computation 39 (159) (1982) 225–234.*

[9] *M. Bellare, P. Rogaway, Optimal asymmetric encryption, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1994, pp. 92–111.*

[10] *M. J. Wiener, Cryptanalysis of short rsa secret exponents, IEEE Transactions on Information theory 36 (3) (1990) 553–558.*

[11] *K. Somsuk, K. Tientanopajai, An improvement of fermat's factorization by considering the last m digits of modulus to decrease computation time., IJ Network Security 19 (1) (2017) 99–111.*

[12] *M. W. Bunder, J. Tonien, A new attack on the rsa cryptosystem based on continued fractions.*

[13] *A. Takayasu, Y. Lu, L. Peng, Small crt-exponent rsa revisited, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2017, pp. 130–159.*

[14] M. Bunder, A. Nitaj, W. Susilo, J. Tonien, A new attack on three variants of the rsa cryptosystem, in: Australasian Conference on Information Security and Privacy, Springer, 2016, pp. 258–268.