

# EFFICIENT METHOD FOR BREAKING RSA SCHEME

**Sattar J Aboud and Mohammad A AL-Fayoumi**  
Middle East University for Graduate Studies  
Faculty of Information Technology  
Amman-Jordan

## ABSTRACT

The security on many public key encryption schemes relied on the intractability of finding the integer factoring problem such as RSA scheme. However, there are great deals of researches related to the RSA factoring modulus compared with the other type of attacks RSA scheme. So the need for more methods of attacks other than RSA factoring modulus to obtain an efficient and faster algorithm to solve this problem is still essential. This paper introduces a new algorithm which attacks the RSA scheme. The suggested algorithm aims to obtain the private key of the RSA scheme and then factoring the modulus based on the public key  $e$  of the RSA scheme. The new idea claimed to be more efficient than the already existed algorithms especially when the public key  $e$  is small, since most of public key encryption schemes select a small encryption exponent  $e$  in order to improve the efficiency of encryption. The suggested algorithm is claim to be more efficient than the already existed algorithms of attack since it is faster and takes less running time.

**Keywords:** Public key cryptography, RSA scheme, factoring problem, RSA attack scheme

## 1 INTRODUCTION

Public key cryptography is one of the mathematical applications that are valuable in sending information via insecure channels, which is counted as the worse case used in the e-commerce and internet today. However, there are some algebraic assumptions which are considered to be an important key in this issue such as prime numbers and integer factoring problem.

Factoring an integer modulus  $n$  means find its prime numbers  $p$  and  $q$ . However, factoring the modulus is in fact a hard problem and most of the popular public key cryptography schemes are relied on [1], but surly not impossible because the RSA-120 is factored using quadratic sieve by Thomsan, Bruce, Arjen and Mark [2]. Also, the RSA-140 is factored using number field sieve by Cavallar, Dodson, Lenstra, Leyland, Lioen, Montgomery, Murphy and Zimmermann [3]. While RSA-155 is factored in 1999, also, the RSA-160 is factored in April 2003, and the RSA-576 is factored in December 2003 by Eric [4]. The RSA-200 is

factored in 2004; the RSA-640 is factored in November 2, 2005 by Bahr, Boehm, Franke and Kleinjung [5] and verified by RSA Laboratories. The relation between factoring and the public key encryption schemes is one of the main reasons that researchers are interested in factoring algorithms [6].

In 1976 Diffie-Hellman [7] creates the first revolutionary research in public key cryptography via presented a new idea in cryptography and to challenge experts to generate cryptography algorithms that faced the requirements for public key cryptosystems. However, the first reaction to the challenge is introduced in 1978 by RSA [8]. The RSA scheme is a block cipher in which the original message and cipher message are integer values in the interval  $[0..n-1]$  where  $n$  a composite modulus. In this paper we take the public key  $(e, n)$  only to disclose the original modulus from the RSA scheme. However, the message in RSA scheme is encrypted in blocks after divide it to blocks, every block must convert to a value smaller than the modulus  $n$ . The intractability of the RSA assumption forms its security. The RSA assumption is the difficulty of

solving the integer modulus  $n$  which is a product of two distinct odd large primes  $p$  and  $q$  with an assistance of another public key  $e$  and an integer cipher text  $c$  [9]. In other words, the RSA difficulty is that of solving  $e^{\text{th}}$  roots mod a composite modulus  $n$ . The conditions determined the modulus  $n$  and the public key  $e$  are to guarantee that for every integer  $c \in (0, 1, \dots, n-1)$  there is just one  $m \in (0, 1, \dots, n-1)$  where  $m^e = c \pmod n$ . However, the RSA scheme is the most employed public key encryption compared with the other schemes. It can be employed for both encryption and digital signature schemes.

## 2 SECURITY OF RSA

This section introduce a security issue related to RSA encryption scheme, based on the small encryption public key  $e$  that we will discuss, as well as an appropriate measures to counteract the threat.

In order to enhance the encryption efficiency, it is enviable to select a small public key encryption as  $e=3$ . When an encryption public key  $e$  is selected arbitrarily, then the RSA encryption scheme employing the repeated square and multiply method takes  $k$  modular squaring and an expected  $k/2$  less with optimizations, modular multiplication, where  $k$  is the size string length of the modulus  $n$ . Then encryption algorithm can be accelerate via choosing the encryption public key  $e$  as small as possible or via choosing the public key  $e$  with a small number of 1's in its binary representation. The encryption public key  $e=3$  is generally used in scheme. In this situation, it is essential that both  $p-1$  and  $q-1$  is divisible via 3. This gives a very fast encryption operation because it just needs 1 modular squaring and 1 modular multiplication.

## 3 RELATED WORK

The RSA cryptography scheme was introduced in 1977 by Rivest, Shamir and Adleman [8]. Kaliski and Robshaw [10] give an outline of the main attack methods on RSA public key encryption and digital signature schemes, and the practical methods of counteracting these methods of attacks. The computational correspondence of computing the decrypted key  $d$  and then factoring the modulus  $n$  was shown by RSA based on previous work done by Miller [11].

The attack on RSA with small encryption public key is discussed by Håstad [12] who illustrated that sending an encryption of more than  $e(e+1)/2$  linearly related messages of the type

$(a_i * m + b_i)$ , where  $a_i$  and  $b_i$  are known allows an adversary to decrypt the messages provided that the modulus  $n_i$  satisfy  $n_i > 2^{(e+1)(e+2)/4} * (e+1)^{(e+1)}$ . Coppersmith [13] introduced a new type of attacks on RSA which enable a passive adversary to recover such message from the corresponding cipher text. This attack is of practical importance since many public key encryption schemes have been proposed which require the encryption of polynomial related messages. For instance include the key distribution protocol of Tatebayashi, Matsuzaki, and Newman [14], and the verifiable signature scheme of Franklin and Haber [15].

Coppersmith [16] introduced an efficient method for finding a root of a polynomial of degree  $k$  over  $z_n$ , where  $n$  is the RSA modulus, provided that there is a root smaller than  $n^{1/k}$ . The method produced two types of attacks on RSA with small encryption public key. When  $e=3$  and if an opponent knows an encrypted message  $c$  and more than  $2/3$  of the message  $m$  related to  $c$  then the opponent can efficiently discover the remainder of the message  $m$ . Assume now that messages are padded with random bit strings and encrypted with public key  $e=3$ . If the opponent knows two encrypted messages  $c_1$  and  $c_2$  which correspond to two encryptions of the same message  $m$  with different padding, then the opponent can efficiently retrieval  $m$  given that the padding is less than  $1/9$  of the size of the modulus  $n$ . The second attack proposes that care should be exercised if employing random padding in conjunction with a small encryption public key.

In this paper we suggest an efficient algorithm to break the RSA scheme. Through define a functional problem of attack taking in its account the public key encryption of the RSA scheme. But before that we are going to discuss the RSA scheme.

## 4 RSA SCHEME

In 1978, RSA [8] developed a public key cryptosystem that is based on the difficulty of integer factoring. The RSA public key encryption scheme is the first example of a provably secure public key encryption scheme against chosen message attacks. Assuming that the factoring problem is computationally intractable and it is hard to find the prime factors of  $n = p * q$ . The RSA scheme is as follows:

### Key generation algorithm

To generate the keys entity  $A$  must do the following:

1. Randomly and secretly choose two large prime

- numbers  $p$  and  $q$  with equally likely.
2. Compute the modulus  $n = p * q$ .
  3. Compute  $\theta(n) = (p-1)(q-1)$
  4. Select random integer  $e, 1 < e < n$  where  $\gcd(e, \theta) = 1$
  5. Use Baghdad method [17] to compute the unique decrypted key  $d, 1 < d < \theta(n)$  where  $e * d \equiv 1 \pmod{\theta(n)}$
  6. Determine entity  $A$  public and private key. The pair  $(d, \theta)$  is the private key. While the pair  $(n, e)$  is the public key.

#### Public key encryption algorithm

Entity  $B$  encrypts a message  $m$  for entity  $A$  which entity  $A$  decrypts.

**Encryption:** entity  $B$  should do the following:

- Obtain entity  $A$ 's public key  $(n, e)$ .
- Represent the message  $m$  as an integer in the interval  $[0..n-1]$
- Compute  $c = m^e \pmod{n}$
- Send the encrypted message  $c$  to entity  $A$ .

**Decryption:** To recover the message  $m$  from the cipher text  $c$ . Entity  $A$  must do the following:

- Obtain the cipher text  $c$  from entity  $B$
- Recover the message  $m = c^d \pmod{n}$

#### Example

**Key generation:** suppose that entity  $A$  selects the prime numbers  $p = 23$  and  $q = 71$ . Then he finds the RSA

modulus  $n = p * q = 1633$  and

$\theta(n) = (p-1)(q-1) = 1540$ . Entity  $A$  chooses  $e = 23$  and using the Baghdad method for multiplicative inverse [17] to find the decrypted key  $d = 67$  where  $e * d \equiv 1 \pmod{\theta}$ . So  $A$ 's public key is the pair  $(n = 1633, e = 23)$  while entity  $A$ 's private key is  $(\theta = 1540, d = 67)$ .

**Encryption:** Suppose entity  $B$  obtain  $A$ 's public key  $(n = 1633)$  and he determines a message  $m = 741$  to be encrypted, entity  $B$  uses repeated square and multiply algorithm [18] of modular exponentiation to compute  $c = 741^{23} \pmod{1633} = 1109$  and send this  $c = 1109$  to entity  $A$ .

**Decryption:** To recover and obtain the original message  $m$  entity  $A$  should first obtain  $c = 1109$  from entity  $B$  then recover the message  $m = c^d \pmod{n} = 1109^{67} \pmod{1633} = 741$  using repeated square and multiply algorithm [18] for exponentiation.

one line spacing above and below. Do not put text aside of them.

## 5 THE PROPOSED ATTACK ALGORITHM

In this section, we address the following question: is there a possible attack on the RSA cryptosystem other than factoring  $n$ . The answer is that yes there are few methods that attack the RSA scheme that does not involve finding the factoring of the modulus  $n$  but most of them carrying some deficiencies.

We will now prove the very interesting result that, as long as the exponent key  $e$  is known, then  $n$  can be factored in polynomial time by means of a randomized algorithm. Therefore we can say that computing this method is no easier than factoring  $n$ . However, this does not rule out the possibility of breaking the RSA cryptosystem without involving  $e$ . Notice that this result is of much more than theoretical interest.

In this paper we proposed a method that breaking the RSA scheme based on the knowing public key  $(e, n)$ . This method will work efficiently if the exponent key  $e$ . It is possible to recover the entire private exponent  $d$  and therefore factor the modulus  $n$ .

#### Algorithm

The steps of the proposed algorithm are as follows:

1. Obtain entity  $A$  public key  $(e, n)$
2. Convert the modulus  $n$  to binary bits
3. Let  $b$  represent the number of bits of  $n$
4. Compute  $d = \lceil b/4 \rceil$
5. Find  $ed \equiv 1 + k(n-s+1) \pmod{2^b}$
6. Repeat  $k$  from 1 to  $e$  until  $p^2 - s * p + n \equiv 0 \pmod{2^b}$  is true
  - a. Compute  $ed \equiv 1 + k(n-s+1) \pmod{2^d}$
  - b. Compute  $p^2 - s * p + n \equiv 0 \pmod{2^d}$
7. compute  $p_0 \equiv p \pmod{2^d}$
8. compute  $q_0 * p_0 \equiv n \pmod{2^d}$  using Baghdad inverse method
9. Compute  $\theta(n)$  as follows :
  - Compute  $n \equiv (2^d * x + p_0) * (2^d * y + q_0)$
  - Compute  $p = (2^d * x + p_0)$
  - Compute  $q = (2^d * x + q_0)$
  - $\theta(n) = (p-1)(q-1)$
10. Compute  $d = e * d - k * \theta(n) = 1$

#### Example

1. Suppose that the public key  $(e = 23, n = 1633)$
2. Convert  $n = 1633$  to binary = 11001100001
3.  $\therefore b = 11$
4.  $\therefore d = \lceil 11/4 \rceil = \lceil 2.75 \rceil = 3$
5.  $(e = 23 * d = 69) \equiv 1 + k(n = 1633 - s + 1) \pmod{2^b = 8}$ 

$$69 \equiv 1 + k(1634 - s) \pmod{8}$$

$$69 \pmod{8} = 5$$

$$5 \equiv 1 + k(1634 - s) \pmod{8}$$

$$4 \equiv k(1634 - s) \pmod{8}$$

6. For  $k = 1$  to 23 do

a.  $4 \equiv 1(1634 - s) \pmod{8}$

$$s \equiv (1634 - 4) \pmod{8}$$

$$s = 1630 \pmod{8}$$

$$s = 6$$

b.

$$p^2 - (s = 6) * p + (n = 1633) \equiv 0 \pmod{2^d = 8}$$

$$p^2 - 6p + 1633 \equiv 0 \pmod{8}$$

$$p^2 - 6p \equiv -1633 \pmod{8}$$

$$p^2 - 6p \equiv 7 \pmod{8}$$

$$7^2 - 6 * 7 \equiv 7 \pmod{8}$$

$$49 - 42 \equiv 7 \pmod{8}$$

$$7 \pmod{8} \equiv 7 \pmod{8}$$

$$\therefore p = 7$$

$$p^2 - (s = 6) * p + (n = 1633) \equiv (0 \pmod{2^b = 8})$$

is true, so stop looping

7.  $p_0 \equiv (p = 7) \pmod{2^d = 8}$

$$p_0 = 7$$

8.  $q_0 * (p_0 = 7) \equiv (n = 1633 \pmod{2^d = 8})$

$$7q_0 \equiv 1633 \pmod{8}$$

$$7q_0 \equiv 1 \pmod{8}, \text{ the inverse of } 7 \pmod{8} \text{ is } 7$$

$$q_0 \equiv 7 \pmod{8}$$

$$\therefore q_0 = 7$$

9. Compute  $\theta(n)$  as follows:

a.  $n \equiv (2^d * x + p_0) * (2^d * y + q_0)$

$$1633 \equiv (8 * x + 7)(8 * y + 7)$$

$$1633 \equiv (8 * 2 + 7)(8 * 8 + 7)$$

$$1633 \equiv (23)(71)$$

$$1633 \equiv 1633$$

$$\therefore x = 2, y = 8$$

b.  $\therefore p = 23$

c.  $\therefore q = 71$

d. So  $\theta(n) = (23 - 1)(71 - 1)$

$$= 1540$$

10.  $(e = 23 * d - (k = 1) * (\theta = 1540)) \equiv 1$

$$23d \equiv 1541$$

$\therefore d = 67$  Using Baghdad method for multiplicative inverse

## 6 DISCUSSION

In this section, we will discuss the efficiency of the suggested attack method, trying to provide a clear idea to the reader about what it would take and what the requirements should be available for this attack method to be used.

### 6.1 Input Size required

The size of input required to this suggested attack method based on input of the modulus  $n$ , and since the binary conversion in this method requires a size of  $n$  number of maximum binary number can be used, and most of the rest used loops based on the public key  $e$ . The suggested attack method will take an approximate input size of  $e + n$ .

### 6.2 Time Efficiency Required

To compute the running time of this algorithm, we need to analyze each used loop separately, finding its time efficiency function and determining its summation formula. However the total time required for this algorithm as follows:

$$T(n) = (n^2 + n) / 2 + (e^4 + 2e^3 + e^2) / 4 +$$

$$(e^2 + e) / 2 + (n^4 + 2n^2 + n^2) / 4$$

$$= (n^2 + e^2 + n + e) / 2 +$$

$$(n^4 + e^4 + 2n^3 + 2e^3 + n^2 + e^2) / 4$$

## 7 CONCLUSION

We are introduced a new algorithm for attacking RSA scheme. The new algorithm aims to obtain the private key of the RSA and then factoring the modulus based on the public key  $e$  of the RSA scheme. The new attack method is amazingly effective under certain circumstances, but rendered important with relative ease especially with large number of iterations. All to do is just to ensure that proper bounds of public key  $e$  are placed on. We claim that the proposed algorithm is more efficient than the already existed algorithms of attack since it is faster and takes less running times.

## 8 REFERENCES

- [1] Bonteh S, "Twenty Years of Attacks on the RSA Cryptosystem", Notices of the American Mathematical Society, 46(2):203-213, 1999
- [2] Thomsan D. Bruce D. Arjen L. and Mark M., "On the Factoring of RSA-120", (169), pp. 166-174, 1994
- [3] Cavallar S, Dodson B, Lenstra A, Leyland P, Lioen W, Montgomery P, Murphy B, and Zimmermann P, "Factoring of RSA-140 using the number field sieve", 1999
- [4] Eric W "Prime Factorization Algorithm", Mathworld.wolfram.com/news/ 2003
- [5] Bahr F, Boehm M, Franke J and Kleinjung T, "For the Successful Factorization of RSA-200" [www.rsasecurity.com](http://www.rsasecurity.com)
- [6] Douglas Stinson "Cryptography Theory and Practice", CRC Press, 3<sup>rd</sup> Edition, pp. 211-214,

2006

- [7] Diffie W and Hellman M, "New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22(6): 644-654, 1976
- [8] Rivest R, Shamir A and Adelman L, "A Method for Obtaining Digital Signature and Public Key Cryptosystems", Communications of the ACM, 21, pp. 120-126, 1978
- [9] Bruce S, "Applied Cryptography", 2<sup>nd</sup> John Wiley and Sons, Inc. 1996
- [10] Kaliski B.S. and Robshaw, M.J.B. "Linear Cryptanalysis Using Multiple Approximation", Advances in Cryptology-CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp.26-39.
- [11] Miller, G.L. "Riemann's Hypothesis and Tests for Primality", Journal of Computer Systems Science, vol.13, no. 3, December 1976, pp.300-317
- [12] Håstad, J. "On Using RSA with low exponent in a public key Network", Advances in Cryptology -CRYPTO '85, Springer-Verlag LNCS 218, pp. 403-408, 1986
- [13] Coppersmith, D. "Attack on the Cryptographic Scheme", Advances in Cryptology-CRYPTO '94, Springer-Verlag, LNCS 839, pp.294-307, 1994.
- [14] Tatebayashi, m., Matsuzaki. N., and Newman Jr. "Key Distribution Protocol for Digital Mobile Communication Systems", Advances in Cryptology -CRYPTO '89, Springer-Verlag LNCS 435, PP. 324-334, 1990.
- [15] Frankin, M. Haber, S, "Joint Encryption and Message Efficient Secure Computation", Advances in Cryptology-CRYPTO '93, Springer-Verlag LNCS 773, pp. 266-277, 1994
- [16] Coppersmith, D. "Another Birthday Attack", Advances in Cryptology-CRYPTO '85, Springer-Verlag, LNCS 218, PP 14-17, 1986.
- [17] Sattar Aboud, "Baghdad Method for Calculating Multiplicative Inverse", International Conference on Information Technology, Las Vegas, Nevada, USA. pp: 816-819, 2004
- [18] Lam K. and Hui L, "Efficiency of square-and-multiply exponentiation algorithms", Electronics Letters, Vol. 30, Issue 25, pp.2115- 2116, 1994