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-Hellmam [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 \( e^b \) roots mod a composite modulus \( n \). The conditions determined the modulus \( n \) and the public key \( e \) are to guarantee that for every integer \( c \in (0,1,\ldots,n-1) \) there is just one \( m \in (0,1,\ldots,n-1) \) where \( m^e = c \mod n \). 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 \((a_i \ast m + b_i)\), where \( a_i \) and \( b_i \) are known allows an adversary to decrypt the messages provided that the modulus \( n_i \) satisfy \( n_i > 2^{e(e+1)/2}\times(1+1)^e \).

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 \( \mathbb{Z}_n \), 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 retrieve \( m \) 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 massage attacks. Assuming that the factoring problem is computationally intractable and it is hard to find the prime factors of \( n = p \ast q \). 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 \( n = p \times q \).
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 \( e \times d = 1 \mod \theta(n) \).
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 \( c = m^e \mod n \).
- 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 \( m = c^d \mod n \).

**Example**

**Key generation:** suppose that entity \( A \) selects the prime numbers \( p = 23 \) and \( q = 71 \). Then he finds the RSA modulus \( n = p \times q = 1633 \) an \( \theta(n) = (p - 1)(q - 1) = 1540 \). Entity \( A \) chooses \( e = 23 \) and using the Baghdad method for multiplicative inverse [17] to find the decrypted key \( d = 67 \) where \( e \times d = 1 \mod \theta \). 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 \( B \) obtains \( A \)'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 \( c = 741^{23} \mod 1633 = 1109 \) 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 \( m = c^d \mod n = 1109^{67} \mod 1633 = 741 \) 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 \( d = [b / 4] \)
5. Find \( ed = 1 + k(n - s + 1) \mod 2^b \)
6. Repeat \( k \) from 1 to \( e \) until \( p^2 - s \times p + n = 0 \mod 2^b \) is true
   a. Compute \( ed = 1 + k(n - s + 1) \mod 2^d \)
   b. Compute \( p^2 - s \times p + n = 0 \mod 2^d \)
7. Compute \( p_0 = p \mod 2^d \)
8. Compute \( q_0 = p_0 = n \mod 2^d \)
9. Compute \( \theta(n) \) as follows:
   a. Compute \( n = (2^d \times x + p_0) \times (2^d \times y + q_0) \)
   b. Compute \( p = (2^d \times x + p_0) \)
   c. Compute \( q = (2^d \times x + q_0) \)
   d. Compute \( \theta(n) = (p - 1)(q - 1) \)
10. Compute \( d = e \times d - k \times \theta(n) = 1 \)

**Example**

1. Suppose that the public key \((e = 23, n = 1633)\)
2. Convert \( n = 1633 \) to binary \( = 11001100001 \)
3. \( \therefore : b = 11 \)
4. \( \therefore : d = [11 / 4] = [2.75] = 3 \)
5. \((e = 23 \times d = d) = 1 + k(n = 1633 - s + 1) \)
\((\mod 2^b = 8) \)
\[ 69 = 1 + k(1634 - s) \mod 8 \]
\[ 69 \mod 8 = 5 \]
6. For \( k = 1 \) to \( 23 \) do
\[
\begin{align*}
\text{a. } & \quad 4 \equiv 1 \cdot (1634 - k) \mod 8 \\
& \quad s = (1634 - 4) \mod 8 \\
& \quad s = 1630 \mod 8 \\
& \quad s = 6 \\
\text{b. } & \quad p^2 - (s = 6) \cdot p + (n = 1633) = 0 \mod (2^d = 8) \\
& \quad p^2 - 6p + 1633 = 0 \mod 8 \\
& \quad p^2 - 6p = -1633 \mod 8 \\
& \quad p^2 - 6p = 7 \mod 8 \\
& \quad 7^2 - 6 \cdot 7 = 7 \mod 8 \\
& \quad 49 - 42 = 7 \mod 8 \\
& \quad 7 \mod 8 = 7 \mod 8 \\
& \quad \therefore p = 7 \\
& \quad p^2 - (s = 6) \cdot p + (n = 1633) = 0 \mod 2^b = 8 \\
& \quad \text{is true, so stop looping}
\end{align*}
\]
8. \( q_0 \cdot (p_0 = 7) = (n = 1633 \mod 2^d = 8) \)
\[
\begin{align*}
& \quad 7q_0 = 1633 \mod 8 \\
& \quad q_0 = 7 \mod 8 \\
& \quad \therefore q_0 = 7
\end{align*}
\]
9. Compute \( \theta(n) \) as follows:
\[
\begin{align*}
\text{a. } & \quad n = (2^d \cdot x + p_0) \cdot (2^d \cdot y + q_0) \\
& \quad 1633 = (8 \cdot x + 7)(8 \cdot y + 7) \\
& \quad 1633 = (8 \cdot 2 + 7)(8 \cdot 8 + 7) \\
& \quad 1633 = (23)(71) \\
& \quad 1633 = 1633 \\
& \quad \therefore x = 2, y = 8 \\
\text{b. } & \quad \therefore p = 23 \\
\text{c. } & \quad \therefore q = 71 \\
\text{d. } & \quad \text{So } \theta(n) = (23 - 1)(71 - 1) = 1540 \\
& \quad 23d = 1541 \\
& \quad \therefore d = 67 \text{ Using Baghdad method for multiplicative inverse}
\end{align*}
\]
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:
\[
\begin{align*}
T(n) & = (n^2 + n) / 2 + (e^4 + 2e^3 + e^2) / 4 + \\
& = (e^2 + e) / 2 + (n^2 + n^2 + n^2) / 4 \\
& = (n^2 + e^2 + n + e) / 2 + \\
& = (n^4 + e^4 + 2n^3 + 2e^3 + n^2 + e^2) / 4
\end{align*}
\]

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


