AN EFFICIENT METHOD FOR FACTORING RABIN SCHEME

SATTAR J ABOUD[1], MAMOUN S. AL RABABAA [2] and MOHAMMAD A AL-FAYOUMI [1]
[1] Middle East University for Graduate Studies/Faculty of IT, Amman, Jordan
[2] Al-al Bayt University/Department of Information Systems, Amman, Jordan

ABSTRACT

The security on many public key encryption schemes relied on the intractability of finding the integer factoring problem. However, there is a great deal of research related to the RSA factoring scheme compared with the other similar schemes such as Rabin factoring algorithm. This paper will present a new technique for factoring the Rabin scheme. The suggested algorithm aims to factoring the Rabin modulus using a new idea that based on a new idea of attack. The new idea claimed to be more efficient than the well known algorithm that is Pollard rho algorithm since it is faster and takes less running time.

Keywords: *Public key cryptography, RSA scheme, Rabin scheme, integer factoring problem, Pollard rho algorithm*

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 encryption schemes are relied on [2], but surly not impossible because the RSA-120 is factored using quadratic sieve by Thomsan, Bruce, Arjen and Mark [17]. Also, the RSA-140 is factored using number field sieve by Cavallar, Dodson, Lenstra, Leyland, Lioen, Montgemery, Murphy and Zimmermann [4]. 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 [7]. The RSA-200 is factored in 2004 the RSA-640 is factored in November 2, 2005 by Bahr, Boehm, Franke and Kleinjung [1]. The factors of RSA-640 are 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].

The first attractive event in the history of public key cryptography occurred in 1976 when Diffie-Hellman [5] published their paper named new direction in cryptography. This paper suggested a great idea for public key cryptography and to construct a scheme that is not need a secure channel, but provides the opportunity for secret communication. However, Diffie-Hellman suggested such mechanism for distributing the private key to be employed in the traditional schemes on insecure communication channel [3]. In 1978 Rivest, Shamir and Adleman (RSA) [13] introduced the first practical scheme which is the most popular public key scheme. The security of the RSA scheme is based on the intractability of factoring the modulus which is the product of two large prime numbers that is a difficult mathematical problem to solve. In 1979, Rabin [12] suggested a scheme also relied on the factoring of a composite modulus, which is the product of large $3 \bmod 4$ prime numbers and the result of decryption scheme is four messages; just one from them is the original message. In 1992, Shimada [16] enhanced Rabin scheme using the extension Rabin public key encryption scheme employing certain assumption in a private key utilizing Jacobi symbol. In 1998, Okamoto [9] proposed a new public key cryptosystem as secure as factoring relied on RSA and Rabin schemes. In 1999, Pointcheval [10] presented a new public key encryption scheme based on the dependent RSA and Rabin Schemes. In 2006, Sahadeo Padhye [14] modified dependent RSA and Rabin public key cryptosystem using certain conditions to public and private keys.

All of the schemes mentioned above relied on intractability of the integer factoring. However, there is great research concerning RSA factoring modulus compared with the other mentioned schemes such as Rabin scheme. Therefore, in this paper we suggest an efficient algorithm to factorize the Rabin scheme. Through define a functional problem of attack.

2. RABIN SCHEME

In 1979, Rabin [12] developed a public key cryptosystem that is based on the difficulty of computing square roots mod some integer n. Rabin 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 $n = p * q$. Rabin scheme is a

good alternative to the RSA scheme, though both depend on the difficulty of integer. The Rabin scheme is as follows:

KEY GENERATION ALGORITHM

To generate the keys entity A should do the following:

1. Randomly chooses two large prime numbers p and q which satisfy $p \equiv q \equiv 3 \mod 4$.
2. Computes the modulus $n = p * q$.
3. Determine entity A public and private key. The pair (p, q) is the private key. While the modulus n 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 public key n.
- Represent the message m as an integer in the interval $[0...n-1]$
- Compute $c = m^2 \mod n$
- 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:

- Compute the four square roots m_1, m_2, m_3, m_4 of $c \mod n$ as follows:
  - $w_1 = c^{(p+1)/4} \mod p$
  - $w_2 = p - w_1$
  - $w_3 = c^{(q+1)/4} \mod q$
  - $w_4 = q - w_3$
- Compute $a = q(q^{-1} \mod p)$
- Compute $b = p(p^{-1} \mod q)$
- Compute four solutions m_1, m_2, m_3, m_4 as follows
  - $m_1 = (a * w_1 + b * w_3) \mod n$
  - $m_2 = (a * w_1 + b * w_4) \mod n$
  - $m_3 = (a * w_2 + b * w_3) \mod n$
  - $m_4 = (a * w_2 + b * w_4) \mod n$

Note that one from these solutions is the result

This shows that Rabin scheme is not injective method. Specifically, as n is the product of two prime numbers, each encrypted message c holds four square roots $\mod n$. As a result Rabin scheme has the drawback that decryption gives not just the original message but also three more square roots of c that expectantly are adequately insignificant so can be ignored. Otherwise, there is one way for entity A to know the original message from these three wrong results via add to the original message m a special redundancy value by which recognizing the original message m .For instance, entity A can repeat a particular block of message for example appends to an original message m the last 64 bits. In this situation the evidence that breaking the Rabin scheme is computationally identical to the RSA scheme. Actually, there is no obvious method that uses the secret key (p, q) for breaking Rabin scheme. Generally, calculating square roots mod certain integer number via unidentified prime factors is the only way to use to attack the Rabin scheme and counted as a difficult problem. The advantage of the suggested factoring algorithm is to use a functional problem to attack the Rabin scheme and reach its secret key (p, q) .

EXAMPLE

Key generation: suppose that entity A selects the prime numbers $p = 43$ and $q = 47$ with $43 \equiv 47 \equiv 3 \mod 4$. Then he finds the Rabin modulus $n = p * q = 2021$. $A's$ public key is $(n = 2021)$ while $A's$ private key is $(p = 43, q = 47)$.

Encryption: Suppose entity B obtain $A's$ public key $(n = 2021)$ and he determines a message $m = 741$ to be encrypted and finds $c = 741^2 \mod 2021$ then send $c = 1390$ to entity A.

Decryption: To recover and obtain the original message m entity A should first compute the four square roots w_1, w_2, w_3, w_4 using square and multiply method [8]:

$w_1 = 1390^{(43+1)/4} = 1390^{11} \mod 43 = 10$

$w_2 = 43 - 10 = 33$

$w_3 = 1390^{(47+1)/4} = 1390^{12} \mod 47 = 36$

$w_4 = 47 - 36 = 11$

Entity A then computes $a = 47(47^{-1} \mod 43) = 11 * 47 = 517$ and $b = 43(43^{-1} \mod 47) = 35*43 = 1505$ using Baghdad method for multiplicative inverse [15] then entity A computes four solutions as follows:

$m_1 = (517 * 10 + 1505 * 36) \mod 2021 = 741$

$m_2 = (517 * 10 + 1505 * 11) \mod 2021 = 1515$

$m_3 = (517 * 33 + 1505 * 36) \mod 2021 = 506$

$m_4 = (517 * 33 + 1505 * 11) \mod 2021 = 1280$

Note that only m_1 is represented the original message m.

3. POLLARD RHO FACTORING METHOD

Prior to describe the proposed factoring algorithm, we will briefly discuss one of the most important special purpose factoring methods that is Pollard rho method. Then compare its results with the results of the suggested method.

This method is based on a combination of two ideas that are also useful for various other factoring methods [11]. The first idea is the well known birthday paradax which is a group of at least 23 randomly selected people contains two persons with the same birthday in more than 50% of the cases. More generally if numbers are picked at random from a set containing p numbers, the probability of picking the same number twice exceeds 50% after $1.117\sqrt{p}$ numbers have been picked. The second idea is the following if p is some unknown divisor of n, x and y are two integers that are suspected to be identical mod p, that is $x \equiv y \mod p$, then this can be checked by computing $\gcd(|x - y|, n)$, more highly this computation may reveal a factorization of n unless x and y are also identical mod n .This method presented as algorithm which has three inputs that are the odd integer n to be factored and pre-specified integers $a = b = 2$. The Pollard rho algorithm is as follows:

ALGORITHM

set $a = b = 2$;

for $i = 1,2,\ldots$ *do*
$a = a^2 + 1 \bmod n;$
$b = b^2 + 1 \bmod n;$
$b = b^2 + 1 \bmod n;$
$d = \gcd(a - b, n);$
if 1 < d < n then return d and terminate with success
if d = n then terminate the algorithm with failure
end .

EXAMPLE

Pollard rho algorithm for finding a non-trivial factor of $n = 455459$. The following table lists the values of variables a, b and d at the end of each an iteration of step for loop of algorithm.

a	b	d
5	26	1
26	2871	1
677	179685	1
2871	155260	1
44380	416250	1
179685	43670	1
121634	164403	1
155260	247944	1
44567	68343	743

Hence two non-trivial factors of 455459 are 743 and 455459/743=613.

4. THE PROPOSED FACTORING ALGORITHM

Suppose that entity T is able to factor the Rabin modulus n. Thus entity T get entity A secret key and can decrypt every message sent to him. Specifically, attacking the Rabin scheme is not difficult than solving the factoring modulus. Equally, we illustrate that factoring modulus is not difficult than attacking the Rabin system, thus these are identically hard problems. So Rabin scheme has an evidence of intractability that is relied on the hypothesis where factoring is computationally hard to solve. In this respect, Douglas Stinson [6] mentioned that Rabin scheme is better compared to other public key encryption schemes such as RSA and Elgamal schemes. However, in this paper we will introduce a new algorithm that can factor the Rabin modulus. The proposed algorithm is more efficient compared with the well known algorithm Pollard raho algorithm regarding the time complexity and the number of iterations to catch the target.

Suppose $n = p * q$ is the Rabin modulus to be factored, such that $p \equiv q \equiv 3 \bmod 4$. The following are the steps of the suggested algorithm that break the Rabin modulus.

Algorithm

var
n, x, j, y, z : int;
ok : *boolean* ;
begin
$z = \lfloor \sqrt{n} \rfloor$;
if z is odd then
$x = (n - z * 2) + 1;$
else
$x = (n - z * 2);$
$ok = true$;
while ok & $x > (z * 2)$*do*
{
$j = n - x + 1;$
$y = j / 2;$
if $(\sqrt{y^2 - n} = \sqrt{y^2 - n})$ *then*
$ok = false;$
else
$x = x - 2;$
}
return(x);
end.

EXAMPLE

Suppose that the Rabin modulus $n = 455459$ where $p \equiv q \equiv 3 \bmod 4$, $z = \lfloor \sqrt{n} \rfloor = 675$ as long as z *is odd* , then we compute $x = (n - z * 2) + 1 = 454110$. Now, we can trace the rest of the algorithm as follows:

n	z	x	j	y	r
455459	675	454110	-	-	-
			1348	675	fraction
		454108	1350	676	fraction
		454106	1352	677	fraction
		454104	1354	678	integer=65

Thus $y - r = p$ or q
$678 - 65 = 613 = p$
$\therefore 455459 / 613 = 743$

5. CONCLUSIONS

We are introduced a new algorithm for factoring the Rabin scheme based on the definition of the Blum integers and on a functional problem of attack scheme. We find that the definition of the Blum integers is a great contribution to attacking the Rabin scheme. Also, we find that the definition of the Blum numbers will open many other ways to attack not only the Rabin scheme but also other schemes based on the difficulty of integer factoring. The suggested algorithm is one from these. We claim that the proposed algorithm is more efficient than the well known algorithm that is Pollard rho algorithm even with long modulus.

References

[1] Bahr F, Boehm M, Franke J and Kleinjung T, "For the Successful Factorization of RSA-200" www.rsasecurity.com
[2] Bonteh S, "Twenty Years of Attacks on the RSA Cryptosystem", Notices of the American Mathematical Society, 46(2):203-213, 1999
[3] Bruce S, "Applied Cryptography", 2nd John Wiley and Sons, Inc. 1996
[4] Cavallar S, Dodson B, Lenstra A, Leyland P, Lioen

W, Montgemery P, Murphy B, and Zimmermann P, "Factoring of RSA-140 using the number field sieve", 1999

[5] Diffie W and Hellman M, "New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22(6): 644-654, 1976

[6] Douglas Stinson "Cryptography Theory and Practice", CRC Press, 3rd Edition, pp. 211-214, 2006

[7] Eric W "Prime Factorization Algorithm", Mathworld.woiframe.com/news/ 2003

[8] Lam K. and Hui L, "Efficiency of square-and-multiply exponentiation algorithms", Electronics Letters, Vol. 30, Issue 25, pp.2115- 2116, 1994

[9] Okamoto T and Uchiyama S "A New Public Key Cryptosystem as Secure as Factoring", in Proceedings of Europcrypt'98, LNCS 1403, Springer Verlag, pp.308-318, 1998

[10] Pointcheval D "New Public Key Cryptosystem Based on the Dependent-RSA Problem", in proceedings of Euorcrypt'99, LNCS 1592, Springer Verlag, pp. 239-254, 1999.

[11] Pollard J. "A Monte Carlo Method for Factorization", BIT, Vol. 15,, pp. 331-334, 1975

[12] Rabin, M. "Digitalized signature and Public Key Functions as intractable as factorization", Technical Report, MIT/ LCS/ Tr, MIT Lab. Computer Science, Cambridge, Jan. 1979.

[13] 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

[14] Sahadeo Padhye, "On DRSA Public Key Cryptosystem", the International Arab Journal of Information Technology, Volume 3, No. 4, October, PP. 334-336, 2006

[15] Sattar Aboud, "Baghdad Method for Calculating Multiplicative Inverse", International Conference on Information Technology, Las Vegas, Nevada, USA. pp: 816-819, 2004

[16] Shimada M "Another Practical Public Key Cryptosystem", Electronic Letters, 5th November, Vol. 28, No. 23, 1992

[17] Thomsan D. Bruce D. Arjen L. and Mark M., "On the Factoring of RSA-120", (169), pp. 166-174, 1994