Malaya J. Mat. 3(4)(2015) 419–422

Malaya Journal of Matematik
www.malayajournal.org

MJM
an international journal of mathematical sciences with computer applications...

ISSN : 2319-3786

A new public key encryption scheme based on two cryptographic assumptions

Pinkimani Goswami[a,*], Madan Mohan Singh[b] and Bubu Bhuyan[c]

[a]Department of Mathematics, North-Eastern Hill University, Shillong-793022, India.

[b]Department of Basic Sciences and Social Sciences, North-Eastern Hill University, Shillong-793022, India.

[c]Department of Information Technology, North-Eastern Hill University, Shillong-793022, India.

Abstract

In this paper we present a new cryptosystem which is a combination of RSA variant namely rebalanced RSA-CRT and general formulation of DGDLP. Its security is depend upon integer factorization problem and general formulation of DGDLP.

Keywords: public key cryptography, integer factorization problem, discrete logarithm problem, generalized discrete logarithm problem, cryptosystem.

2010 MSC: 94A60.

1 Introduction

The public key cryptography has a major advantage over the symmetric key cryptography. In symmetric key cryptography, a prior communication of secret key is required. The public key cryptography eliminate the necessity of sharing secret key. It has own public key which is known by everybody and has corresponding private key which is known only by the intended recipient. The public key cryptography is based on one-way trapdoor function, where the encryption rule is easy to compute, but decryption rule is computationally infeasible without any additional information. Thus the security of public key cryptosystem are based on the intractability of hard mathematical problems such as integer factorization problem, discrete logarithm problem etc.

Up to now, most of the public key schemes are based on one cryptographic assumption. Although these schemes are secure but it is possible that in future efficient algorithms will be developed to break these assumptions. To enhance security is the major motivation for developing cryptosystems based on multiple cryptographic assumptions, since it is very unlikely that these assumptions would simultaneously become easy to solve. In 1988, K. S. McCurley [7] proposed the first key distribution scheme based on two hard dissimilar assumptions. The scheme is modification of ElGamal cryptosystem. Instated of using an arithmetic modulus a prime p, he used a modulus n that is a product of two primes. To break the scheme requires the prime factorization of n and ability to solve DLP. In [6], L.Harn proposed a cryptosystem based on two cryptographic assumption. To break the cryptosystem requires to solve simultaneously a Diffie-Hellman problem in a subgroup of $\mathbb{Z}_p^*$, where p is a large prime such that $p = 2p' \times q' + 1$ and p', q' are large primes which are part of the private key, and to factor $(p-1)/2$. After that many public key schemes was developed which are based on two cryptographic assumptions (for example [9], [4], [5] etc).

By this motivation, we proposed a public key scheme whose security is based on RSA variant namely rebalanced RSA-CRT [3] and generalization of GDLP. Rebalanced RSA-CRT is a variant of RSA that enables

*Corresponding author.
E-mail address: pinkimanigoswami@yahoo.com (Pinkimani Goswami), mmsingh2004@gmail.com (Madan Mohan Singh), b.bhuyan@gmail.com (Bubu Bhuyan)

us to rebalanced the difficulty of encryption and decryption. It speed up the RSA decryption procedure. Generalization of GDLP stated that given a finite group of order n and elements $\alpha, \gamma \in G$, find an integer x modulo n such that $\alpha^x = \gamma$, provided that such an integer exists. In this formulation, it is not required that G be a cyclic group, and even it is, it is not required to consider generator of the group. Since α is not generator of the group so α^x is not unique, which makes the problem harder to solve than GDLP [8], [4]. In this proposed scheme, an attacker has to solve simultaneously two generalized GDLP (we call it generalization of DGDLP or general formulation of DGDLP) and IFP. One advantage of this scheme is that it include non-cyclic groups. Another advantage is that because of the use of Chinese remainder theorem (CRT), decryption process of the proposed cryptosystem is fast.

The remainder of this paper is organized as follows. In section 2, we present our cryptosystem. Section 3 is devoted to security of the proposed cryptosystem and in section 4 we deal with its performance. Section 5 is the conclusion of the paper. Throughout the paper all notations are usual. For example the multiplicative group of $\mathbb{Z}_n$ is denoted by $\mathbb{Z}_n^*$, the Eular's phi function of n is denoted by $\phi(n)$ etc.

2 The proposed public key cryptosystem

In this section we present our public key cryptosystem.

Public and private key generation:

A user $\mathcal{A}$, who wants to create a public and private key, have to do the following steps:

1. Choose two large prime p and q of almost same size such that $(p-1, q-1) = 2$.
2. Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$.
3. Choose two integer d_p and d_q such that $(d_p, p-1) = 1$, $(d_q, q-1) = 1$ and $d_p \equiv d_q \ (mod\ 2)$.
4. Find d such that $d \equiv d_p \ (mod\ p-1)$ and $d \equiv d_q \ (mod\ q-1)$.
5. Compute $e \equiv d^{-1} \ (mod\ \phi(n))$.
6. Choose a, b such that $0 \leq a, b \leq \phi(n) - 1$.
7. Choose $\alpha, \beta \in \mathbb{Z}_n^*$ and compute $y_1 \equiv \alpha^a \ (mod\ n)$ and $y_2 \equiv \beta^b \ (mod\ n)$

The public key of $\mathcal{A}$ is (n, e, y_1, y_2) and the corresponding private key is $(a, b, \alpha, \beta, d_p, d_q)$.

Encryption:

The plaintext space is $\mathbb{Z}_n$. Suppose that another user $\mathcal{B}$ want to send a message $m \in \mathbb{Z}_n$ to $\mathcal{A}$ using $\mathcal{A}$'s public key. $\mathcal{B}$ have to do the following step:

1. Compute $c \equiv (my_1y_2)^e \ (mod\ n)$

$\mathcal{B}$ send to $\mathcal{A}$ the encrypted message c.

Decryption:

For the decryption of the message c, $\mathcal{A}$ should do the following steps:

1. Compute $d_1 \equiv \alpha^{\phi(n)-a} \ (mod\ n) \equiv \alpha^{-a} \ (mod\ n)$ and calculate $d_1^e \ (mod\ n)$.
2. Compute $d_2 \equiv \alpha^{\phi(n)-b} \ (mod\ n) \equiv \alpha^{-b} \ (mod\ n)$ and calculate $d_2^e \ (mod\ n)$.
3. Compute $M_p \equiv (d_1^e d_2^e c)^{d_p} \ (mod\ p)$ and $M_q \equiv (d_1^e d_2^e c)^{d_q} \ (mod\ q)$.
4. Then using CRT, $\mathcal{A}$ recover the plaintext m.

3 Security

The security of this proposed cryptosystem is based on factoring and discrete logarithm problem. A third party who intercepts the encrypt message c can recover m, by finding the primes factors p and q of n and so d and next by finding a and b from $y_1 \equiv \alpha^a \pmod n$ and $y_2 \equiv \beta^b \pmod n$ where α and β both are unknown. That is to break this scheme the attacker has to compute prime factorization of n and ability to solve DLP. The best way to factorized $n = pq$ is by using the number field sieve method. This method is just depend on the size of n and it is computationally infeasible to factor an integer of size 1024 bits and above. We consider the primes p and q in such a way that they resist factorization attack. Also, both d_p and d_q are atleast 160 bits long to prevent the attack proposed in [3]. Since d is large so it prevent the small-d attacks [2, 10]. The primes p and q are consider in such a way that DLP is intractable. To find a and b, a third party need to solve two generalization of GDLP (we called it general formulation of DGDLP or generalized DGDLP). The general formulation of DGDLP does not require that the multiplicative group $\mathbb{Z}_n^*$ be a cyclic group, and so, it is not required that α and β be generators of the group. Therefore the values of power of α and β are not unique and hence this problem is harder to solve than GDLP. As α and β are not public so it makes the problem more harder to solve in general.

Note that if an attacker finds easily a method to compute d or factoring n, then he has still to solve general formulation of DGDLP. Alternatively, if the attacker can easily solve the general formulation of DGDLP, then he also has to compute d by factoring n. Thus, in any case an attacker has to solve two hard problem.

Also, if $a = 0 = b$ then $y_1 = 0 = y_2$ and so Rebalanced RSA-CRT cryptosystem is a special case of the proposed cryptosystem. Hence if there is an oracle that can break the proposed cryptosystem then the oracle can break Rebalanced RSA-CRT. So, the proposed cryptosystem is atleast as secure as Rebalanced RSA-CRT.

4 Performance analysis

The encryption algorithm for our scheme requires two modular multiplications and one modular exponentiation. One modular multiplication can be done in advance. Thus, the encryption requires only one modular multiplication and one modular exponentiation. The decryption algorithm required four modular exponentiation viz. d_1^e, d_2^e, $(d_1^e d_2^e c)^{d_p}$ and $(d_1^e d_2^e c)^{d_q}$, two modular multiplication viz. $d_1^e d_2^e$ and $d_1^e d_2^e c$ and two applications of extended Euclidean algorithm for computation of $(\alpha^a)^{-1}$, $(\beta^b)^{-1}$ mod n. Thus the decryption algorithm required one modular multiplication viz. $d_1^e d_2^e c$ and two modular exponentiation viz. $(d_1^e d_2^e c)^{d_p}$ and $(d_1^e d_2^e c)^{d_q}$ and others can be done in advance. Hence, the encryption scheme is as efficient as the encryption scheme described in section iv of [5], if both the schemes have same e. Since e is large so encryption take more time than [5]. Since d_p and d_q are small so decryption scheme is fast compare to the decryption scheme in [5]. Also, plain-text and cipher-text is of same length.

5 Conclusion

In this paper we have proposed a public key cryptosystem which is based on rebalance RSA-CRT and general formulation DGDLP. Decryption of the proposed cryptosystem is faster than decryption of [5]. The proposed scheme is more secure than rebalanced RSA-CRT.

References

[1] D. Boneh and G. Durfee, New results on cryptanalysis of low private exponent RSA, *Preprint*, (1998), 1–18.

[2] D. Boneh and G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, *IEEE Trans. Information Theory*, 46(4) (2000) 1339-1349.

[3] D. Boneh and H. Shacham, Fast variants of RSA, *CryptoBytes*, 5(1) (2002), 1–9.

[4] H. Elkamchouchi, K. Elshenawy and Heba. A. Shaban, Two new public key techniques in the domain of Gaussian integers, *Twenteith National radio science conference(NRSC2003). In: Proceedings of Twenteith national*, C17 (2003), 1–8.

[5] H. M. Elkamchouchi, M. E. Nasr and R. Esmail, New public key techniques based on double discrete logarithm problem, 21st *National radio science conference(NRSC2004). In: Proceeding of Twenty-First national*, C23 (2004), 1–9.

[6] L. Harn, Public-key cryptography design based on factoring and discrete logarithms, *IEEE Proceedings*, 141 : 3 (1994) 193-195.

[7] K. S. McCureley, A key distribution system equivalent to factoring, *Journal of Cryptography*, 1 : 2 (1988) 95-106.

[8] A. J. Menezes, P. C. Van O orshot and S. A. Vnstone, Handbook of Applied Cryptography, *CRC Press*, 1996.

[9] D. Poulakis, A public key encryption scheme based on factoring and discrete logarithm, *Journal of Discrete Mathematical Sciences and Cryptography*, 12(6) (2009) 745–752.

[10] M. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Trans. Information Theory*, 36(3) (1990) 553-558.

Received: July 27, 2015; *Accepted*: August 23, 2015