ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Public Key Cryptosystem based on IFP and DLP

Chandrashekhar Meshram*
Department of Applied Mathematics
Shri Shankaracharya Engineering College, Junwani
Bhilai (C.G.), India
cs_meshram@rediffmail.com

S.A.Meshram
Department of Mathematics
R.T.M.Nagpur University
Nagpur (M.S.) India
meshram_sa2011@in.com

Abstract: Design the most existing cryptosystem incorporate just one cryptographic assumption, such as integer factorization problem or discrete logarithms. These assumptions appear secure today; but, it is possible that efficient algorithms will be developed in the future lo break one or more of these assumptions. It is very unlikely that multiple cryptographic assumptions would simultaneously become easy to solve. Enhancing security is the major objective for cryptosystems based on multiple assumptions. K.S. McCauley [12] proposed the first key distribution system based on two dissimilar assumptions, both of which appear to be hard. In his design, the sizes of the security parameters for these two assumptions are quite different. The modulus to satisfy the proper security requirement for one assumption is too large for the other assumption. The side effects are (1) the public key size is larger than the original Dime-Hellman key distribution scheme; and (2) more computation time is required. In the paper, public key encryption scheme is designed which is based on two problems namely integer factorization problem and Discrete Logarithm problem with double exponent. The adversary has to solve the two problems simultaneously in order to recover a corresponding plaintext from the received cipher text. Therefore, this scheme is expected to gain a higher level of security .we next show that, the newly developed scheme is efficient with respect to encryption and decryption since it requires only minimal operations in both algorithms.

Keywords: Public Key Cryptosystem, Integer Factorization Problem (IFP), Discrete Logarithm Problem (DLP).

I. INTRODAUCTION

In 1976 Diffie and Hellman [1] proposed the concept of the public-key cryptosystem to solve the secret communication key distribution problem. Since then several public-key cryptosystems [3-5] which can provide both digital signature and encryption have been proposed. One common feature among all these systems is that the security of each cryptosystem is based on just one cryptographic assumption, such as integer factorization problem or discrete logarithms.

According to [6], the solution of the discrete logarithm requires $0\{\exp[\text{const.}\sqrt{(\log p \log\log p)}]\}$ integer multiplication, where p is the modulus. For more information on computing discrete logarithms [see (7-8)]. According to [9], the asymptotic running times for many integers factorization algorithms are given in the form of $0\{\exp[\text{const.}\sqrt{(\log n \log\log n)}]\}$, where n is the product of two large primes. For more information on factoring [see (10-11)].

Recent advanced techniques imply that the computational difficulties of these two assumptions are almost the same. Thus, in order to achieve the same security level for these two different assumptions, the size of the modulus p for the discrete logarithm problem and the size of modulus n for the factoring problem should be the same.

Although these cryptographic assumptions appear secure today, it is still very likely in the future that a clever cryptanalyst will discover an efficient way to factor integers or to compute discrete logarithms. Thus, cryptosystems based on the corresponding assumption will surrender their security. To enhance security is the major motivation for developing cryptosystems based on multiple cryptographic assumptions.

This is because of the common belief that it is very unlikely that multiple cryptographic assumptions would simultaneously become easy to solve.

In 1988 K.S. McCurley [12] proposed the first key distribution system based on two dissimilar assumptions, both of which appear to be hard. Instead of using arithmetic modulo p that is a prime (as in the Diffie- Hellman key distribution scheme), the distribution scheme [12] in uses a modulus n that is a product of two primes. Breaking the system requires the factoring of n into two primes, p and q, and the ability to solve the Diffie-Hellman discrete logarithm problem in subgroups of Z_p^* and Z_q^*. Thus, it is impossible to select proper modulo p and q to achieve the same difficulty for these two assumptions. In 1992 E.F. Brickell and K.S.

McCurley [13] proposed an interactive identification scheme also based on discrete logarithms and integer factorization problem, but these two assumptions are not as general as the two assumptions stated previously. In 1994 L.Harn [2] develops a cryptosystem based on two different cryptographic assumptions integer factoring and discrete logarithm problem and enhances the security of that cryptosystem.

In this paper, we design a new public key encryption scheme based on integer factorization problem and discrete logarithm problem with double distinct exponent to enhance the security of this public key cryptosystem.

II. THE PUBLIC KEY ENCRYPTION BASED ON INTEGER FACTORIZATION PROBLEM AND DISCRETE LOGARITHM PROBLEM

In this section, we introduce some notation and parameters, which will be used throughout this paper:

Two large prime numbers p and q are safe primes and set $n = pq$ .one may use method in [15] to generate strong random primes. A function $\varphi(n)=(p-1)(q-1)$ is a phi–Euler function and two integers g_1 and g_2 are primitive's elements in Z_n^* with order n satisfying $g_1^{n-1}\equiv 1(\mathrm{mod}\, n)$ and $g_2^{n-1}\equiv 1(\mathrm{mod}\, n)$.

The algorithm consists of three sub algorithm, Key generation, Encryption and Decryption

A. Key Generation:

The key generation algorithm runs as follows (entity A should do the following)

a. Pick random an integer $e, 1\le e\le\varphi(n)$ from $Z_{\varphi(n)}^*$ such that gcd $(e,\varphi(n))=1$.

b. Select two random integer a and b such that $2\le ab\le\varphi(n)-1$ (with no upper bounds).

c. Compute $y_1=g_1^a(\mathrm{mod}\, n)$ and $y_2=g_2^b(\mathrm{mod}\, n)$.

d. Use the extended Euclidean algorithm to compute the unique integer $d, 1\le d\le\varphi(n)$ such that $ed\equiv 1(\mathrm{mod}\, n)$.

The public key is formed by (n,e,y_1,y_2) and the corresponding private key is given by (d,a,b).

B. Encryption:

An entity B to encrypt a message m to entity A should do the following:

a. Obtain public key (n,e,y_1,y_2).

b. Represented the message $m\in[1,n]$

c. Select two random integer i and j such that $2\le ij\le\varphi(n)-1$ (with no upper bounds)

d. Compute $\alpha_1=g_1^i(\mathrm{mod}\, n)$ and $\alpha_2=g_2^j(\mathrm{mod}\, n)$.

e. Compute $\beta=m(y_1)^i(y_2)^j(\mathrm{mod}\, n)$.

f. Compute $C_1=\alpha_1^e(\mathrm{mod}\, n)$, $C_2=\alpha_2^e(\mathrm{mod}\, n)$ and $\gamma=\beta^e(\mathrm{mod}\, n)$.

The cipher text is given by $C=(C_1,C_2,\gamma)$.

C. Decryption:

To recover the plaintext m from the cipher text C, entity A should do the following:

a. Compute $C_1^{\varphi(n)-a}(\mathrm{mod}\, n)=C_1^{-a}(\mathrm{mod}\, n)$ and $C_2^{\varphi(n)-b}(\mathrm{mod}\, n)=C_2^{-b}(\mathrm{mod}\, n)$.

b. Recover the plaintext m by compute $(C_1^{-a},C_2^{-b},\gamma)^d(\mathrm{mod}\, n)$.

III. CONSISTENCY OF THE ALGORITHM

In Encryption:

$$\alpha_1=g_1^i(\mathrm{mod}\, n) \text{ and } \alpha_2=g_2^j(\mathrm{mod}\, n)$$

$$\beta=m(y_1)^i(y_2)^j(\mathrm{mod}\, n)$$

$$C_1=\alpha_1^e(\mathrm{mod}\, n)=(g_1^i)^e(\mathrm{mod}\, n)=(g_1^{ie})(\mathrm{mod}\, n)$$

$$C_2=\alpha_2^e(\mathrm{mod}\, n)=(g_2^j)^e(\mathrm{mod}\, n)=(g_2^{je})(\mathrm{mod}\, n)$$

$$\gamma=\beta^e(\mathrm{mod}\, n)=[m(y_1)^i(y_2)^j]^e(\mathrm{mod}\, n)$$

In Decryption:

$$C_1^{\varphi(n)-a}(\mathrm{mod}\, n)=C_1^{-a}(\mathrm{mod}\, n)=y_1^{-ie}(\mathrm{mod}\, n)$$

$$C_2^{\varphi(n)-b}(\mathrm{mod}\, n)=C_2^{-b}(\mathrm{mod}\, n)=y_2^{-je}(\mathrm{mod}\, n)$$

$$(C_1^{-a},C_2^{-b},\gamma)^d(\mathrm{mod}\, n)$$

$$=[y_1^{-ie}y_2^{-je}m^e y_1^{ie}y_2^{je}]^d(\mathrm{mod}\, n)$$

$$=m^{ed}(\mathrm{mod}\, n)$$

$$= m(\mathrm{mod}\, n)$$

IV. EXAMPLE

To make our construction easy to comprehend, we illustrate an example to show the basic principle of our scheme. However, practitioners are not recommended to choose such keys or parameters in practice since inappropriate parameters will make this scheme vulnerable to attacks.

Let the two primes be $p=29$ and $q=43$ and set $n=1247$ and $\varphi(n)=1176$.

A. Key Generation:

The key generation algorithm runs as follows (entity A should do the following)

a. Select number $e=11$ and $\gcd(11,1176)=1$.

b. Select two integers $a=19$ and $b=17$.

c. Compute $y_1=31^{19}(\mathrm{mod}\, 1247)=1012$ and $y_2=41^{17}(\mathrm{mod}\, 1247)=766$.

d. Use the extended Euclidean algorithm to compute the unique integer $d=107$, $1\le d\le\varphi(n)$ such that $11d\equiv 1(\mathrm{mod}1176)$.

The public key is formed by (n,e,y_1,y_2) and the corresponding private key is given by (d,a,b).

B. The Encryption:

a. To encrypt a message $m=1122$ A person B
b. Select two random integer i and j such that $2\le ij\le\varphi(n)-1$ .Where $i=21$ and $j=51$
c. Compute $\alpha_1=1119$ and. $\alpha_2=133$.
d. Compute $\beta=600$.
e. Compute $C_1=302$, $C_2=41$ and $\gamma=600$.

The cipher text is given by $C=(C_1,C_2,\gamma)$.

C. The Decryption:

a. A should Compute

$C_1^{\varphi(n)-a}(\mathrm{mod}\,n)=C_1^{-a}(\mathrm{mod}\,n)=302$,

$C_2^{\varphi(n)-b}(\mathrm{mod}\,n)=C_2^{-b}(\mathrm{mod}\,n)=1177$.

b. Recover the plaintext m by computing

$(C_1^{-a},C_2^{-b},\gamma)^d(\mathrm{mod}\,n)=1122$

c. Return the value of $m=1122$.

V. SECURITY ANALYSIS

In this section, we shall show three possible attacks by which an adversary may try to take down the new encryption scheme. For each attack, we define the attack and give reason why this attack could be failed.

A. Direct Attack:

An attacker wishes to obtain all secrete keys using all information available from the system. In this case, an attacker needs to solve factoring and discrete logarithm problem with double distinct discrete exponent. The best way to factorize $n=pq$ is by using the number field sieve method (NFS) [16].but this method is just dependent on the size of modulus . It is computationally infeasible to factor a 1024-bit integer and to increase the security of our scheme; we should select strong primes [17] to avid attacks using special purpose factorization algorithms. To maintain the same security level for discrete logarithm problem with double distinct discrete exponent, one must uses $n=pq$ with $(p-1/2)$ and $(q-1/2)$ respectively is product of two 512-bit primes.

B. Factoring Attack:

Assume that the attacker successfully solves the factoring problem so that he knows secrete d .Thus he may obtain $(C_1^{-a},C_2^{-b},\gamma)^d(\mathrm{mod}\,n)=m^{ed}(\mathrm{mod}\,n)$.

Unfortunately, at this stage he still does not knows secrete a and b . Also he cannot exact act the plaintext m from the above expression.

C. Discrete log Attack:

An attacker should solve a discrete logarithm problem twice to obtain the private key given the public as following:

(A). In this encryption the public key is given by (n,e,y_1,y_2) and the corresponding secret key is given by (d,a,b).

To obtain the private key (a) he should solve the DLP

$$a\equiv\log_{g_1}y_1(\mathrm{mod}\,n)$$

To obtain the private key (b) he should solve the DLP

$$b\equiv\log_{g_2}y_2(\mathrm{mod}\,n)$$

This information is equivalent to computing the discrete logarithm problem over multiplicative cyclic group Z_n^* and corresponding secrete key a and b will never be revealed to the public.

(B). Say that attacker is able to obtain the secret integer i and j from solve the DLP as $u\equiv\log_{g_1}\alpha_1(\mathrm{mod}\,n)$ and $v\equiv\log_{g_2}\alpha_2(\mathrm{mod}\,n)$. He could derive the plaintext m if and only if he manages to get $(C_1^{-a},C_2^{-b},\gamma)^d(\mathrm{mod}\,n)$.

VI. CONCLUSION

In this present paper, we design a public key cryptosystem scheme based on integer factorization problem and discrete logarithm problem with double exponent. This scheme definitely provides a new scheme with a longer and higher level of security than that based on two distinct hard problem as integer factorization problem and discrete logarithm problem to enhance the security of the system. In other words, one must break of two integer factorization problem and discrete logarithm problem, systems simultaneously to break our system. We also show that the performance of the scheme, requires minimal operation in encryption and decryption, which makes it is very efficient. Some possible attacks have considered and show that the scheme is secure from those attacks.

VII. REFERENCES

[1] W.Diffie and M.E.Hellman, "New directions in cryptography", IEEE Trans., 1976, Vol. IT-22, pp. 644-654.

[2] L. Harn "Public key cryptosystem design based on factoring and discrete logarithm" IEEE Pro.Comput.Digit.Tech. 1984, Vol. 141(3),pp.193-195.

[3] R.L.Rivest, A.Sihamir and L. Adelman, "A method for obtaining digital signatures and public-key cryptosystem" Commun. ACM, 1978, Vol.21, (2), pp. 120-126.

[4] T.Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms" IEEE Trans., 1985, Vol.IT-31, pp. 469-472.

[5] R.J.Mceliece "A public-key cryptosystem based on algebraic coding theory" DSN Progress Report1978, 42-44, pp. 114-1 16.

[6] A.M.Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance" Advances in Cryptology - EUROCRYPT '89 (Springer, Berlin, 1990**),** pp. 224-314.

[7] B.Lamacchia and A.Odlyzko "Computation of discrete locarithms in prime finite fields" Advances in Cryptology - CRYPTO **'**90 (Springer, Berlin, 1991).

[8] K.S. McCurley, "The discrete logarithm problem" Proceedings of Symposia in Applied Mathematics**,** Providence, Rhode Island, 1990**,** Vol. 42**,** American Mathematical Society, pp. 49-74.

[9] C. Pomerance "Analysis and comparison of some integer factoring algorithms" Computational Methods in Number Theory, 1982, Vol.154, pp. 89-139

[10] A.K.Lenstra and M.S. Manasse, "Factoring by electronic mail" Advances in CrvDtolorv - EUROCRYPT **'**89 C.h.r ine-e r.Berlin, 1990**),** pp. 355-371**.**

[11] C. Pomerance, "Factoring" Proceedings of Symposia in Applied Mathematics**,** Providence. Rhode Island. 1990**,** Vol. 42**.** American Mathematical Society, pp. 27-48.

[12] K.S. McCurley "A key distribution system equivalent to factoring" J. Cryptology, 1988, Vol.1, (2), pp. 95-106.

[13] E.F.Brickell, and K.S. McCurley, "An interactive identification scheme based on discrete logarithms and factoring" J. Cryptology, 1992, Vol.5, (l), pp. 29-40.

[14] W. Baocang and H. Yupu, "Public key cryptosystem based on two cryptographic assumptions" IEE Proc. –Commun., Vol. 152, (6), 2005, pp. 861-865.

[15] S. Barnett "Matrix methods for engineers and scientists" McGraw-Hill Book Company, 1979.

[16] A.K. Lenstra, H.W. Lenstra. , M.S. Manesse, and J.M.Pollard, "The number field sieve" Proc. 22nd ACM Symp. On Theory of Computing, Baltimore, Maryland, USA, 1990, pp. 564-572.

[17] J. Gordon "Strong RSA keys" Electron. Lett. 1984, 20(12),pp. 514-516.

[18] K.H. Rosen "Elementary number theory and its applications" (Addison-Wesley, 1992,3rd edn)