# An Encryption Scheme Based On Integer Factorization and Discrete Logarithm

**Rekha Yadav, Anand Joshi**
Department of Mathematics, Dayalbagh Educational Institute, Agra

*Abstract*— **Public key cryptography is one of the mathematical applications valuable in sending information via insecure channel. In this paper we propose a new scheme of encryption and decryption of message, the security of which is based on the integer factorization problem and discrete logarithm problem.**

***Index Terms*—Public key, Discrete logarithm, Integer factorization, encryption.**

## I. INTRODUCTION

In this paper, we present and analyze a new public-key [1] encryption scheme. The proofs of security of this scheme rely on the factorization of large integer [6] and discrete logarithm problem [4]. Public-key cryptography refers to a cryptographic algorithm which requires two separate keys, one of which is secret (or private) and one of which is public. In public key cryptosystem each user places in a public _le an encryption procedure E. That is, the public file is a directory giving the encryption procedure of each user. The user keeps secret the details of his corresponding decryption procedure D. These procedures have the following four properties:

1. Deciphering the enciphered form of a message M yields M. Formally, D(E(M)) = M.
2. Both E and D are easy to compute.
3. By publicly revealing E the user does not reveal an easy way to compute D. This means that in practice only he can decrypt messages encrypted with E, or compute D efficiently.
4. If a message M is First deciphered and then enciphered, M is the result. Formally, E(D(M)) = M

An encryption (or decryption) procedure[3] typically consists of a general method and an encryption key. The general method, under control of the key, enciphers a message M to obtain the enciphered form of the message, called the ciphertext C. Everyone can use the same general method; the security of a given procedure will rest on the security of the key. Revealing an encryption algorithm then means revealing the key. A function E satisfying (1)-(3) is a trap-door one-way function, if it also satisfies (d) it is a trap-door one-way permutation. Diffie and Hellman [1] introduced the concept of trap-door one-way functions.

All classical encryption methods suffer from the key distribution problem. The problem is that before a private communication can begin, another private transaction is necessary to distribute corresponding encryption and decryption keys to the sender and receiver, respectively. Typically a private courier is used to carry a key from the sender to the receiver. Such a practice is not feasible if an electronic mail system is to be rapid and inexpensive. A public-key cryptosystem needs no private couriers; the keys can be distributed over the insecure communications channel. If Bob want to send a private message M to Alice in a public-key cryptosystem, then first he retrieves $E_A$ from the public file. Then he sends her the enciphered message $E_A$ (M). Alice deciphers the message by computing $D_A(E_A(M)) = M$. By property (3) of the public-key cryptosystem only she can decipher $E_A(M)$. She can encipher a private response with $E_B$, also available in the public file. There are no private transactions between Alice and Bob are needed to establish private communication. The only setup required is that each user who wishes to receive private communications must place his enciphering algorithm in the public file. Here in this paper we proposed a new message encryption and decryption public key scheme based on the difficulty of the factorization of sufficiently large integer and discrete logarithm problem.

## II. PRELIMINARIES

RSA [2] is a well known public key cryptosystem. In RSA public key cryptosystem a message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, N, of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e.d \equiv 1 \pmod{(p-1)(q-1)}$. The security of the RSA system rests in part on the difficulty of factoring the published divisor, N. Discrete logarithm is another well known public key cryptography scheme. Suppose that G is a group and $g \in G$ has finite order m. Then for each $t \in < G >$ the integers n with $g^n = t$ form a residue class mod m. Denote it by $\log_g t$. The discrete logarithm problem is the computational task of finding a representative of this residue class; that is, finding an integer n with $g^n = t$.

## III. ALGORITHM AND PROOF OF THE PROPOSED ENCRYPTION AND DECRYPTION SCHEME

1. Key generation

- Choose two large prime numbers $p$ and $q$.
- Compute $N = p.q$.

  

- Choose $1< e < \Phi(N)$, with $gcd(e, \Phi(N)) = 1$, where $\Phi(N) = (p-1)(q-1)$.
- Determine d such that $e.d = 1 \bmod (\Phi(N))$
- Let $g \in U(N)$ such that g has sufficiently large order, where $U(N)$ is the unit group of N in modulo N.
- Form a cyclic subgroup generated by g, i.e. <g>
- Choose an element _ from this cyclic group < g > such that $\alpha = g^x \pmod N$.
- Public keys {N, e, α, g}
- Private Keys {d, x}.

2. Encryption: For encrypting a message sender do the following
   - Obtains the recipients' public keyS {N, e, α, g}
   - Find the ASCII code of the message and make it into a string of equal length, by padding enough zeros in front and concatenate them into a single large string.
   - Encrypting the each sub-string with recipients public keys {N, e, α, g}.

   That is computing cipher text for each sub-string like this is $C = (M, \alpha)^s \pmod N$.
   - Performing padding on each encrypted value by adding enough zeros in front as necessary so that length of each substring and then concatenating all substring into a single string and then convert this substring into text string. Thus, on doing so we obtain an encrypted cipher text C in text form.
   - Sends the cipher text C to recipient.
3. Decryption: Recipient does the following:-
   - First converts the C in digital form.
   - Decrypting each substring by using the recipients private key {d, x}
   - For this compute $M = (v^s C)^d \pmod N$ where $v = g^{\varphi(N)-x} \pmod N$
   - Perform padding (adding enough zeros in front) on each substring and then concatenating each substring in natural order.
   - Then translating each substring into character form to obtain the plain text message.

Theorem: Let {N, e, α, g} be the public key and {d, x} be the private key as proposed above then

$$M = (v^s C)^d \pmod N$$

where $v = g^{\varphi(N)-x} \pmod N$, for any integer M with $0 \le M < N$.

Proof: Consider

$$(v^e C)^d = [(g^{\Phi(N)-x})^e (M\ \alpha)^e]^d \bmod N$$

$$= (g^{e\Phi(N)-ex})^d (M^e g^{xe})^d \bmod N$$

$$= g^{ed\Phi(N)} g^{-xed} M^{ed} g^{xed} \bmod N$$

$$= g^{ed\Phi(N)} M^{ed} (g^{xed})(g^{xed})^{-1} \bmod N$$

$$= g^{ed\Phi(N)} M^{ed} .1 \bmod N$$

$$= (g^{\Phi(N)})^{ed} M^{ed} \bmod N$$

$$(Since\ g^{\Phi(N)} \equiv 1 \pmod N)$$

$$= M^{ed} \bmod N$$

Since $e.d \equiv 1 \pmod{(p-1)(q-1)}$, therefore there is an integer k with $ed = 1+k(p-1)(q-1)$

Therefore $M^{ed} = M^{1+k(p-1)(q-1)} = MM^{k(p-1)(q-1)}$. It follows that $M^{ed} \equiv M(M^{p-1})^{(q-1)k} \equiv M \pmod p$

If p is not a divisor of m, then this congruence follow from Fermet's little theorem. Otherwise, the assertion is trivial because both sides of the congruence are 0 (mod p). Analogously, we see that $M^{ed} \equiv M \pmod q$.

Because p and q are distinct prime numbers, we obtain $M^{ed} \equiv M \pmod N$. This assertion follows from the fact that $0 \le M < N$. Thus $(v^s C)^d \equiv M \pmod N$.

## IV. DEMONSTRATION OF THE PROCEDURE

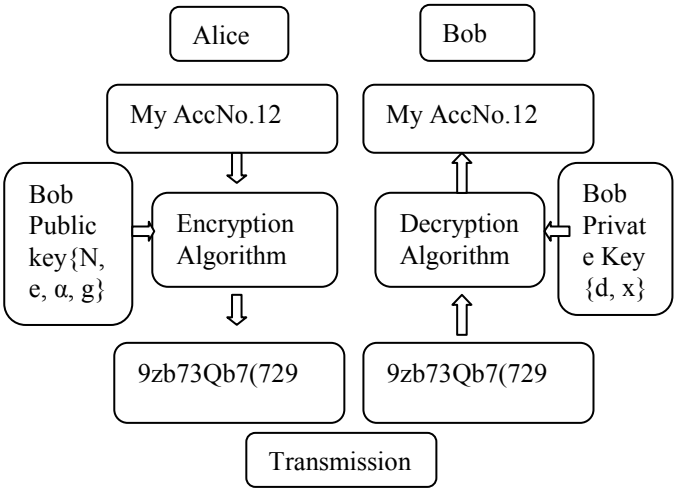


Fig.1: Proposed Cryptosystem

The above figure shows the proposed cryptosystem in which the message send by Alice is My AccNo.12 . We demonstrate the proposed method by this example in which the message is My AccNo.12.

Key Generation: We choose p = 23, q = 29. The value of N is: 667. The public key e is: 3 The value of Phi is: 616 .The private key d is: 411. Size of N is: 3.Select random integer x: 2. Select another random number g: 5. The value of α: 25

Encryption Process: Enter the message: **My AccNo.12**

ASCII code of the message is: 77 121 32 65 99 99 78 111 46 32 49 50 Concatenated padded ASCII value:

  

077121032065099099078111046032049050 Encrypting substring of length = 3 (No. of digits of N) by using the senders public Key e = 3, α =25 using $c_i = ( m_i * \alpha )^e \bmod N$ Encrypted ciphertext for each substring is: 579 98 555 126 198 198 95 540 92 555 501 357 Concatenated Encrypted ciphertext after performing padding: 579098555126198198095540092555501357 Converted digital string in text form: 9Zb73Qb 7( 72 9 Ciphertext of the message is: **9Zb73Qb 7( 729**

Decryption Process:- Recipients obtains: 9Zb73Qb7(729 . Converting the text string in digitized form: 579098555126198198095540092555501357. Dividing the string into substring(of length=3): 579 98 555 126 198 198 95 540 92 555 501 357.Decrypting each substring by using the recipients private Key: d = 411, x = 2 , g = 5 by using $m_i = (v^e C)^d = [(g^{\Phi(N)-x})^e c_i]^d \bmod N$. Decrypted ciphertext for each substring is: 77 121 32 65 99 99 78 111 46 32 49 50 .Concatenated Padded decrypted string is: 077121032065099099078111046032049050 .Dividing the string into substring (of length=3): 77 121 32 65 99 99 78 111 46 32 49 50 .Converting the digital decrypted string into into text form: My AccNo.12

Original Message: **My AccNo.12**

The whole encryption and decryption process for the above example is shown diagrammatically in the next figure.

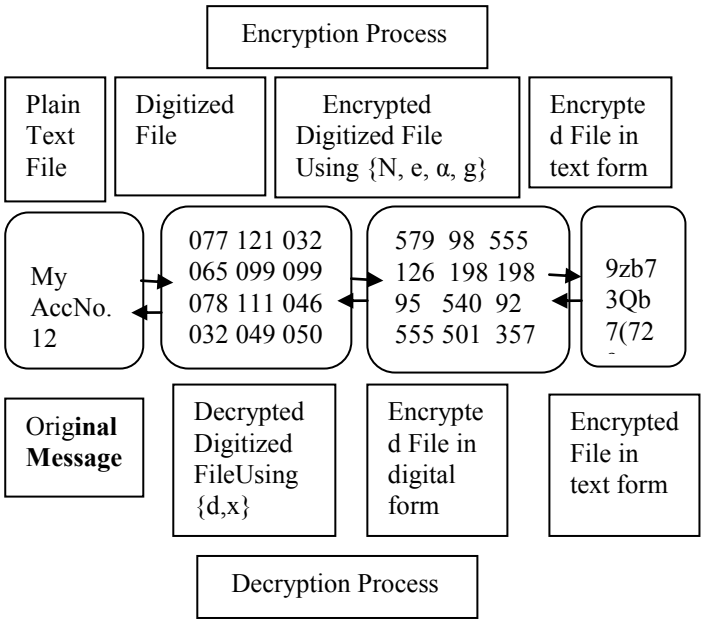


Fig.2 Encryption and decryption process for the proposed cryptosystem for a particular example.

## V. Security Analysis of the Proposed Method

Any approach of breaking this system is as difficult as the factoring of large integer and the difficulty of discrete logarithm problem. The factors of N enable us to compute Φ(N) and thus d. This approach also depends on the discrete factorization problem. This is a hybrid cryptosystem based on the difficulty of two known approach. The complexity of this algorithm is better than the method which is based on only one problem.

## VI. Conclusion

We have proposed a method for implementing a public-key cryptosystem whose security is based on the difficulty of factoring large numbers and discrete logarithm problem. The complexity of this algorithm is better than that of other known algorithm which is based only either on factoring of large number or discrete logarithm problem. The security of our method seems to be adequate, so it permits to establish secure communications without the use of couriers to carry keys.

## REFERENCES

[1] Diffie, W., and Hellman, M, "New directions in cryptography", IEEE Trans. Inform. Theory IT-22, (Nov. 1976), 644-654.

[2] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of ACM 21-2 February 1978.

[3] B. schneier, \Applied cryptography,", NY: John Wiley and Sons, Inc., 1996.

[4] Kevin S. McCurley, "The discrete logarithm problem",

  

Proceedings of symposia in applied mathemaics, volume 42, 1990, 49-74.

[5] L. Adleman, "A subexponential algorithm for the discrete Logarithm problem with applications to cryptography, Proceedings of the IEEE 20th Annual Symposium on Foundations of Computer Science (1979), 5560.

[6] Stefania Cavallar, Bruce Dodson, Arjen Lenstra, Paul Leyland, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman te Riele, and Paul Zimmermann, "Factorization of RSA-140 Using the Number Field Sieve", Proceedings of Asiacrypt '99, Singapore, November 14-18, 1999

  