Public Key Cryptosystem based on Number Theoretic Transforms

C. Porkodi and R. Arumuganathan

***Abstract*—**In this paper a Public Key Cryptosystem is proposed using the number theoretic transforms (NTT) over a ring of integer modulo a composite number. The key agreement is similar to ElGamal public key algorithm. The security of the system is based on solution of multivariate linear congruence equations and discrete logarithm problem. In the proposed cryptosystem only fixed numbers of multiplications are carried out (constant complexity) and hence the encryption and decryption can be done easily. At the same time, it is very difficult to attack the cryptosystem, since the cipher text is a sequence of integers which are interrelated. The system provides authentication also. Using Mathematica version 5.0 the proposed algorithm is justified with a numerical example.

***Keywords*—**Cryptography, decryption, discrete logarithm problem encryption, Integer Factorization problem, Key agreement, Number Theoretic Transform.

I. Introduction

As the progress of modern information technology is rapid, security is an important technique of many applications including electronic commerce, secure internet access and virtual private networks. To protect the transmitted data from eavesdropping by an adversary we need to disguise the message before sending it in to the insecure communication channel. This is achieved by a cryptosystem. Specially designed mathematical algorithms can transform messages into some thing unreadable (encryption) and back (decryption). Most of these algorithms are based on modular exponentiation and number theoretic functions like Euler totient function, Carmichael function and so on [3, 9, and 11].

The most popular and well defined security primary technique RSA algorithm [9] is based on modular exponentiation, the security of the system is based on integer factorization problem. i.e., given n, the product of two large prime numbers of same size it is computationally infeasible to find the factors. In RSA the cipher text C is obtained by first encoding the message as a number M and then taking the modular exponentiation $C = M^e \bmod n$, where e is the public key, relatively prime with the Euler totient function $\phi(n)$ and $1 < e < \phi(n)$. Decryption is done by computing the modular exponentiation $C^d \bmod n$, where d is the secret key such that $1 < d < \phi(n)$ and $ed \equiv 1 \bmod \phi(n)$.

Another modular exponentiation based cryptosystem is ElGamal encryption and decryption scheme [4, 11], which is described on the multiplicative cyclic group Z_n^* of the field Z_n generated by $\alpha \neq 1$ with n to be a composite number. To communicate secretly with A, entity B first gets A's public key $\left(n, \alpha, \alpha^a\right)$ where $1 \le a \le n-1$. Then B chooses a random integer k, $2 \le k \le n-1$ and encrypts the message M as $\delta \equiv M\left(\alpha^a\right)^k \bmod n$. B sends the cipher text as (γ, δ) where $\gamma \equiv \alpha^k \bmod n$. From the cipher text (γ, δ), A obtains the plaintext by finding the product $\gamma^{-a}\delta \bmod n$.

The security of the public key cryptosystem proposed by W. Diffie and M. Hellman [3] depends on discrete logarithm problem. Two entities A and B to communicate privately use $\alpha^{ab} \bmod q$, where α is a fixed primitive element of the finite field is $GF(q)$ and a, b are the secret keys of A and B, respectively.

The security of Public Key cryptography with matrices [6] depends on the difficulty of solving a system of multivariate congruence equations over a specified commutative ring. In this paper we proposed a public key cryptosystem using Number theoretic transforms (NTT) [7, 8, and 12] over the ring of integer modulo a composite number m. Number theoretic transforms (NTT) find applications in fast coding, decoding, digital filtering, image processing, convolution, deconvolution and cryptography. The key agreement in the proposed system is similar to that of Elgamal cryptosystem and the system has the advantage of high speed encryption and decryption rates compared with RSA system as the encryption and decryption algorithm involve only two modular exponentiation terms g^{ab} and g^{-ab}. It is a system with constant complexity, because only a fixed number of multiplications are involved. The security of the system is well protected, because it involves the difficulty of solving the system of multivariate congruence equations over a specified

C. Porkodi is with the Department of Mathematics and Computer Applications, PSG College of Technology, Coimbatore 641 004, INDIA. (phone: 0422 - 2572177; fax: 2573833 e-mail: porkodi_c2003@ yahoo.co.in).

Dr. R. Arumuganathan is with the Department of Mathematics and Computer Applications, PSG College of Technology, Coimbatore 641 004, INDIA. (phone: 0422 - 2572177; fax: 2573833 e-mail: ran_psgtech@ yahoo.co.in).

commutative ring [2, 5] and discrete logarithm problem. The system however requires a large key for encryption and decryption, as the key agreement is based on Elgamal algorithm. The cipher text is sent as a sequence of numbers through packets or virtual circuits so that the order of the elements in the sequence cannot be shuffled or altered by an adversary.

The paper is organized such that, section II discusses the Mathematical model, section III discusses the key agreement algorithm, section IV discusses symmetric key encryption and decryption algorithm, section V discusses about the security aspect, section VI gives a small example of key agreement, symmetric key encryption and decryption and lastly section VII concludes this paper.

II. The Mathematical model

In this section we discuss basic definitions and results behind the encryption and decryption algorithm.

A. Number Theoretic Transform (NTT) in a Ring of Integer modulo a composite number

Let $\{h_n\}$ be a sequence of N integers (N - point integer sequence) and g be an integer such that g and N are mutually prime with a composite number m. Then the NTT is defined as

$$H_k \equiv \sum_{n=0}^{N-1} h_n g^{nk} \bmod m,\ k = 0,1,2...N-1 \quad \text{-----} \quad (1)$$

and the Inverse number theoretic transforms (INTT) is defined as

$$h_l \equiv N^{-1} \sum_{k=0}^{N-1} H_k g^{-lk} \bmod m,\ l = 0,1,2,...,N-1 \quad \text{-----} \quad (2)$$

Where $NN^{-1} \equiv 1 \bmod m$, $g^N \equiv 1 \bmod m$ and

$\sum_{k=0}^{N-1} g^{uk} = 0 \bmod m$, Equivalently, $[(g^u - 1), m)] = 1$ for every u such that $\frac{N}{u}$ is a prime.

B. Euler totient function

If $n \geq 1$ the Euler totient function $\phi(n)$ is defined to be the number of positive integers not exceeding n, which are relatively prime to n.

C. Discrete logarithm problem

Given a finite cyclic group G of order n, a generator α of G and an element $\beta \in G$, find the integer $x, 0 \leq x \leq n-1$ such that $\alpha^x = \beta \bmod n$.

.

D. Integer Factorization problem

Given a positive integer n, find its prime factorization: that is, write $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ where p_i 's are pair wise distinct primes and $e_i \geq 1$.

E. Theorem

If a and m are relatively prime then the unique solution of the linear congruence $ax \equiv b \pmod m$ is $x \equiv ba^{\phi(m)-1} \pmod m$ (according to [10] page 114).

By little Fermat's theorem $a^{\phi(m)} \equiv 1 \bmod m$ we get $x \equiv ba^{-1} \bmod m$.

III. Key Agreement Algorithm

To communicate with each other privately the entities A and B generates two large and distinct primes p and q, each roughly of same size, computes the product $m = pq$, $\phi(m) = (p-1)(q-1)$ and $r = \gcd(p-1, q-1)$.

The entity A computes an integer $g > 1$, $N > 1$ each mutually prime with m and satisfying $g^N \equiv 1 \bmod m$ and $\sum_{k=0}^{N-1} g^{uk} = 0 \bmod m$ for every u such that $\frac{N}{u}$ is a prime. Then A chooses a large random integer $a, 1 < a \leq m-1$ computes $g^a \bmod m$ and $x = (g^a \bmod m)(r + k_1) \bmod \phi(m)$, where k_1 is the least positive integer such that $r + k_1$ is relatively prime with $\phi(m)$ and the product $(g^a \bmod m)(r + k_1)$ exceeds $\phi(m)$. A's public key is $(g, N, g^a \bmod m, x)$ and private key is a. B chooses the integer $b,\ 1 < b \leq m-1$ computes $g^b \bmod m$ and $y = (g^b \bmod m)(r + k_2) \bmod \phi(m)$, where k_2 is the least positive integer such that $r + k_2$ is relatively prime with $\phi(m)$ and the product $(g^a \bmod m)(r + k_2)$ exceeds $\phi(m)$. B's public key is $(g, g^b \bmod m, y)$ and private key is b.

A sends the public key $(g, g^a \bmod m, x)$ to B. Using this public key and the known values $r, \phi(m)$ entity B frames the congruence equation $(g^a \bmod m)(r + k_1) \equiv x \bmod \phi(m)$ and solve for $g^a \bmod m \equiv x(r + k_1)^{-1} \bmod \phi(m)$ [by Theorem II.E]. Here $(r + k_1)^{-1}$ is the inverse of $(r + k_1)$ with respect to $\bmod \phi(m)$. Thus B conforms that the message is from A. Hence authentication holds good in this cryptosystem.

Because of the trapdoor integer factorization problem, it is computationally infeasible for an intruder to find the Euler

totient function $\phi(m)$. The intruder cannot guess $\phi(m)$ send $(g^c \bmod m)(r+k) \bmod \phi(m)$ where c is his secret key. Thus he cannot impersonate like A or B. Hence in this scenario the man in middle attack is impossible.

IV. Proposed Cryptosystem

The integers $g > 1$ and N are chosen such that they are mutually prime with m, $g^N \equiv 1 \bmod m$ and $\gcd\left(g^u - 1, m\right) = 1$ for every u such that $\frac{N}{u}$ is a prime.

According to [7] page 312, finding g and N satisfying $\gcd\left(g^u - 1, m\right) = 1$ for every u such that $\frac{N}{u}$ is a prime equivalent to

$$\sum_{n=0}^{N-1} g^{nu} \equiv 0 \bmod m \tag{3}$$

The plaintext is encoded as a N-point integer sequence h_n where each $h_n \le m-1$.

The encryption is done by using NTT over a ring of composite number m as

$$H_k \equiv \left(g^b\right)^a \sum_{n=0}^{N-1} h_n g^{nk} \bmod m, \quad k = 0,1,2...N-1$$

$$H_k \equiv g^{ab} \sum_{n=0}^{N-1} h_n g^{nk} \bmod m, \quad k = 0,1,2...N-1 \tag{4}$$

Using INTT as does the decryption

$$h_l \equiv N^{-1}\left(g^a\right)^{-b} \sum_{k=0}^{N-1} H_k g^{-lk} \bmod m, \quad l = 0,1,2...N-1 \tag{5}$$

A. Encryption

The plain text message is converted to integers $h_0, h_1, h_2 \ldots h_{N-1}$ all less than m.

$$H_0 \equiv g^{ab} \sum_{n=0}^{N-1} h_n \bmod m \tag{6}$$

$$H_1 \equiv g^{ab} \sum_{n=0}^{N-1} h_n g^n \bmod m \tag{7}$$

$$H_2 \equiv g^{ab} \sum_{n=0}^{N-1} h_n g^{2n} \bmod m \tag{8}$$

$$\vdots$$

$$H_{N-1} \equiv g^{ab} \sum_{n=0}^{N-1} h_n g^{(N-1)n} \bmod m \tag{9}$$

Now the cipher text is $\{H_0, H_1, H_2 \ldots H_{N-1}\}$

B. Decryption

Using the cipher text $H_0, H_1, H_2 \ldots H_{N-1}$ and decryption algorithm (4.3) the receiver frames the system of equations given by the matrix form

$$\begin{pmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ \cdot \\ \cdot \\ \cdot \\ h_{N-1} \end{pmatrix} \equiv N^{-1} g^{-ab} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & g^{-1} & g^{-2} & g^{-3} & \cdots & g^{-(N-1)} \\ 1 & g^{-2} & g^{-4} & g^{-6} & \cdots & g^{-2(N-1)} \\ 1 & g^{3} & g^{6} & g^{9} & \cdots & g^{-3(N-1)} \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ 1 & g^{-(N-1)} & g^{-2(N-1)} & g^{-3(N-1)} & \cdots & g^{-(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} H_0 \\ H_1 \\ H_2 \\ H_3 \\ \cdot \\ \cdot \\ \cdot \\ H_{N-1} \end{pmatrix} \bmod m$$

This matrix equation gives the values of $h_0, h_1, h_2 \ldots h_{N-1}$ as follows

$$h_0 = N^{-1} g^{-ab} \sum_{k=0}^{N-1} H_k \bmod m$$

$$= N^{-1} g^{-ab} \left(g^{ab} \sum_{n=0}^{N-1} h_n + g^{ab} \sum_{n=0}^{N-1} h_n g^n + g^{ab} \sum_{n=0}^{N-1} h_n g^{2n} + \ldots + g^{ab} \sum_{n=0}^{N-1} h_n g^{(N-1)n} \right) \bmod m$$

Using (4.1.1), (4.1.2), (4.1.3) and (4.1.4) we get

$$h_0 = N^{-1} \left(\sum_{n=0}^{N-1} h_n + \sum_{n=0}^{N-1} h_n g^n + \sum_{n=0}^{N-1} h_n g^{2n} + \ldots \sum_{n=0}^{N-1} h_n g^{(N-1)n} \right) \bmod m$$

$$= N^{-1} \left(N h_0 + h_1 \sum_{n=0}^{N-1} g^n + h_2 \sum_{n=0}^{N-1} g^{2n} + \ldots + \sum_{n=0}^{N-1} g^{(N-1)n} \right) \bmod m$$

Using (4.1), we get

$$h_0 = N^{-1}(N\ h_0) \bmod m$$

$$h_0 = h_0 \bmod m$$

$$h_1 = N^{-1} g^{-ab} \sum_{k=0}^{N-1} g^{-ab} H_k \bmod m$$

$$= N^{-1} g^{-ab} \left(g^{ab} \sum_{n=0}^{N-1} h_n + g^{-1} g^{ab} \sum_{n=0}^{N-1} h_n g^n + g^{-2} g^{ab} \sum_{n=0}^{N-1} h_n g^{2n} + \ldots + g^{-(N-1)} g^{ab} \sum_{n=0}^{N-1} h_n g^{(N-1)n} \right) \bmod m$$

Using (4.1.1), (4.1.2), (4.1.3) and (4.1.4) we get

$$h_1 = N^{-1} \left(h_0 \sum_{n=0}^{N-1} \left(g^{-1}\right)^n + N h_1 + h_2 \sum_{n=0}^{N-1} g^n + \ldots + h_{N-1} \sum_{n=0}^{N-1} g^{(N-2)n} \right) \bmod m$$

Using (4.1) we get

$$h_1 = N^{-1}(N h_1) \bmod m$$

$$h_1 = h_1 \bmod m.$$

Similarly $h_3, h_4 \ldots h_{N-1}$ can be obtained.

V. Security of the Cryptosystem

We assume that no one modifies or shuffle the cipher text sequence. The security of the system depends on the key d. Using the encryption and decryption algorithm an intruder can frame $2N$ equations $AX \equiv B \bmod m$ involving the N unknowns

$g^{ab}h_0, g^{ab}h_1, g^{ab}h_2, g^{ab}h_3, \ldots g^{ab}h_{N-1}$. The coefficient matrix A is of order $(2N \times N)$ with the $(N \times N)$ identity matrix as a part of it. So the rank of A is N. The augmented matrix (A/B) is of order $(2N \times N+1)$.The rank of (A/B) must be either N or $N+1$.

If rank of (A/B) is $N+1$ then the system is inconsistent, as rank of (A/B) is not equal to rank of A.

If rank of (A/B) is N then the system is consistent and the values of $g^{ab}h_0, g^{ab}h_1, g^{ab}h_2, g^{ab}h_3, \ldots g^{ab}h_{N-1}$ can be obtained. But using these values it is impossible to find each $g^{ab}, h_0, h_1, h_2, \ldots h_{N-1}$ separately.

VI. Numerical Illustration

In this section we justified the proposed algorithm with an example.

Entities A and B agrees the product of two primes $m = 37 \times 73 = 2701$ and computes $\phi(m) = 2592$ and $r = \gcd(36,72) = 36$.

A. Key Agreement

To communicate with A, B first gets A's public key is $\left(g = 16, N = 9, g^a \bmod m = 1973, \left[(g^a \bmod m)(r + k_1)\right] \bmod \phi(m) = 425\right)$

A has chosen the secret as $a = 2689$. Also $g^{-1} = 1857$ and $N^{-1} = 2401$.

B chooses $b = 2657$ and computes $g^b \bmod m = 16^{2657} \bmod 2701 = 256$. B's public key is $\left(g = 16, N = 9, g^b \bmod m = 256, (g^b \bmod m)(r + k_2) \bmod \phi(m) = 1696\right)$

Now the key used for encryption is $g^{ab} \bmod m = 588$ and the key for decryption is $g^{-ab} \bmod m = 712$.

B. Encryption

Suppose the plaintext message is

"PUBLIC KEY CRYPTOSYSTEMS USING NTTS".

It is encoded as

1621 0212 0903 0011 0525 0003 1825 1620 1519 2519 2005 1319 0021 1909 1407 0014 2020 1900

As it contains more than $N = 9$ blocks we represent it as a two 9-point integer sequence

$\{1621, 0212, 0903, 0011, 0525, 0003, 1825, 1620, 1519\}$ and

$\{2519, 2005, 1319, 0021, 1909, 1407, 0014, 2020, 1900\}$.

By taking the first sequence of integers as

$h_0 = 1621, h_1 = 0212, h_2 = 0903, h_3 = 0011, h_4 = 0525, h_5 = 0003, h_6 = 1825, h_7 = 1620, h_8 = 1519$

$$\begin{pmatrix} H_0 \\ H_1 \\ H_2 \\ H_3 \\ H_4 \\ H_5 \\ H_6 \\ H_7 \\ H_8 \end{pmatrix} \equiv 588 \times \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 16 & 16^2 & 16^3 & 16^4 & 16^5 & 16^6 & 16^7 & 16^8 \\ 1 & 16^2 & 16^4 & 16^6 & 16^8 & 16^{10} & 16^{12} & 16^{14} & 16^{16} \\ 1 & 16^3 & 16^6 & 16^9 & 16^{12} & 16^{15} & 16^{18} & 16^{21} & 16^{24} \\ 1 & 16^4 & 16^8 & 16^{12} & 16^{16} & 16^{20} & 16^{24} & 16^{28} & 16^{32} \\ 1 & 16^5 & 16^{10} & 16^{15} & 16^{20} & 16^{25} & 16^{30} & 16^{35} & 16^{40} \\ 1 & 16^6 & 16^{12} & 16^{18} & 16^{24} & 16^{30} & 16^{36} & 16^{42} & 16^{48} \\ 1 & 16^7 & 16^{14} & 16^{21} & 16^{28} & 16^{35} & 16^{42} & 16^{49} & 16^{56} \\ 1 & 16^8 & 16^{16} & 16^{24} & 16^{32} & 16^{40} & 16^{48} & 16^{56} & 16^{64} \end{pmatrix} \begin{pmatrix} 1621 \\ 0212 \\ 0903 \\ 0011 \\ 0525 \\ 0003 \\ 1825 \\ 1620 \\ 1519 \end{pmatrix} \bmod 2701$$

$H_0 = 1639, H_1 = 2123, H_2 = 2211, H_3 = 2463, H_4 = 1585, H_5 = 2307, H_6 = 0590, H_7 = 2419, H_8 = 0825$

Similarly the second sequence is encrypted as the sequence

$\{2378,1437,0992, 0572, 1439,1320, 2440, 0992, 0347\}$

C. Decryption

$$\begin{pmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \\ h_7 \\ h_8 \end{pmatrix} \equiv 2401 \times 712 \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1857 & 1857^2 & 1857^3 & 1857^4 & 1857^5 & 1857^6 & 1857^7 & 1857^8 \\ 1 & 1857^2 & 1857^4 & 1857^6 & 1857^8 & 1857^{10} & 1857^{12} & 1857^{14} & 1857^{16} \\ 1 & 1857^3 & 1857^6 & 1857^9 & 1857^{12} & 1857^{15} & 1857^{18} & 1857^{21} & 1857^{24} \\ 1 & 1857^4 & 1857^8 & 1857^{12} & 1857^{16} & 1857^{20} & 1857^{24} & 1857^{28} & 1857^{32} \\ 1 & 1857^5 & 1857^{10} & 1857^{15} & 1857^{20} & 1857^{25} & 1857^{30} & 1857^{35} & 1857^{40} \\ 1 & 1857^6 & 1857^{12} & 1857^{18} & 1857^{24} & 1857^{30} & 1857^{36} & 1857^{42} & 1857^{48} \\ 1 & 1857^7 & 1857^{14} & 1857^{21} & 1857^{28} & 1857^{35} & 1857^{42} & 1857^{49} & 1857^{56} \\ 1 & 1857^8 & 1857^{16} & 1857^{24} & 1857^{32} & 1857^{40} & 1857^{48} & 1857^{56} & 1857^{64} \end{pmatrix} \begin{pmatrix} 1639 \\ 2123 \\ 2211 \\ 2463 \\ 1585 \\ 2307 \\ 0590 \\ 2419 \\ 0825 \end{pmatrix} \bmod 2701$$

Hence the plain text is

$h_0 = 1621, h_1 = 0212, h_2 = 0903, h_3 = 0011, h_4 = 0525, h_5 = 0003, h_6 = 1825, h_7 = 1620, h_8 = 1519$

Second sequence of cipher text is decrypted as $\{2519, 2005, 1319, 0021, 1909, 1407, 0014, 2020, 1900\}$

After decryption as the receiver gets the encoded message

0212 0903 1621 0011 0525 0003 1825 1620 1519 2519 2005 1319 0021 1909 1407 0014 2020 1900

and hence gets the plain text

"PUBLIC KEY CRYPTOSYSTEMS USING NTTS"

D. Security

Because of the discrete logarithm problem from known $g = 16, g^a = 1973$ and $g^b = 256$, it is infeasible to find a and b. So the agreed key $g^{ab} \bmod m$ cannot be evaluated by an adversary and hence he cannot recover the plaintext from the cipher text.

Also as $\phi(m) = 2592$, $r = 36$ is unknown to a third person, he cannot impersonate as A or B.

VII. Conclusion

In this paper we discussed a public key cryptosystem by using the number theoretic transforms over a ring of integer modulo a composite number m . As the key agreement is done similar to Elgamal cryptosystem our system is also very secured one. The security of the system is based on the solvability of multivariate linear congruence equations that is very complex and the discrete logarithm problem. This cryptosystem also provides authentication by the agreement of the first element of the N -point integer sequence. Impersonation is also not possible as it is computationally infeasible to find the Euler totient function.

References

[1] Alfred Menezes J, Paul Van Oorchot C, Scott A Vanstone, "Hand book of Applied Cryptography", CRC Press, 1997.

[2] S. Cabay and T.P.L. Lam, "Congruence Techniques for the Exact Solution of Integer Systems of Linear Equations, ACM Transactions on Mathematical Software,Vol.3,No.4, pp386-397, December 1977.

[3] W. Diffie and M. Hellman,"New Directions in Cryptography", IEEE Transactions on Information Theory,vol.IT-22,pp472-492,1976.

[4] Elsayed Mohammed, .E. Emarah and KH. El-Shennawy, "A Blind Signature Scheme based on Elgamal Signature", Seventeenth National Radio Science Conference Feb.22-24, 2000, Minufiya University, Egypt.

[5] Jacques Patarin, "Hidden Field Equations (HFE) and Isomorphism of Polynomials (IP): two new families of Asymmetric Algorithms", Eurocrypt'96, Springer Verlag, pp.33-48.

[6] Mukesh Kumar Singh, "Public Key Cryptography with Matrices", Proceedings of the IEEE Workshop on Information Assurance, United States Military Academy pp146-152, June 2004.

[7] H.J. Nussbaumer, "Fast Fourier Transform and Convolution Algorithms", second edition, Springer-Verlag Berlin Heidelberg, New York.

[8] Ramesh C. Agarwal and C. Sidney Burrus, "Number Theoretic Transforms to Implement Fast Digital Convolution", Proceedings of the IEEE, vol.63, No.4, April 1975.

[9] Ronald L. Rivest, Adi Shamir and Leonard M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, vol21, no2, pp.120-126, Feb 1978.

[10] Tom M. Apostol, "Introduction to Analytic Number Theory", Springer-Verlag 1976.

[11] Taher Elgamal,"A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, vol.IT31, No4, July 1985.

[12] Vassil S. Dimitrov, Todor V. Cooklev and Borislav Donevsky," Number Theoretic Transforms Over the Golden Section Quadratic Field", IEEE Transactions on signal Processing, vol.43, No.8, August 1995.