International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 3, June 2018, pp. 1814~1821
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i3.pp1814-1821

Design and Implementation of a Secure Communication Protocol

M. K. Viswanath[1], M. Ranjith Kumar[2]
[1]Departement of Mathematics, Rajalakshmi Engineering College, Thandalam, Chennai – 602 105, Tamil Nadu, India
[2]Research Scholar, Research and Development Centre, Bharathiar University, Coimbatore – 641 046, Tamil Nadu, India

Article Info

Article history:

Received May 22, 2017
Revised Nov 30, 2017
Accepted Dec 7, 2017

Keyword:

Chen's theorem
Fermat's two squares theorem
Pseudo inverse
Rabin cryptosystem
Vinogradov's theorem

ABSTRACT

The main object of this paper is to present a mutual authentication protocol that guarantees security, integrity and authenticity of messages, transferred over a network system. In this paper a symmetric key cryptosystem, that satisfies all the above requirements, is developed using theorems of J.R. Chen, I.M. Vinogradov and Fermat and the decimal expansion of an irrational number.

Corresponding Author:

M. Ranjith Kumar,
Department of Mathematics,
Bharathiar University,
Coimbatore – 641 046, Tamil Nadu, India.
Email: annam.ranjith@gmail.com

1. INTRODUCTION

The cryptographic community has been pertinently more successful in the related field of identification and integrity, where the authentic users try to convince each other of their identity and the integrity of the secret message exchanged over an electronic channel [1], [2]. In ordinary communications an intruder can see all the exchanged messages, can delete, add or alter and redirect messages, can initiate the protocol with another party and re-use messages from part of communications [3], [4]. Hence cryptographic tools are very crucial in secret communications, as it prevents unauthorized persons from acquiring, stored data between computers or messages transferred between two mutually authenticated parties.

We describe in this paper how the above capabilities are incorporated in the communication system developed here using the broad idea proposed in [5]. However the techniques used here are quite different from the one used in [5], but is close to the one used in [6]. We make use of [7]-[9] and the Fermat's two squares theorem [10] in creating the keys for encrypting the plaintext and also the Rabin cryptosystem [11], without the modulus being made public for encrypting the message digest. In this protocol both the sender and receiver of a message can construct each other's key in addition to their own key as in the case of [6].

The rest of the paper is organized as follows. In Section 2 we describe the basic idea of Rabin cryptosystems. In Section 3 we give some background about the pseudo inverse of a rectangular matrix [12], [5]. In Section 4 we explain the Goldbach conjecture and Fermat's two squares theorem. Readers familiar with Section 1 to 4, may proceed directly to Section 5 of this paper. The working of the algorithm is illustrated with an example in Section 6 and the paper concludes with a Section on the security aspects of the system.

2. RABIN CRYPTOSYSTEM

The aim of this chapter is to discuss the Rabin cryptosystems whose security is based on computational assumptions related to the integer factorization [13]. The Rabin public-key encryption scheme [1], [14] was the first example of a provably secure public-key encryption scheme- the problem faced by a passive adversary of recovering plaintext from some given ciphertext is computationally equivalent to factoring. The security of Rabin is more closely related to factoring than RSA. It deals with the problem that if $n = p.q$ where p and q are distinct primes then squaring is a four-to-one map, so it is necessary to have a rule to choose the correct solution while decrypting the cryptotext.

1) Choose two random primes p and q such that $p \equiv q \equiv 3 \pmod 4$ and set $n = p.q$.
2) n is made public and (p, q) is kept as secret. To encrypt a message m , compute $C \equiv m^2 \pmod n$
3) To recover plaintext m from C , one does the following:
   a. Use the extended Euclidean algorithm to find the integers a and b satisfying $a.p + b.q = 1$. Note that a and b can be computed once and for all during the key generation stage.
   b. Compute $r \equiv C^{\frac{(p+1)}{4}} \pmod p$ and $s \equiv C^{\frac{(q+1)}{4}} \pmod q$.
   c. Find the four square roots of C modulo n . They are

$$m_1 \equiv a.p.s + b.q.r \pmod n$$
$$m_2 \equiv a.p.s - b.q.r \pmod n$$
$$m_3 = n - m_1$$
$$m_4 = n - m_2$$

and decides which of these is m .

A drawback of Rabin's public-key scheme is that the receiver is faced with the task of selecting the correct plaintext from among the four possibilities. This ambiguity in decryption can easily be overcome in practice by adding pre-specified redundancy to the original plaintext prior to encryption. Then, with high probability, exactly one of the four square roots m_1, m_2, m_3, m_4 of a legitimate ciphertext C will possess this redundancy, and the receiver will select this as the intended plaintext. If none of the square roots of C possesses this redundancy, then the receiver should reject C as a fraudulent message. This case does not arise with the problem in hand.

3. MOORE-PENROSE INVERSE (PSEUDO INVERSE)

3.1. Definition

Let $A \in R^{m \times n}$ and $X \in R^{n \times m}$, then the following equations are used to define the pseudo inverse of a rectangular matrix A [12], [14].

$$AXA = A \tag{1}$$

$$XAX = X \tag{2}$$

$$(AX)^T = AX \tag{3}$$

$$(XA)^T = XA \tag{4}$$

Equations (1) through (4) are called the Penrose conditions [15].

3.2. Definition

A pseudo inverse of rectangular matrix $A \in R^{m \times n}$ is also a rectangular matrix $X = A^{\#} \in R^{n \times m}$ satisfying Equations (1) through (4). A pseudo inverse is sometimes called the Moore – Penrose inverse after the pioneering work done by Moore (1920, 1935) and Penrose (1955).

3.3. Construction of pseudo inverse

For a given $A \in R^{m \times n}$, the pseudo inverse $A^{\#} \in R^{n \times m}$ is unique.

a. If $m=n$ and $rank(A)=m$ then $A^{\#}=A^{-1}$.

b. If $m<n$ and $rank(A)=m$ then AA^T is non-singular and

$$A^{\#}=A^T\left(AA^T\right)^{-1} \tag{5}$$

c. If $m>n$ and $rank(A)=n$ then A^TA is non-singular and

$$A^{\#}=\left(A^TA\right)^{-1}A^T \tag{6}$$

3.4. Conjecture

a. If A is a rectangular matrix in $R^{m\times n}$ formed by the mn consecutive decimal places of any irrational number, with $m<n$, then $rank(A)=m$ and A is always right invertible.

b. If A is a rectangular matrix in $R^{m\times n}$ formed by the mn consecutive decimal places of any irrational number, with $m>n$, then $rank(A)=n$ and A is always left invertible.

4. THE GOLDBACH CONJECTURE

In 1742, C. Goldbach conjectured that, *"every odd number greater than nine is expressible as the sum of three primes"* and *"every even number greater than four is expressible as the sum of two odd primes"*. The first one is called the odd Goldbach conjecture and the second one is called the even Goldbach conjecture [17]. In 1937, I.M. Vinogradov established the odd Goldbach conjecture. But the even Goldbach conjecture is still an open question and the best result obtained so far is given by Jin Run Chen in 1966.

4.1. Vinogradov's theorem

It was shown in 1937 by I.M. Vinogradov [9] that, *"All sufficiently large odd integers are expressible as a sum of three primes"*. Vinogradov proved the three - primes theorem by analytical means, using major arc/minor arc decomposition.

4.2. Chen's theorem

In 1966 Jin Run Chen [7] made considerable progress in setting the even Goldbach conjecture; in [8] Chen proved the following theorem. *"A large even integer can be expressed as the sum of a prime and the product of atmost two primes"*. Chen's theorem is a giant step towards solving the Goldbach conjecture, and is a remarkable result using the Sieve methods.

5. THE NEW SCHEME

The main idea of this paper is, to develop a new cryptosystem using Chen's theorem, Vinogradov's theorem and the Fermat's two squares theorem, which provides confidentiality, authenticity and integrity of the secret message shared over a public channel. This work is a novel method of developing a communication protocol which is secure against all the known possible attacks. The protocol is as follows:

We are looking for numbers which satisfy the following decomposition (a) and (b) given below and call these numbers as feasible numbers. Not all the odd and even integers are feasible. For example 11 and 14 are not feasible. A MATLAB programme is developed to check whether a given even or odd number is feasible. Using MATLAB the following numbers are found to be feasible: 100, 101, 1002, 999, 150, 151, 1029, 1578 and their decompositions are given by $100=79+7\cdot3$, $101=89+7+5$, $1002=967+5\cdot7$, $999=991+3+5$, $150=73+7\cdot11$, $151=139+5+7$, $1029=1021+5+3$, $1578=1543+5\cdot7$. Bob and Alice choose only feasible numbers for this protocol.

a. Suppose N is a large even integer, then N satisfies the decomposition $N=P+r_1\cdot s_1$, where r_1 and s_1 are distinct primes and P is the largest prime satisfying this relation.

b. If M is a large odd integer, then M satisfies the decomposition $M=Q+r_2+s_2$, where r_2 and s_2 are appropriate distinct primes and Q is the largest primes satisfying this relation.

Chen's and Vinogradov's theorems guarantee the existence of two primes P and Q from the sufficiently large feasible numbers N and M.

5.1. Initial setup

As before, assume two protagonists, Alice and Bob. An authentication protocol is executed by Bob to make sure that Alice wants to communicate with him.

Alice and Bob choose two large numbers N and M respectively and after ascertaining their identity, exchange it over a secure channel. Alice then chooses the largest primes N_1 of the form $4t+1$, N_2 of the form $4t+3$ less than N. Similarly, Bob chooses the largest primes M_1 of the form $4t+1$, M_2 of the form $4t+3$, less than M.

We recall the Fermat's two squares theorem,

"*If p is a prime number of the form $4n+1$, then $p=a^2+b^2$ for some integers a, b*".

We exploit this theorem of Fermat's, to obtain the pair of numbers (A_1, B_1) and (A_2, B_2) when the primes N_1 and M_1 of the form $4t+1$ are known. $N_1=A_1^2+B_1^2$ and $M_1=A_2^2+B_2^2$. Now Bob and Alice, both possess A_1, B_1, A_2 and B_2 once they are aware of N and M. For example, if $N_1=104681$, then $104681=155^2+284^2$ and if $M_1=100957$ then $100957=309^2+74^2$.

Thus both the users Bob and Alice have the numbers N and M and both can compute (N_1, N_2, A_1, B_1) and (M_1, M_2, A_2, B_2). They keep the pair of four tuples safely with them. Bob and Alice agree for an irrational number I which has a decimal expansion upto more than million places of decimals and I is kept as secret.

5.2. Plaintext encryption protocol

When Alice wants to send a secret message P to Bob, then Alice has the key tuples (N_1, N_2, A_1, B_1) and (M_1, M_2, A_2, B_2) with her, computed from the numbers N and M exchanged over a secure channel.

a. If B_1 is a feasible number, then she applies Chen's theorem to B_1 and computes (p, p_1, p_2) such that $B_1=p+p_1p_2$, where p is the largest prime and $p_1>p_2$, p_1, p_2 are distinct primes satisfying this relation. Similarly if A_2 is feasible, she computes (q, q_1, q_2) from the odd feasible number A_2 using Vinogradov's theorem, such that $A_2=q+q_1+q_2$, where q is the largest prime and q_1, q_2 suitable distinct primes $(q_1>q_2)$.

b. Now, Alice computes the first encryption key $K_1=k_1k_2k_3\cdots$, a sequence of decimal places from the position q in the expansion of the irrational number I, which is used to begin the encryption. The number at q^{th} place, say k_1 is used to substitute the beginning letter of the plaintext P by shifting the alphabet by k_1 units. Afterwards the process is continued with the next integer k_2 and the next alphabet in the plaintext and so on, till the entire message is encrypted. This encrypted message say C' is obtained by using the key q of Bob.

c. Next, Alice computes her encryption key matrix K_A using the number p, where K_A is a $p_1\times p_2$ rectangular matrix and the entries of K_A are the $p_1\cdot p_2$ consecutive decimal places picked from the position p in the expansion of I.

d. She arranges the cryptotext C' in blocks of length p_2 with its numerical equivalents and obtains the final ciphertext C by $C=K_AC'$.

5.3. Message integrity encryption protocol

Alice computes the product $n=N_2M_2$. The integrity of the message is obtained by considering the letters $m_1, m_2, m_3, m_4=m$(say) occurring in the p_1, p_2, q_1, q_2 th places of the first sentence in P. The compilation of word in the exact order is taken as message digest. She encrypts the word m as $w\equiv m^2 \pmod n$. Now the ciphertext C and the encrypted message digest w are sent to Bob through an open channel, for decryption.

5.4. Ciphertext decryption protocol

Once Bob receives the ciphertext pair (C, w), he does the following for decryption.

He knows, p is the position of the decimal place to start, in the expansion of the irrational number I. From this position of p, he collects the $p_1 p_2$ consecutive digits from the decimal expansion of I and obtains the rectangular matrix K_A of order $p_1 \times p_2$. He then computes the pseudo inverse $K_A^{\#}$ of K_A and applies this decryption key to the ciphertext C and obtains C', $C' = K_A^{\#} C$, where C is arranged in blocks of p_1-tuples with its numerical equivalent. Now he knows his key value q and obtains the decimal places from the q^{th} position of the decimal expansion of I where the first encryption process has begun. Then he can easily obtains the plaintext P by decrypting C' using the inverse substitution cipher of Bob. This process establish the authenticity of the message received from Alice as the message is locked with the keys of Bob and Alice, without formally exchanging the message P between Bob and Alice.

5.5. Decryption Protocol for Integrity:

Bob wants to compute $\sqrt{w} \pmod{n}$ and he does it by the following method.

a. He computes $m_{N_2} \equiv w^{\frac{(N_2+1)}{4}} \pmod{N_2}$ and $m_{M_2} \equiv w^{\frac{(M_2+1)}{4}} \pmod{M_2}$.

b. By extended Euclidean algorithm, he finds y_{N_2} and y_{M_2} such that $y_{N_2} \cdot N_2 + y_{M_2} \cdot M_2 = 1$.

c. Then he computes the four possibilities for m, such that

$$r_1 \equiv y_{N_2} \cdot N_2 \cdot m_{M_2} + y_{M_2} \cdot M_2 \cdot m_{N_2} \pmod{n}$$
$$r_2 = n - r_1$$
$$r_3 \equiv y_{N_2} \cdot N_2 \cdot m_{M_2} - y_{M_2} \cdot M_2 \cdot m_{N_2} \pmod{n}$$
$$r_4 = n - r_3 .$$

If Bob wants to reply to the message of Alice, he obtains the new keys K_2 and K_B using the values of B_2 and A_1 and continues the algorithm executed by Alice. He computes K_B with his key value q and computes K_2 with the help of p. If Alice wants to continue the encryption process, Alice selects N_3, N_4, $N_3 = 4t+1$, $N_4 = 4t+3$, where N_3, N_4 are the first prime numbers occurring just after N and Bob selects M_3 and M_4, where M_3, M_4 are the first primes of the form $4t+1$ and $4t+3$ occurring just after M. The keys K_i, K_A, K_B are computed as before and thus these keys are dynamic.

6. WORKING OF THE SYSTEM

Assume that the system uses a 29-letter alphabet

a	b	c	⋯	x	y	z	_	.	?
↓	↓	↓	⋯	↓	↓	↓	↓	↓	↓
00	01	02	⋯	23	24	25	26	27	28

Consider the case, the irrational number $I = \pi$ and let $N = 28816$ and $M = 47635$. Then

$$(N_1, N_2, A_1, B_1) = (28813, 28807, 93, 142)$$
$$(M_1, M_2, A_2, B_2) = (47629, 47623, 195, 98)$$

such that $N_1 = A_1^2 + B_1^2$ and $M_1 = A_2^2 + B_2^2$.

6.1. Encryption

Assume Alice contacts Bob for the first time. She picks the even number B_1 from N_1 and the odd number A_2 from M_1. If B_1, A_2 are feasible numbers, then she computes the decomposition

$B_1 = 142 = 127 + 5 \cdot 3 = p + p_1 \cdot p_2$ for the even number 142 and finds the decomposition, $A_2 = 195 = 181 + 11 + 3 = q + q_1 + q_2$ which exist for feasible numbers by definition. Here Bob's key is 181 and the key of Alice is 127.

First Alice finds the decimal places from the position $q = 181$ in the expansion of π. Now, K_1 =6440229489 549303819644288109756659.... Alice encrypts the confidential message, namely the Plaintext *P="meet at the little schoolhouse"* using K_1 as, each character in the plaintext is shifted with the corresponding numbers in K_1 using (mod 29). Then she computes the initial cryptotext C' with its numerical equivalent and arranges this in columns of length three, as a matrix. This matrix C' is given by,

$$C' = \begin{bmatrix} 18 & 25 & 28 & 16 & 20 & 22 & 06 & 11 & 19 & 00 \\ 08 & 28 & 01 & 09 & 11 & 19 & 19 & 16 & 08 & 25 \\ 08 & 02 & 27 & 01 & 19 & 15 & 15 & 22 & 14 & 09 \end{bmatrix}$$

Alice finds the sequence of decimal places from the position $p = 127$ and chooses $p_1 \cdot p_2 = 15$ consecutive decimals from this position in the expansion of π. This decimal sequence "609550582231725" is arranged in the form of a $5 \times 3 = p_1 \times p_3$ rectangular matrix K_A. This is given by,

$$K_A = \begin{bmatrix} 6 & 0 & 3 \\ 0 & 5 & 1 \\ 9 & 8 & 7 \\ 5 & 2 & 2 \\ 5 & 2 & 5 \end{bmatrix}$$

Then C' is converted into the final cryptotext

$$C \equiv K_A \cdot C' \pmod{29}$$

$$\equiv \begin{bmatrix} 6 & 0 & 3 \\ 0 & 5 & 1 \\ 9 & 8 & 7 \\ 5 & 2 & 2 \\ 5 & 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 18 & 25 & 28 & 16 & 20 & 22 & 06 & 11 & 19 & 00 \\ 08 & 28 & 01 & 09 & 11 & 19 & 19 & 16 & 08 & 25 \\ 08 & 02 & 27 & 01 & 19 & 15 & 15 & 22 & 14 & 09 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 16 & 11 & 17 & 12 & 03 & 03 & 25 & 16 & 11 & 27 \\ 19 & 26 & 03 & 17 & 16 & 23 & 10 & 15 & 25 & 18 \\ 21 & 28 & 14 & 20 & 24 & 20 & 27 & 04 & 14 & 02 \\ 06 & 11 & 22 & 13 & 15 & 04 & 03 & 15 & 23 & 10 \\ 01 & 17 & 16 & 16 & 14 & 20 & 21 & 23 & 07 & 08 \end{bmatrix} \pmod{29}$$

Thus the ciphertext C is *"qtvgbl_?lrrdowqmrunqdqypodxueuz k.dvqpepxlzoxh.scki"*. Note that $|P| = 30$ and $|C| = 50$.

For message integrity, Alice chooses the p_1^{th} p_2^{th} q_1^{th} and q_2^{th} characters in the plaintext namely, "_eee". This message digest with its numerical equivalent $m: 26040404$ is enciphered as w by using $n = N_2 \cdot M_2 = 1371875761$. That is

$$w \equiv m^2 \pmod{n}$$

$$\equiv (26040404)^2 \pmod{n = 1371875761} \equiv 914330048 \pmod{n = 1371875761}$$

Now the ciphertext C and the encrypted message digest w are sent to Bob through an open channel.

6.2. Decryption

Bob can compute the rectangular matrix K_A by applying the key p of Alice to the decimal expansion of π. Then he obtains the pseudo inverse of K_A,

$$K_A{}^{\#} \equiv \left(K_A{}^T K_A\right)^{-1} K_A{}^T \pmod{29} \equiv \begin{bmatrix} 25 & 25 & 26 & 05 & 17 \\ 13 & 06 & 15 & 08 & 19 \\ 14 & 15 & 13 & 11 & 01 \end{bmatrix} \pmod{29}$$

He divides the ciphertext C into clocks of length five and decrypts it by applying $K_A{}^{\#}$ to C, $C' \equiv K_A{}^{\#} C \pmod{29}$. He computes the decimal sequence K_1, starting from the position q in the decimal expansion of π. These decimal places are used to decrypt C' by the inverse substitution cipher and Bob obtains the original secret message $P = "meet\ at\ the\ schoolhouse"$.

For decryption of the message digest, Bob finds

$$m_{N_2} \equiv w^{\frac{(N_2+1)}{4}} \pmod{N_2} \equiv 1124 \pmod{28807}$$

$$m_{M_2} \equiv w^{\frac{(M_2+1)}{4}} \pmod{M_2} \equiv 38246 \pmod{47623}$$

$y_{N_2} = 2083,\ y_{M_2} = -1260$ such that $y_{N_2} \cdot N_2 + y_{M_2} \cdot M_2 = 1$ and it returns the four possible roots,

$$r_1 \equiv y_{N_2} \cdot N_2 \cdot m_{M_2} + y_{M_2} \cdot M_2 \cdot m_{N_2} \pmod{n} \equiv 950545703$$
$$r_2 = n - r_1 = 421330058$$
$$r_3 \equiv y_{N_2} \cdot N_2 \cdot m_{M_2} - y_{M_2} \cdot M_2 \cdot m_{N_2} \pmod{n} \equiv 26040404$$
$$r_4 = n - r_3 = 1345835357$$

Among these four, r_3 gives him the original message digest. Bob can confirm it by considering the letters in the $p_1, p_2, q_1, q_2{}^{th}$ place of the plaintext P. Bob can reply to Alice by using the $(odd, even)$ pair key (A_1, B_2) as before. This process is then continued by Alice using the new prime pairs (N_3, N_4) and (M_3, M_4) and it can be repeated any number of times as long as the initial numbers N, M are kept secret.

7. CONCLUSION

The cryptosystem proposed here is quite secure as it is difficult to obtain the keys K_i, K_A and K_B without knowledge of N and M. As the prime pairs (N_1, N_2) and (M_1, M_2) changes for each encryption, the keys K_i, K_A and K_B are dynamic and hence the system is secure against chosen plaintext attack. It also ensures the authenticity of the messages transferred between the sender and the receiver as t is locked with the keys of Bob and Alice. The Rabin's cryptosystem without the modulus being made public, is used in encrypting the message digest and it ensures the integrity of the message transferred.

The use of the integers appearing in the decimal expansion of π (not made public) in encryption/decryption, enables it to be safe against the usual methods of cryptographic attacks. As long as N and M are not known it is impossible for an intruder to break this system. If an intruder pretends as Alice and sends Bob a message, Bob can send a standard text for encryption. The ciphertext of this standard message from the intruder, enables Bob to assert the authenticity of the intruder.

The proposed data encryption scheme given above has advantages of large key space, high level security and is mathematically and computationally simple like [5], [18]. The system is secure against brute force attack since the keys are dynamic and the length of the plaintext and the ciphertext are not equal. Thus the system is secure against all possible known attacks.

REFERENCES

[1] A.J. Menezes, P.C. Van Oorchot and S.A. Vanstone, *"Handbook of Applied Cryptography"*, CRC Press, 2000.
[2] John Mark B. Espalmado and Edwin R. Arboleda, "Dare Algorithm: A New Security Protocol by Integration of Different Cryptographic Techniques," *International Journl of Electrical and Computer Engineering*, vol. 7, no. 2, pp. 1032-1041, 2017.
[3] Neal Koblitz, *"A course in Number Theory and Cryptography"*, Springer, 2nd edition, 1994.
[4] Rhee and Man Young, *"Cryptography and Secure Communications"*, McGraw - Hill co., 1994.
[5] M.K. Viswanath and M. Ranjithkumar, "A secure cryptosystem using the decimal expansion of an Irrational number," *Applied Mathematical Sciences*, vol. 9, pp. 5293-5303, 2015.
[6] M.K. Viswanath and M. Ranjithkumar, "Goldbach Conjecture and Cryptography," *International Journal of Pure and Applied Mathematics*, vol. 116, no. 2, pp. 403-413, 2017.
[7] J.R. Chen, "On the representation of a large even integer as the sum of a prime and the product of atmost two primes," *Kexue Tongbao (Chinese)*, vol. 17, pp. 365-386, 1966.
[8] J.R. Chen, "On the representation of a large even integer as the sum of a prime and the product of atmost two primes," *Sci. Sinica*, vol.16, 1973, pp. 157-176. *Ibid*, 21, 1978, pp.477-494 (Chinese).
[9] I.M. Vinogradov, "The representation of an odd number as a sum of three primes," *Dokl.Akad. Nauk*, SSSR 15, 1937, pp.169-172, Russia.
[10] I.N. Herstein, *"Topic in Algebra"*, 2nd Edition, Wily Eastern Limited.
[11] S. Lester Hill, "Cryptography in an algebraic alphabet," *Amer. Math.*, pp. 306-312, 1929.
[12] R. Penrose, "A generalized Inverse for matrices," Communicated by J.A. Todd Received 26 July 1954.
[13] R.L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems" *Communications of the ACM*, vol. 21, no. 2 pp.120-126, 1978.
[14] Sushma Pradhan and Birendra Kumar Sharma, "An Efficient RSA Cryptosystem with BM-PRIME Method," *International Journal of Information & Security*, vol. 2, no. 1, pp. 103-108, 2013.
[15] Predrag Stanimirovic and Miomir Stankovic, "Determinants of rectangular matrices and Moore-Penrose inverse," *Novi sad J. Math.*, vol .27, no. 1, pp. 53-69, 1997.
[16] T.L. Boullion and P.L. Odell, "Generalized Inverse Matrices," Wiley, Newyork, pp. 41-62, 1971.
[17] J. Pintz and I.Z. Puzsa, "On Linnik's approximation to Goldbach's problem," *I. Acta Arithmatica*, vol. 109, no. 2, pp.169-194, 2003.
[18] M.K. Viswanath and M. Ranjithkumar, "A Public Key Cryptosystem Using Hill's Cipher," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 18, no. 1 & 2, pp. 129-138, 2015.

BIOGRAPHIES OF AUTHORS

M. K. Viswanath was born on 8th April 1950 at Tellicherry, Kerala, India. He took his masters degree M.Sc. in Mathematics from the University of Madras in 1971. He joined as a Tutor in Mathematics at the Madras Christian College immediately after completing the M.Sc. degree. He obtained M.Phil. Degree (Mathematics) in 1979 and the Ph.D. degree (Mathematics) from the University of Madras in the year 1987 for his thesis titled Harmonic Analysis on $SP(2,\square)$ His research interest include Quantum groups, Functional Analysis, Number Theory, Cryptography and Ancient Indian Mathematics. He retired as Reader in Mathematics from the Madras Christian College in May 2008 and thereafter served as Professor of Mathematics at the Rajalakshmi Engineering College, Chennai till May 2016. He is a member of the Cryptographic Research Society of India and the Kerala Mathematics association. He has published 21 research articles in various national and international journals. He is a reviewer for the zbMATH for the past 21 years. He is married and is blessed with two sons.

M. Ranjith Kumar was born on 14th June 1985 at Vellore, Tamil Nadu, India. He is a research scholar in the Department of Mathematics, Bharathiar University, India. He received the M.Sc. degree in Mathematics from University of Madras (RIASM) in 2007. He completed M.Phil. Mathematics from University of Madras in the year 2010. His research mainly focuses on Number Theory and Cryptography. He has published five research articles in various national and international journals.