International Journal of Pure and Applied Mathematics
Volume 116 No. 2 2017, 403-413
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v116i2.12

GOLDBACH CONJECTURE AND CRYPTOGRAPHY

M.K. Viswanath[1], M. Ranjith Kumar[2] §

[1]Department of Mathematics
Rajalakshmi Engineering College, Thandalam
Chennai, 602 105, Tamil Nadu, INDIA

[2]Department of Mathematics
Research and Development Centre
Bharathiar University
Coimbatore, 641 046, Tamil Nadu, INDIA

Abstract: The main object of this paper is to develop 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 the decimal expansion of an irrational number.

AMS Subject Classification: 11T71, 14G50, 68P25, 68R01, 94A60
Key Words: Vinogradov's theorem, Chen's theorem, RSA algorithm, Pseudo inverse

1. Introduction

The field of cryptography and its applications has increased rapidly during the past two decades. The advent of e-commerce and electronic transactions in defence and other sectors has necessitated the need for developing secure communication systems [1]. In ordinary communications an intruder can see all the exchanged messages, can delete, add or alter and redirect messages, can initiate the communication with another party and can re-use messages

Received: May 1, 2017
Revised: June 15, 2017
Published: October 7, 2017

§Correspondence author

from part of communications. Hence cryptographic tools are very crucial in secret communications ([2], [3], [4]), as it prevents unauthorised persons from acquiring stored data exchanged between computers or messages transferred between two mutually authenticated parties.

We demonstrate 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 existing cryptosystems. We make use of theorems of J.R. Chen ([6], [7]) and I.M. Vinogradov [8] in creating the keys K_A and K_B and also the RSA system ([9], [10]) without the modulus being made public, for encrypting the message digest. Readers familiar with the material given in Koblitzs book [11] and pseudo inverse of a rectangular matrix ([12], [13], [14]) and results of Chen and Vinogradov, 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 proposed system.

2. RSA Algorithm

The RSA system is a public key cryptosystem with two keys, one key for encrypting the plaintext and the other key for decrypting the cryptotext. The modulus $n = pq$, is made public. It was created by Ron Rivest, Adi Shamir and Leonard Adleman [9], hence the name RSA. The algorithm is based on the difficulty of factoring large numbers. Public and private keys are functions of a pair of large prime numbers. To generate the two keys:

1. Choose randomly two large primes p and q.
2. Generate the modulus $n = pq$.
3. Choose a random encryption key e, such that e and $\varphi(n) = (p-1)(q-1)$, are relatively prime.
4. Compute the decryption key d such that $e \cdot d \equiv 1 \pmod{\varphi(n)}$.
5. Discard p and q, and make $(n,\ e)$ public.

To encrypt a message, divide it into numerical blocks smaller than n, then the cryptotext of each chunk M_i is: $C_i \equiv M_i^e \pmod{n}$. Decrypting a chunk requires performing the same operation using the key $d : M_i \equiv C_i^d \pmod{n}$.

3. Pseudo Inverse

Definition 1. Let $A \in R^{\mathrm{m} \times \mathrm{n}}$ and $X \in R^{\mathrm{n} \times \mathrm{m}}$, then the following equations are used to define the pseudo inverse of a rectangular matrix A [13].

$$A\,X\,A = A, \tag{1}$$

$$X\,A\,X = X, \tag{2}$$

$$(A\,X)^{T} = A\,X, \tag{3}$$

$$(X\,A)^{T} = X\,A. \tag{4}$$

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

Definition 2. A pseudo inverse of rectangular matrix $A \in R^{\mathrm{m} \times \mathrm{n}}$ is also a rectangular matrix $X = A^{\#} \in R^{\mathrm{n} \times \mathrm{m}}$ satisfying equations (1) through (4). A pseudo inverse is sometimes called the Moore - Penrose inverse [14] after the pioneering work done by Moore (1920, 1935) and Penrose (1955).

3.1. Construction of Pseudo Inverse

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

1. If $m = n$ and $rank\,(A) = m$ then $A^{\#} = A^{-1}$.
2. If $m < n$ and $rank\,(A) = m$ then $A\,A^{T}$ is non-singular and
$$A^{\#} = A^{T}\left(A\,A^{T}\right)^{-1} \tag{5}$$
3. If $m > n$ and $rank\,(A) = n$ then $A^{T}A$ is non-singular and
$$A^{\#} = \left(A^{T}\,A\right)^{-1}A^{T} \tag{6}$$

3.2. Conjecture

1. If A is a rectangular matrix in $R^{\mathrm{m} \times \mathrm{n}}$ formed by the mn consecutive decimal places of any irrational number, with $m < n$, then $rank\,(A) = m$ and A is always right invertible.
2. If A is a rectangular matrix in $R^{\mathrm{m} \times \mathrm{n}}$ 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 [15], *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. 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 [8] that, *All sufficiently large odd integers are expressible as a sum of three primes.* Vinogradov proved the three - primes theorem by analytical means, using a major arc/minor arc decomposition.

4.2. Chen's Theorem

In 1966 Jin Run Chen [6] made considerable progress in settling the even Goldbach conjecture; In [7] 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. Construction of the Proposed Cryptosystem

The main object of this paper is to develop a mutual authentication protocol using theorems of J.R. Chen and I.M. Vinogradov and the decimal expansion of an irrational number, which provides confidentiality, integrity and authenticity of the information shared over a public channel. This work is a novel method of developing a communication protocol, which is safe against all the known attacks. The protocol is as follows:

We are looking for numbers which satisfy the following decomposition 1 and 2 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 $100 = 79+7\cdot3$, $101 = 89+7+5$, $1002 = 967+5\cdot7$, $999 = 991+3+5$, $150 = 73 + 7 \cdot 11$, $151 = 139 + 5 + 7$, $1029 = 1021 + 5 + 3$, $1578 = 1543 + 5 \cdot 7$. Bob and Alice choose only feasible numbers for this protocol.

1. 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.

2. If M is 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 prime 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 exchanged over a secure channel.

After ascertaining Alice's identity, Bob asks Alice to send him a large feasible even number. If N_1 is the number sent by Alice to Bob then it is possible to find a decomposition $N_1 = P_1 + r_1 \cdot s_1$, where $r_1 < s_1$ and P_1 is the largest prime satisfying this property. Then Bob chooses a suitable large feasible odd number M_1 (say), then using Vinogradov's theorem $M_1 = Q_1 + r_2 + s_2$, where $r_2 > s_2$, $s_1 = s_2$ and Q_1 is the largest prime satisfying this equation. Bob sends this number M_1 to Alice and she can find the decomposition $M_1 = Q_1 + r_2 + s_2$, and $s_1 = s_2$. Thus, both the users Bob and Alice have the numbers N_1, M_1, and both can compute $(P_1,\ r_1,\ s_1)$ and $(Q_1,\ r_2,\ s_2)$. They keep the pair of three tuples safely with them. Bob and Alice choose an irrational number I for which a decimal expansion up to more than million decimal places are there and I is kept as a secret.

When Alice wants to send a confidential message P to Bob then Alice has the tuples $(P_1,\ r_1,\ s_1)$ and $(Q_1,\ r_2,\ s_2)$ with her, computed from the numbers N_1 and M_1 exchanged over a secure channel.

5.1. Plaintext Encryption Protocol

1. She computes $\alpha_1 \equiv N_1 + M_1 + (r_1 \cdot s_1)^{\delta+1} \pmod{P_1}$ and $\beta_1 \equiv N_1 + M_1 + (r_2 \cdot s_2)^{\delta+1} \pmod{Q_1}$, where δ is a positive integer chosen randomly.

2. Alice computes $r_1\, s_1$ sequence of decimal places from the position α_1 in the expansion of the irrational number I and forms the $r_1 \times s_1$ rectangular matrix K_A.

3. Similarly, she computes the rectangular matrix K_B of order $r_2 \times s_2$ and the entries of K_B are the $r_2 s_2$ consecutive decimal places picked from the position β_1 in the decimal expansion of I.

4. She arranges the plaintext P in blocks of length r_1 with its numerical equivalents and obtains the ciphertext C by:
$C = K_B K_A^{\#}\,\mathrm{P}$.

5.2. Encryption Protocol for Integrity

Alice computes the product $n_1 = P_1 Q_1$ and obtains $\varphi(n_1) = (P_1 - 1)(Q_1 - 1)$. Alice chooses a number e such that, e and $\varphi(n_1)$ are relatively prime. The integrity of the message is maintained by considering the words w_1 and w_2 (say) occurring in the r_1^{th} place and s_1^{th} place of the first sentence in P and considering the words w_3 and w_4 occurring in the r_2^{th} place and s_2^{th} place of the second sentence in P respectively. The compilation of words in the exact order is taken as a message digest. If w_i is a word in the message digest then she encrypts w_i as $m_i \equiv {w_i}^e \pmod{n_1}$, $i = 1,\ 2,\ 3,\ 4$. Now the ciphertext C, the encrypted message digest $m_1 m_2 m_3 m_4$ and the key δ are sent to Bob through an open channel protected by the one-time password(OTP) for decryption. The key pair $(e,\ l)$ is sent to Bob through a secure channel. The OTP used by Alice is $[e \cdot l\,(t_1 + t_2 + t_3 + t_4)]$, where t_1 and t_2 are the numbers occurring in the decimal expansion of I in the r_1^{th} and s_1^{th} place from α_1 and t_3, t_4 are the numbers occurring in the r_2^{th} and s_2^{th} place from β_1 respectively. This is a dynamic password as we use α_1 and β_1 only once for encryption. Similarly Bob sends a reply, with the OTP $[e' \cdot l' \cdot (t_1{}' + t_2{}' + t_3{}' + t_4{}')]$ where $t_1{}'$ and $t_2{}'$ are the numbers occurring in the decimal expansion of I in the r_1^{th} and s_1^{th} place from the position α_2, and $t_3{}'$ and $t_4{}'$ are the numbers occurring in the r_2^{th} and s_2^{th} place from the position β_2 respectively. Here l, l' denotes the length of the ciphertexts sent by Alice and Bob respectively and e' is such that $(e',\ \varphi(n_2)) = 1$ and $n_2 = P_2 Q_2$.

5.3. Decryption Protocol of Integrity

Bob computes the inverse d of e so that $e\,d \equiv 1 \pmod{\varphi(n_1)}$. He then computes $(m_i)^d \pmod{n_1}$, which gives him w_i, $i = 1, 2, 3, 4$. Bob checks the appearance of $w_1,\ w_2,\ w_3$ and w_4 in the appropriate places in the plaintext P and thereby confirms the validity of the ciphertext received.

Assume that the prime numbers from $P_1\,(P_1 < Q_1,$ say) are ordered by the relation $'\ \leq\ '$. If Bob wants to reply to the message of Alice, he selects the

prime numbers P_2, Q_2 occurring immediately after P_1, Q_1 and continues the algorithm given above with the same $r_1,\ s_1$ and $r_2,\ s_2$. Let $N_2 = P_2 + r_1 + s_1$ and $M_2 = Q_2 + r_2 + s_2$, Bob computes $\alpha_2 \equiv N_2 + M_2 + (r_1 \cdot s_1)^{\delta+2} \pmod{P_2}$ and $\beta_2 \equiv N_2 + M_2 + (r_2 \cdot s_2)^{\delta+2} \pmod{Q_2}$ and obtains the new set of keys K_A, K_B. Using these keys he replies to Alice as before. In general for any i, $\alpha_i \equiv N_i + M_i + (r_1 \cdot s_1)^{\delta+i} \pmod{P_i}$ and $\beta_i \equiv N_i + M_i + (r_2 \cdot s_2)^{\delta+i} \pmod{Q_i}$. The keys K_A and K_B changes according to the changing values of the primes P_i, Q_i and with these variable keys Bob and Alice can contact each other continuously without requiring any additional information. The cryptosystem developed here satisfies all the requirements of a secure cryptosystem.

6. Illustration with Small Parameters

Assume that the system used a 29-letter alphabet,

a	b	c	d	$\cdots$	w	x	y	z	_	.	,
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\cdots$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
0	1	2	3	$\cdots$	22	23	24	25	26	27	28

Consider the case $I = \pi,\ \delta = 4,\ e = 17,\ N = 98$ and $M = 101$ are feasible numbers as $98 = 83 + 5 \cdot 3$ and $101 = 89 + 7 + 5$. Therefore, $(P_1,\ r_1,\ s_1) = (83,\ 3,\ 5)$ and $(Q_1,\ r_2,\ s_2) = (89,\ 7,\ 5)$.

Encryption

Assume Alice contacts Bob for first time. Then

$$\alpha_1 \equiv (N_1 + M_1) + (r_1 \cdot s_1)^{\delta+1} \equiv (98 + 101) + (3 \times 5)^{4+1} \equiv 41\,(\mathrm{mod}83)$$

$$\beta_1 \equiv (N_1 + M_1) + (r_2 \cdot s_2)^{\delta+1} \equiv (98 + 101) + (7 \times 5)^{4+1} \equiv 59\,(\mathrm{mod}89)$$

Alice finds the two sequences α and β of decimal places by choosing $r_1 \cdot s_1 = 15$ and $r_2 \cdot s_2 = 35$ consecutive decimal places respectively from the positions $\alpha_1 = 41$ and $\beta_1 = 59$ in the decimal expansion of π. In this case the sequence of decimals are $\alpha = 693993751058209$ and $\beta = 44592307816406286208998628034825342$. She generates the rectangular matrices K_A and K_B of order 3×5 and 7×5

respectively with $\alpha,\ \beta$.

$$K_A = \begin{pmatrix} 6 & 9 & 7 & 0 & 2 \\ 9 & 9 & 5 & 5 & 0 \\ 3 & 3 & 1 & 8 & 9 \end{pmatrix} K_B = \begin{pmatrix} 4 & 7 & 2 & 9 & 4 \\ 4 & 8 & 8 & 8 & 8 \\ 5 & 1 & 6 & 6 & 2 \\ 9 & 6 & 2 & 2 & 5 \\ 2 & 4 & 0 & 8 & 3 \\ 3 & 0 & 8 & 0 & 4 \\ 0 & 6 & 9 & 3 & 2 \end{pmatrix}$$

Then she computes ${K_A}^{\#}$by,

$${K_A}^{\#} \equiv K_A^T \left(K_A K_A^T\right)^{-1} \equiv \begin{pmatrix} 23 & 27 & 22 \\ 4 & 0 & 19 \\ 16 & 11 & 12 \\ 5 & 16 & 7 \\ 17 & 11 & 24 \end{pmatrix} (\bmod 29)$$

Alice encrypts the plaintext P =*Enemy will attack tomorrow, hit the target tonight.* Then the plaintext is divided into blocks of length three with its numerical equivalent,

$$\mathrm{P} = \begin{pmatrix} 4 & 12 & 22 & 11 & 19 & 2 & 19 & 14 & 14 & 26 & 19 & 7 & 19 & 6 & 26 & 13 & 7 \\ 13 & 24 & 8 & 26 & 19 & 10 & 14 & 17 & 22 & 7 & 26 & 4 & 0 & 4 & 19 & 8 & 19 \\ 4 & 26 & 11 & 0 & 0 & 26 & 12 & 17 & 28 & 8 & 19 & 26 & 17 & 19 & 14 & 6 & 27 \end{pmatrix}$$

This P is converted into the cryptotext
$C \equiv K_B {K_A}^{\#} P \pmod{29}$

$$\equiv \begin{pmatrix} 24 & 1 & 0 & 18 & 28 & 4 & 9 & 5 & 7 & 23 & 12 & 1 & 13 & 11 & 28 & 3 & 13 \\ 8 & 19 & 25 & 21 & 10 & 5 & 28 & 14 & 1 & 8 & 12 & 21 & 22 & 0 & 17 & 10 & 28 \\ 18 & 10 & 1 & 24 & 23 & 4 & 6 & 8 & 19 & 12 & 13 & 7 & 11 & 11 & 18 & 8 & 8 \\ 0 & 24 & 28 & 11 & 5 & 13 & 28 & 20 & 19 & 17 & 2 & 10 & 2 & 16 & 14 & 24 & 18 \\ 20 & 17 & 13 & 23 & 3 & 1 & 19 & 8 & 12 & 14 & 14 & 27 & 18 & 23 & 22 & 6 & 20 \\ 18 & 7 & 19 & 14 & 5 & 1 & 6 & 1 & 18 & 5 & 18 & 19 & 25 & 7 & 20 & 27 & 21 \\ 24 & 16 & 18 & 24 & 26 & 4 & 5 & 12 & 17 & 18 & 10 & 17 & 22 & 25 & 22 & 3 & 1 \end{pmatrix}$$

Thus the ciphertext C =*yisausybtkyrhqazb,ntssvylxoy,kxfdf_efenbbe j,g,tgffoiuibmhbttmsrximrofsmmncoskbvhktrnwlcszwlalqxhz,rsowuwd kiyg.dn,isuvb.* Note that $|\mathrm{P}| = 51 \neq 119 = |C|$.

For message integrity, Alice chooses the 3^{rd} and 5^{th} words in the plaintext namely "*attackhit*" as the plaintext is only a message with one sentence. This message digest is broken into of two letters "$(at)\,(ta)\,(ck)\,(\_h)\,(it)$" with its numerical equivalent given by $(0019)\,(1900)\,(0210)\,(2607)\,(0819)$. Since $e =$

17, the blocks are enciphered with $\varphi(n_1) = (P_1 - 1)(Q_1 - 1) = 7216$, $n_1 = P_1 Q_1 = 7387$.

$$m_1 = {w_1}^e = (0019)^{17} \equiv 7018 \pmod{7387},$$

$$m_2 = {w_2}^e = (1900)^{17} \equiv 2344 \pmod{7387},$$

$$m_3 = {w_3}^e = (0210)^{17} \equiv 6219 \pmod{7387},$$

$$m_4 = {w_4}^e = (2607)^{17} \equiv 0952 \pmod{7387},$$

$$m_5 = {w_5}^e = (0819)^{17} \equiv 1058 \pmod{7387}.$$

Thus the encrypted form of the message digest "*attack hit*" is (7018) (2344) (6219) (0952) (1058). Now the ciphertext C, the encrypted message digest and δ are sent to Bob through an open channel protected by the OTP $[el(t_1 + t_2 + t_3 + t_4)] = 28322$, for decryption. The key pair $(e,\ l) = (17,\ 119)$ is sent to Bob through a secure channel.

Decryption

First Bob unlocks the message pair with the $OTP = 28322$ of Alice, and then finds the rectangular matrices K_A and K_B using α_1 and β_1 in the decimal expansion of I. Then he obtains ${K_B}^{\#}$ as follows:

$${K_B}^{\#} \equiv \left(K_B K_B^T\right)^{-1} K_B^T \equiv \begin{pmatrix} 5 & 24 & 18 & 19 & 12 & 2 & 24 \\ 21 & 25 & 22 & 0 & 26 & 20 & 18 \\ 25 & 14 & 15 & 19 & 20 & 17 & 14 \\ 28 & 22 & 18 & 11 & 8 & 10 & 25 \\ 24 & 26 & 13 & 17 & 12 & 17 & 2 \end{pmatrix} \pmod{29}$$

He divides the ciphertext into blocks of length seven and decrypts C by applying $K_A {K_B}^{\#}$ to C and obtain the plaintext $P =$"*Enemy will attack tomorrow, hit the target tonight.*". For the decryption of the message digest, Bob finds the multiplicative inverse $d = 849$ of $e = 17$ such that $e \cdot d \equiv 1 \pmod{7216}$. Then he decrypts the entire message digest by computing $w_i = (m_i)^{849} \pmod{7387}$, $i = 1,\ 2,\ \ldots,\ 5$, which gives him the original message digest "*attack hit*". Bob can reply to Alice by using the prime numbers occurring immediately after 83 and 89. This process is then continued by Alice, and can be repeated any number of times as long as the initial numbers N_1, M_1 are kept as secret.

7. Conclusion

The cryptosystem proposed here is quite secure as it is difficult to obtain the keys K_A and K_B without the knowledge of N and M. As the primes P_i, Q_i changes for each encryption, the keys K_A and K_B are dynamic and hence the system is secure against chosen plaintext attack.

The use of Diffie-Hellman key agreement $K_B K_A{}^{\#}$ and $K_A K_B{}^{\#}$ for encryption and decryption respectively, ensures the authenticity of the messages transferred between the Sender and the Receiver. Using the RSA system, without the modulus being made public, in encrypting the message digest, ensures the integrity of the message transferred. 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 along with an odd number. The ciphertext of this standard message from the intruder, enables Bob to find 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 the one given in ([4], [5], [16]).

The system is secure against Brute force attack since the number of keys are large and the length of the plaintext and the ciphertext are not equal. Thus the system is secure against all possible known attacks.

References

[1] Man Young Rhee, *Cryptography and Secure Communications*, McGraw-Hill Series on Computer Communications, Singapore (1994).

[2] M. Eisenberg *Hill ciphers and Modular Linear Algebra*, Mimeographed Notes, University of Massachusetts, USA (1998).

[3] I.A. Ismail, M. Amin and H. Diab, How to repair the Hill cipher, *Journal of Zhejiang University Science*, **7**, No. 12 (1998), 2022-2030.

[4] S. Lester Hill, Cryptography in an algebraic alphabet, *The American Mathematical Monthly*, **36** No. 6 (1929), 306-312.

[5] M.K. Viswanath and M. Ranjithkumar, A secure cryptosystem using the decimal expansion of an Irrational number, *Applied Mathematical Sciences*, **9**, No. 106 (2015), 5293-5303.

[6] 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)*, **17** (1966), 365-386.

[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, *Sci. Sinica*, **16** (1973), 157-176.

[8] I.M. Vinogradov, The representation of an odd number as a sum of three primes, *Dokl. Akad. Nauk. SSSR*, **16** (1937), 139-142.

[9] R.L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM*, **21**, No. 2 (1978), 120-126.

[10] A.J. Menezes , P.C. Van Oorchot and S.A. Vanstone *Handbook of Applied Cryptography*, CRC Press, USA (2000).

[11] Neal Koblitz, *A course in Number Theory and Cryptography*, Springer, USA (1994).

[12] T.L. Boullion and P.L. Odell, *Generalized Inverse Matrices*, Wiley, New York (1971).

[13] R. Penrose, A generalized Inverse for matrices, *Pvoc. Cambridge Phil. SOC*, **51** (1955), 406-413.

[14] Predrag Stanimirovic and Miomir Stankovic, Determinants of rectangular matrices and Moore-Penrose inverse, *Novi sad J.Math.*, **27**, No. 1 (1997), 53-69.

[15] J. Pintz and I.Z. Puzsa, On Linnik's approximation to Goldbach's problem, *I. Acta Arithmatica*, **109**, No. 2 (2003), 169-194.

[16] M.K. Viswanath and M. Ranjithkumar, A Public Key Cryptosystem Using Hills Cipher, *Journal of Discrete Mathematical Sciences and Cryptography*, **18**, No. 1-2 (2015), 129-138.