International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

FORMULATION OF A SECURE COMMUNICATION PROTOCOL AND ITS IMPLEMENTATION

M. Ranjith Kumar

Department of Mathematics, Jeppiaar Institute of Technology, Sriperumbudur, Chennai – 631 604.

Abstract - *The main objective of this paper is to develop a two-party mutual authentication protocol providing secure communications, focusing on those using a symmetric techniques. In this paper a cryptosystem with authentication and data integrity, using the Goldbach conjecture and the decimal expansion of an irrational number is obtained.*

Key Words: Hill cipher, RSA algorithm, Pseudo inverse of a rectangular matrix, Goldbach conjecture and Chen's theorem.

1. INTRODUCTION

In our information age, the need for protecting information is more pronounced than ever. Secure communication for the sensitive information is not only compelling for military of government sectors but also for the business and private individuals. As the world becomes more connected, the dependency on electronic services has become more pronounced. In order to protect valuable data in communication systems from unauthorized disclosure ad modification, reliable non-interceptable means for data storage and transmission must be adopted.

In a communications[14], an intruder can see all the exchanged messages, can delete, alter, inject and redirect messages, can initiate the communications with another party, and can re-use messages from past communications. Hence the two communicating parties, exchanging a number of messages at the end of which they have assurances of each other's identities. In an authenticated key exchange, there is the additional goal that the two parties end up sharing a common key known only to them. This secret key can then be used for some time thereafter to provide privacy, data integrity or both.

We demonstrate in this paper how the above capabilities are incorporated in the communication system developed here using an idea proposed in [22]. However, some of the techniques that we use are quite different from the usual ones and make use of Goldbach conjecture [3, 4, 17] and new variants of RSA problem [15]. This resulting system provide relatively small block size, high speed and high security. Mainly, this paper surveys the development of symmetric key cryptosystem form their inception to present day implementations. Readers familiar with Hill Cipher, Pseudo inverse of a rectangular matrix, RSA algorithm and Goldbach conjecture may directly go to section seven for the working of our algorithm. Finally, the paper is finished of a small illustration, security analysis and the conclusion of the proposed system.

2. HILL n-CIPHER

Hill cipher was first introduced by Lester S. Hill in 1929 in the journal *The American Mathematical Monthly* [**5, 8]**. Hill cipher is the first polygraphic cipher. A polygraphic cipher is a cipher where the plaintext is divided into blocks of adjacent letters of the same fixed length *n*, and then each such block is transformed into a different block of n-letters. This polygraphic feature increased the speed and the efficiency of the Hill cipher. Besides, it has some other advantages in data encryption such as its resistance to frequency analysis. The core of Hill cipher is matrix multiplication. It is a linear algebraic equation $C \equiv KP \left(\bmod N \right)$, where C represent the ciphertext block, P represent the plaintext block, K is the key matrix and N is the number of alphabets used. The key K is a $n \times n$ matrix and what is needed for decryption, is the inverse key matrix K^{-1}.

3. Digital Signature

A digital signature is an electronic signature that can be used to authenticate the identity of the sender or the signer of a document, and to ensure the original content of the message or document that has been sent are unchanged **[9]**. The digital signature provides the following three features:

3.1 Authentication

Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.

3.2 Integrity

In many cases, the sender and the receiver of a message need assurance that the message has not been altered during transmission. Digital signatures provide this feature by using cryptographic message digest functions.

3.3 Non-Repudiation

Digital signatures ensure that the sender who has signed the information cannot at a later date deny having signed it.

4. RSA ALGORITHM

RSA is a public key algorithm which generates two keys and allow data encrypted with one of them to be decrypted with the other. It was created by Ron Rivest, Adi Shamir and Leonard Adleman [15], 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

i. Choose two random large primes p and q.
ii. Generate the modulus n=p.q
iii. Choose a random encryption key, e such that e and $\varphi(n)=(p-1)(q-1)$ are relatively primes.
iv. To compute the decryption key d such that $ed\equiv 1\left(\bmod \varphi(n)\right)$.
v. Discard p and q.

To encrypt a message, divide it into numerical blocks smaller than n, encryption 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: $M_i\equiv C_i^d \pmod n$.

5. THE GOLDBACH CONJECTURE

In a letter to Euler dated 7 June of 1742, Goldbach stated the following conjectures [12]:

*"If N is an integer such that $N=p_1+p_2$, with p_1 and p_2 are primes, then for every $2\le k\le N$,
$N=p_1+p_2+\cdots+p_k$ with $p_1, p_2, \cdots, p_k$ are primes."*

We have to keep in mind that in Goldbach's time the number 1 was considered to be a prime, in contrast with the modern definition. In the margin of the same letter, Goldbach stated another conjecture,

"If N is an integer greater than 2, then $N=p_1+p_2+p_3$, with p_1, p_2 and p_3 are primes."

In this reply letter, dated 30 June of the same year, Euler wrote a third conjecture which is ascribed to Goldbach.

"If N is a positive even integer, then $N=p_1+p_2$ with p_1 and p_2 are primes."

Today, these three conjecture are known to be equivalent, while the modern version of the third conjecture is the famous Goldbach conjecture [12].

Although Goldbach conjecture is still an open conjecture to show that all even numbers are expressible as a sum of two primes, the case for odd numbers is easier.

5.1 Chen's theorem

In 1996 Chen Jing Run [3] made a considerable progress in the research of the binary Goldbach conjecture; in [4] he proved the well-known Chen's theorem:

"Let N be a sufficiently large even integer then the equation $N=p+P$ is solvable, where p is a prime and P is an almost prime with atmost two prime factors."

Chen's theorem is a giant step towards the Goldbach conjecture, and a remarkable result of the Sieve methods.

6. CONSTRUCTION OF THE PROPOSED CRYPTOSYSTEM

The main objective of this paper is to develop a two party mutual authentication protocol using Goldbach conjecture and the decimal expansion of an irrational number, which provide confidentiality, integrity and authenticity of the informatics shared over a public channel. This work is a novel method of developing a two party communication protocol which prevents from all the known attacks. The protocol is as follows:

Bob and Alice chooses two large numbers (even) and exchanges it over a secure channel. The above Chen's theorem guarantee the existence of two primes *P* and *Q* from the numbers *N* and *M* (say) exchange over secure channel. We exploit the theorem of J.R.Chen, obtaining the primes *P* and *Q* where integers *N* and *M* are given. Suppose *N* is even, then choose the largest prime *P* such that $N=P+r_1s_1$ where r_1 and s_1 are suitable primes. As *N* and *M* are exchanged over a secure channel only. Bob and Alice are aware of it for example if N=100, then 100=79+7.3.

After ascertaining Alice's identity, Bob asks Alice to send him a largest even number N_i. Then by Chen's theorem Alice sends the even number N_i to Bob, N_i can be expressed as $N_1=P_1+r_1.s_1$ where $r_1<s_1$. Then Bob chooses a suitable even number M_i such that Q_i is the largest prime that satisfies $M_1=Q_1+r_2.s_2$ and $r_2>s_2$ and $s_1=s_2$. Bob sends this number M_i to Alice. Thus both the users Bob and Alice have the numbers N_i and M_i and both compute (P_1, r_1, s_1) and (Q_1, r_2, s_2). They keep this three tuples with them respectively. Bob and Alice chooses an irrational number I which has a decimal expansion upto more than million places of decimals.

When Alice wants to send a confidential message *P* to Bob then Alice has both tuples (P_i, r_1, s_1) and (Q_i, r_2, s_2) with her even though the numbers exchanged over the secure channel are N_i and M_i.

6.1 Plaintext encryption protocol:

a. Alice computes $\alpha_1 = N_1.M_1 + (r_1.s_1)^{\delta+j} \pmod{P_1}$ and $\beta_1 = N_1.M_1 + (r_2.s_2)^{\delta+j} \pmod{Q_1}$. She chooses an integer δ randomly. Here j denotes the number of messages exchanged between Alice and Bob. The keys δ and j are security parameters.

b. She computes $r_1 s_1$ sequence of decimal places from the position α_i in the expansion of the irrational number *I* and forms the $r_1 \times s_1$ rectangular matrix K_A.

c. Similarly she computes the rectangular matrix K_B using Bob's number M_i. where K_B is a $r_2 \times s_2$ rectangular matrix and the entries of K_B are the $r_2 s_2$ consecutive decimal places picked from β_i in the decimal expansion of I.

d. She arranges the plaintext P in blocks of length r_1 with its numerical equivalents and the ciphertext C is obtained by $C = K_B K_A^{\#} P$.

6.2 Encryption protocol for integrity

Alice computes the product $n_i = P_i Q_i$ and finds $\varphi(n_1) = (P_1 - 1)(Q_1 - 1)$. Alice chooses a number e such that $(e, \varphi(n_1)) = 1$. The integrity of the message is maintained by considering the words occurring in the r_1th place and s_1th place of the first sentence in P and considering the words occurring in the appropriate places of the second sentence using the number M_i. 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 $m_i = w_i^e \pmod{n_1}$. She sends the encrypted and the password protected message pair $(C, m_1 m_2 m_3 m_4, \delta)$ to Bob along with the key pair (e, l). The one time password (OTP) used for protection by Alice is $[el(t_1 t_2 t_3 t_4)]$ where t_1 and t_2 are the numbers occurring in the decimal expansion of *I* in the r_1th and s_1th place of α_i respectively, and t_3 and t_4 are the numbers occurring in the r_2th and s_2th place from β_i respectively. This is a dynamic passwords as we use α_i and β_i are only once for encryption. Similarly when Bob sends a reply with the OTP is $[dl'(t'_4 t'_3 t'_2 t'_1)]$ where t'_1 and t'_2 are the numbers occurring in the decimal expansion of I in the r_1th and s_1th place of α_i respectively, and t'_3 and t'_4 are the numbers occurring in the r_2th and s_2th place from β_i respectively. Here l denotes the length of the ciphertext.

6.3 Ciphertext decryption protocol:

a. Once Bob receives the password protected message pair $(C, m_1 m_2 m_3 m_4, \delta)$ along with the key pair (e, l), he first unlock it with the respective OTP $(e(t_1 t_2 t_3 t_4) l)$.

b. He checks the length of ciphertext C and confirms whether $|C| = l$.

c. Bob knows α_i and β_i, and so he can computes both the keys K_A and K_B.

d. He applies the key $K_A K_B^{\#}$ to C, obtaining the original plaintext by $P = K_A K_B^{\#} C$.

e.

6.4 Decryption protocol for integrity:

Bob computes the multiplication inverse *d* of *e* such that $ed \equiv 1 \pmod{\varphi(n_1)}$. He then computes $(m_1)^d \pmod{n_1}$ which gives him w_i. Bob checks the appearance of w_1, w_2, w_3 and w_4 in the appropriate places in the plaintext P and can confirm the validity of the ciphertext obtained. Bob can reply to Alice by using the prime numbers occurring immediately after P_i and Q_i. Since the prime numbers are changing the N_i and M_i, keys K_A and K_B changes rapidly and thus way one can contact each other continuously without providing any additional information. The cryptosystem developed here is a secure communication protocol satisfying all the requirements of a good cryptosystem.

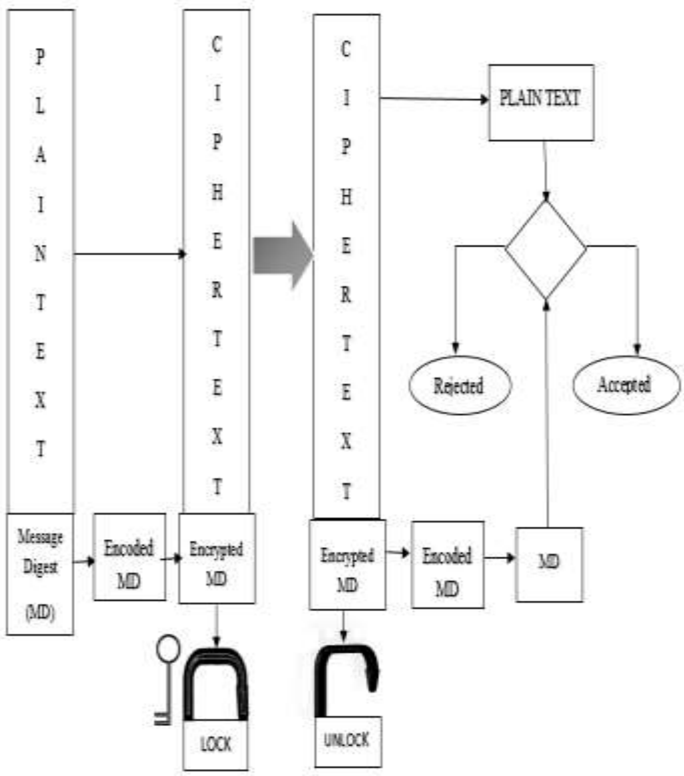

Fig -1: Algorithm Structure

7. ILLUSTRATION

Assume that the system uses a 29-letter alphabet

$$\begin{array}{cccccccccc} a & b & c & d & \dots & y & z & \_ & . & ! \\ \downarrow & \downarrow & \downarrow & \downarrow & \dots & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 & 3 & \dots & 24 & 25 & 26 & 27 & 28 \end{array}$$

Consider the case the irrational number $I=\pi$, e=17, $\delta=4$, $N_1=98$ and $M_1=1002$ then $(P_1, r_1, s_1)=(83,3,5)$ and $(Q_1, r_2, s_2)=(967,7,5)$

Encryption:

Assume Alice contacts Bob for first time, therefore $j=1$. Then

$$\alpha_1 \equiv (N_1 \times M_1)+(r_1 s_1)^{\delta+1} \equiv (98\times 1002)+(3\times 5)^{4+1} \equiv 15 \pmod{83}$$

$$\beta_1 \equiv (N_1 \times M_1)+(r_2 s_2)^{\delta+1} \equiv (98\times 1002)+(7\times 5)^{4+1} \equiv 766 \pmod{967}$$

Alice finds the two sequences of decimal places from the positions of $\alpha_1=15$ and $\beta_1=766$, and chooses $r_1.s_1=15$ and $r_2.s_2=35$ consecutive decimals say α and β respectively from this position in the decimal expansion of π. In this cases the sequence of decimals are $\alpha=693993751058209$ $\beta=44592307816406286208998628034825342$. She generates the two rectangular matrices K_A and K_B of order 3×5 and 7×5 respectively from α and β.

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

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

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

Alice encrypts the secret plaintext P="*Enemy will attack tomorrow, hit the target tonight.*" Then the plaintext is divided into blocks of length three with the numerical equivalent and apply the plaintext encryption process $C\equiv K_B K_A^{\#} P \pmod{29}$ which gives the ciphertext C,

"*yisausybtkyrhqazb,ntssvylxoy,kxfdfefenbbej,g,tgffoiuibmhbt tmsrximrofsmmncoskbvhk.trnwlcszwlalqxhz,rsowuwdkiyg.d n,isuvb*".

Note that $|P|=51\neq 119=|C|$.

For message integrity, Alice chooses 3rd and 5th words in the plaintext are "*attack hit*" and she can encode two letters per block, substituting a two digit numerical value for each letter. Thus the message "(at)(ta)(ck)(_h)(it)" is encoded: (0019)(1900)(0210)(2607)(0819). Since e=17, the blocks are enciphered with $n_1=P_1Q_1=80261$, $\varphi(n_1)=(P_1-1)(Q_1-1)=79212$.

$$m_1=w_1^{\,e}=(0019)^{17}\equiv 7018 \pmod{80261},$$
$$m_2=w_2^{\,e}=(1900)^{17}\equiv 2344 \pmod{80261},$$
$$m_3=w_3^{\,e}=(0210)^{17}\equiv 6219 \pmod{80261},$$
$$m_4=w_4^{\,e}=(2607)^{17}\equiv 0952 \pmod{80261},$$
$$m_5=w_5^{\,e}=(0819)^{17}\equiv 1058 \pmod{80261}.$$

The whole message enciphered as

(7018)(2344)(6219)(0952)(1058).

Now the encrypted plaintext and message digest pair protected by the password $\left(e(t_1+t_2+t_3+t_4)l\right)=\left(17\times(3\times 9\times 2)\times 119\right)=2109242$ is sent to Bob for decryption along with the key tuple $(e,l,\delta)=(17,119,4)$.

Decryption:

First Bob unlocks the message pair using the prearranged password 28322 and 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 as $P\equiv K_A K_B^{\#} C \pmod{29}$. Which gives the original plaintext P: "Enemy will attach tomorrow, Hit the target tonight."

The decryption of the message digest, Bob finds the multiplication inverse d=849 of e=17 such that $ed \equiv 1 \pmod{7018}$. Then he decrypts the entire message digest by computing $w_i = (m_i)^{849} \pmod{80261}$, which gives the decrypted original message digest "attack hit".

8. CONCLUSIONS

We have proposed a method for implementing a cryptosystem whose security rests in part on the difficulty of finding the encryption/decryption keys. The security of our method proves to be adequate, it permits secure communication to be established without the use of couriers to carry the actual keys, as the keys and password used are dynamic and it also permits authentication, non-repudiation and message integrity of digitized documents.

The security of this system needs to be examined in more detail. In particular, the use of integers appearing in the decimal expansion of π in the encryption will make the decryption difficult by the usual methods of cryptography. The encryption/decryption keys known only to both Bob and Alice, it is not possible for any intruder to break this system. Also since N and M changes each time during an encryption, and also the encryption/decryption keys K_A and K_B are dynamic, hence the system is secure against known-plaintext attack. The proposed data encryption scheme given above has advantages of large key space, high level security and is mathematically and computationally simple, unlike the existing cryptosystems.

The proposed system also takes care of data integrity and authentication. Even if an intruder pretends as Alice and sends Bob a message, Bob can send a standard message to the intruder for encryption along with the key (e, l, δ) different form the one already used. The ciphertext of the standard message form the intruder will en able Bob to determine the authenticity of the intruder. This system is very secure against Brute-force attacks, since the number of possible keys are very large. Length of the plaintext and ciphertext are nor equal, hence does this system prevent from frequency attack. And also this system is secure against all possible known attacks.

REFERENCES

1) **M. Bellare, R. Canetti and H. Krawczyk**, Keying hash functions for message Authentication. In N. Koblitz, editor, CRYPTO'96, vol.1109 of LNCS, Pages 1-15, Springer-Verlag, 1996.

2) **T.L. Boullion and P.L. Odell**, Generalized Inverse Matrices. Wiley, Newyork, pages 41-62, 1971.

3) **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.

4) **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. Ibid, 21, 1978, 477-494 (Chinese).

5) **M. Eisenberg,** Hill ciphers and Modular Linear Algebra. Mimeographed Notes, University of Massachusetts, 1998.

6) **Howard Anton and Rorres chris**, Elementary Linear Algebra. 8th edition, Newyork: John-Wiley & Sons Inc., pages 678-688, 2000.

7) **I.A. Ismail, M. Amin and H. Diab,** How to repair the Hill cipher. Journal of Zhejiang University Science vol.7, no.12, 2006.

8) **S. Lester Hill,** Cryptography in an algebraic alphabet. Amer. Math., pages 306-312, 1929.

9) **A.J. Menezes, P.C. Van Oorchot and S.A. Vanstone,** Handbook of Applied Cryptography. CRC Press, 2000.

10) **Neal Koblitz,** A course in Number Theory and Cryptography, Springer, 2nd edition, 1994.

11) **R. Penrose,** A generalized Inverse for matrices. Communicated by J.A. Todd Received 26 July 1954.

12) **J. Pintz and I.Z. Puzsa,** On Linnik's approximation to Goldbach's problem, I. Acta Arithmatica, 109(2), 2003, 169-194.

13) **Predrag Stanimirovic and Miomir Stankovic,** Determinants of rectangular matrices and Moore-Penrose inverse. Novi sad J.Math., Vol.27, No.1, pages 53-69, 1997.

14) **Rhee and Man Young,** Cryptography and Secure Communications. McGraw - Hill co., 1994.

15) **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 pages 120-126, 1978.

16) **A. Selberg,** An elementary proof of the Prime-number theorem, Ann. Of Math, (2), 50, 1949, 305-313.

17) **I.M. Vinogradov,** The representation of an odd number as a sum of three primes, Dokl.Akad. Nauk, SSSR 15, 1937, 169-172, Russia.

18) **M.K. Viswanath,** Transcendental Numbers and Cryptography. Applied Mathematical Sciences, Vol. 8, no. 174, pages 8675 – 8677, 2014.

19) **M.K. Viswanath and A.R. Deepti,** An improvised version of Hill's Cipher. Journal of Discrete Mathematical Sciences and Cryptography, volume 11, No.2, India, 2008.

20) **M.K. Viswanath and A.R. Deepti,** A New Approach to a Secure Cryptosystem using the Microcontroller, Journal of Information Assurance Security, Volume 1, Issue 4, USA, 2006.

21) **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, pages. 129–138, 2015.

22) **M.K. Viswanath and M. Ranjithkumar,** A secure cryptosystem using the decimal expansion of an Irrational number. Applied Mathematical Sciences, Vol. 9, pages 5293-5303, 2015.