Simulation and comparative analysis of modified RSA algorithm with Hill Cipher Algorithm

Dharitri Talukdar[1], Prof. (Dr.) Lakshmi Prasad Saikia[2]

[1] *PhD Research Scholar, Department of CSE, Assam down town University, Assam, India*
[2] *Professor , Dept. of Computer Sc. & Engineering, Assam down town University, Assam, India*

Abstract - *One of the principal challenges of resource sharing on data communication network is its security. The study discovers the progress of Encryption algorithms in terms of their diversity of applications. Some of the Encryption algorithms have been developed to make transmission and storage of data more secured and confidential. Different levels of securities are offered by different algorithms depending on how difficult is to break them. If it is difficult to recover the plain text in spite of having substantial amount of cipher text then an algorithm is unconditionally secured. In this paper we come with new design of encryption and decryption algorithm based on modified RSA whose output have been compared with Hill cipher using MATLAB.*

Key Words: Algorithm, RSA, Hill cipher, Encryption, Decryption, Cryptography.

1. INTRODUCTION

Cryptography is playing a major role in data security in applications running in a network environment. It allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender. It has become more critical to our day-to-day life because thousands of people interact electronically every day; through e-mail, e-commerce, ATM machines, cellular phones, etc. Thus security is more important with increasing interaction of applications running in a network environment.

1.1 *RSA:* One of the well known public key cryptosystems firstly described in 1977 for encryption of blocks of data, key exchange or digital signatures is the Rivest-Shamir-Adleman (RSA) cryptosystem. The level of speed and security of RSA algorithm is affected by some important parameters. The complexity of decomposing RSA algorithm into its factors increases by increasing the modulus length which plays an important role, due to which the length of private key will increase and so hard to be decrypted without decryption key.

The length of encrypted message will comparatively change if the length of message is changes. While studying [3] when the era of electronic email was awaited to arise that time RSA was introduced. Two important ideas were implemented by it-

Public-Key Encryption: The person with the correct decryption key can decipher an encrypted message because in RSA algorithm, encryption keys are public, but the decryption keys are not.Digital Signatures: It is

important for the receiver to verify that transmitted messages are actually originated from the sender (signature), and have not just come from there (authentication). It is done with the sender's decryption key, using the corresponding public encryption key later the signature can be verified by anyone. Therefore the signatures cannot be forged. So, no signer can later refuse having signed the message.

1.2 Digital signatures in practice [8]

For digital signatures to be useful in practice, concrete realizations of the preceding concepts should have certain additional properties. A digital signature must-

Be easy to compute by the signer (the signing function should be easy to apply);

Be easy to verify by anyone (the verification function should be easy to apply); and Have an appropriate lifespan, i.e., be computationally secure from forgery until the signature is no longer necessary for its original purpose.

1.3 The RSA Algorithm

1.Key generation:

Select random prime numbers p and q, and check p! =q.

Compute modulus n=p*q.

Compute phi, Ø= (p-1)(q-1).

Select public exponent e, 1<e<Ø such that gcd (e, Ø)=1.

Compute private exponent, (d*e) mod Ø=1.

Public key is {n, e}, private key{d}.

1)Encryption:

c = (m^e) mod n.

1) **Decryption:**

m = (c^d) mod n.

Digital signature:

s = (H(m)^d)mod n

2) **Verification**:

m=(s^e) mod n.

If m‟=H(m) signature is correct.

H is publicly known hash function

1.3. Proposed RSA:

The proposed approach is instead of using two prime numbers to generate public and private key, we will going to generate five prime numbers with reduced size which will generate variable N with large size. Hence factorization in this case will be more difficult than original algorithm. The three phases are as follows-

- Key generation
- Encryption
- Decryption

Key generation:

- Select five prime numbers- p, q, r, s and t.
- Calculate n=p*q*r*s*t.
- Calculate phi = (p-1)*(q-1)*(r-1)*(s-1)*(t-1).
- Select an integer e such that 1<e<phi and GCD (e, phi) = 1; e and phi are co prime.
- Choose a number relatively prime to phi and call it d.
- Find d such that e*d=1mod phi

Encryption:

Cipher text, C= M^e mod n

Decryption:

Plain text, M= C^d mod n

1.5 Hill cipher algorithm

The core of hill cipher algorithm is matrix multiplication. It is a multi-letter cipher, developed by the mathematician Lester Hill in 1929 [12].

For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In Hill cipher, each character is assigned a numerical value like:

a=0, b=1,……………………..z=25

The substitution of cipher text letters in place of plaintext leads to m linear equations. For m=3, the system can be described as follows:

C1= $(K_{11}P1+K_{12}P2+K_{13}P3)$MOD26

C2= $(K_{21}P1+K_{22}P2+K_{23}P3)$MOD26

C3= $(K_{31}P1+K_{32}P2+K_{33}P3)$MOD26

This can be expressed in terms of column vectors and matrices:

C=KP

Where C and P are column vectors of length 3, representing the plaintext and the cipher text and K is a 3*3 matrix, which is the encryption key. All operations are performed mod 26 here. Decryption requires the inverse of matrix K. The inverse K-1 of a matrix K is defined by the equation.

K K-1= I where I is the Identity matrix.

K-1 is applied to the cipher text, and then the plain text is recovered. In general terms we can write as follows:

For encryption: C=Ek(P)=Kp

For decryption: P=Dk(C) =K^{-1} C= K^{-1}Kp=P

2. Literature review

Quentin Galvane and Baptiste Uzel[3] in their study said, after some research on the web to find an interesting cryptographic primitive to implement, they decided to implement RC4 stream cipher as it was most widely used and it is used by important and famous protocols and standards such as SSL, TSL, WEP, as well it was known for its efficiency and simplicity.

Khushdeep Kaur [1] et.al a proposal of a combination of DSA, RSA and MD5 as a hybrid link for wireless devices was made. They had also considered case study for Manet networks so that they could suggest the applications of proposed algorithm.

Atul M. Gonsai and Lakshadeep M. Raval [2] provide a beneficial comparison between three well known symmetric key cryptography algorithms: DES, AES, and Blowfish. The performance of algorithms under different settings is the main concern here; the presented comparison takes into consideration performance of the algorithm and the behavior when different data loads are used. These parameters key size, block size, and speed are the base of comparison.

Radu Terec [4] et.al. in their paper said that the quantum cryptography is not a quantum encryption algorithm but rather a method of creating and distributing private keys. It is based on the fact that photons send towards a receiver changing irreversibly their state if they are intercepted. Quantum cryptography was developed starting with the 70s in Universities from Geneva, Baltimore and Los Alamos.

Tarun Narayan Shankar and G.Sahoo [6] provide a brief overview of elliptic curve cryptography and obtain the ASCII table with Karatsuba Multiplier for fast encryption and decryption. The strength of encryption depends on its key, if we use the alphabetical table then there will be no impact on strength and runtime performance.

Shikha Kuchhal and Ishank Kuchhal[7] in their research paper concluded that encryption and decryption algorithm's security depends on the algorithm as well as on the key's confidentiality, once the key is leaked, it means any one can encrypt or decrypt the data, it means the whole procedure become useless. Therefore, how to distribute the private key and how to save both transmission keys are very important. They introduce the concept of RSA algorithm, and, thereby design and analyze the performance of improved implementation. They have developed a program for encrypting and decrypting text files. In addition, the encryption procedure and code implementation is provided.

Mamatha et.al. combined concept of AES and 3DES to obtain a hybrid model which can be used for uploading the data into the cloud server by encrypting data and downloading the data from cloud server by decrypting the same data. Thus the hybrid model gives a better non linearity to the plain AES and as it is merged with 3DES, there is better diffusion. Hence the possibility of an algebraic attack on the hybrid model is reduced [13].

Nagesh Kumar et.al. [9] conducted a comparative analysis for the performance evaluation of symmetric and asymmetric encryption algorithms i.e. AES, DES and RSA in term of computation time, memory usage and output bytes on different file sizes. The result of their experiments showed that DES algorithm performed better among others in term of encryption time, AES has least memory usage and RSA algorithm generated least output file.

Maqabkeh et.al [10] compared the performance of RSA and NTRU asymmetric algorithms on variable text file sizes with the key size of 51 bits and 20 bits for encryption and decryption process respectively. They concluded that NTRU performed better in term of encryption, decryption and authentication than RSA.

Vijayalakshmi et.al. compared the performance of RSA and Elliptic Curve Cryptosystem (ECC) asymmetric algorithms over execution time and memory size for encryption and decryption process with variable word lengths and different key sizes. Their results showed the superiority of ECC over RSA in term of execution time and memory requirement [11].

3. Simulation and comparative analysis of modified RSA and Hill cipher algorithm

Simulation results have also been drawn using MATLAB 12a. To implement proposed algorithm we have to focus on three parts which are a) key generation, b) encryption process, and c) decryption process.

Key Generation*:* Generate five large prime numbers p, q, r, s and t. Here first we have to input five large prime numbers and then we calculate the value of d and e which were used to generate private and public key respectively.

Choose

p=51 q=43 r=13 s=19 t=7

Compute N= 3791697

Compute phi= 2721600

Let e=41

Find d such that e*d=1 mod phi

d= 132761

Public key (e, n) = (41, 3791697)

Private Key (d, n) = (132761, 3791697)

Encryption Process: With the help of public key we are able to encrypt the value of plaintext. Enter the value of plaintext and we get the cipher text.

Suppose the message to be encrypted is: ALGORITHM

Table1: **Encryption of message**

Plain text	M(ASCII code)	M^e	Cipher text (M^e mod n)
A	65	213524455152715236049015011728325682046312468310134136117994785308837890625	3402893
L	76	129824686791822543194085639764751145102253838334631845473451939269078025240576	1831486
G	103	3359898925759046598697426680663567493058203756714418053846286946644763246570827 0503	993940
O	79	634907917517787687870401884685337901013621532795443507239557870430105727875279	1097968
R	82	2926630860055278500997552034267543400541920722186054355964082740007147071864832	3460285
I	73	2490217409050022454881852444506957393620019561254721922394884925225355977127 3	330832
T	84	7860510072379334666888938844341580026313724135227776831331864400967815590313984	2523003
H	72	141459576538856797618928841644310172191756436165747367560242428005992596766 72	446730
M	77	221880804596155822483916220420443821810533948253748281037527829169937762144877	3615416

Decryption Process: With the help of the private key the cipher text can be converted to plain text. Compute $P=C^d$ mod n by using private key.

Table2: Decryption of message

Cipher text (m^e mod n)	c^d mod n	Plain text letter
3402893	65	A
1831486	76	L
993940	103	G
1097968	79	O
3460285	82	R
330832	73	I
2523003	84	T
446730	72	H
3615416	77	M

Decrypted value of the cipher text: ALGORITHM

Table3: Time analysis of optimized RSA and Hill Cipher algorithm

File size (bytes)		934
Modified RSA Algorithm	Encryption (seconds)	0.870456
	Decryption (seconds)	0.0006366
Hill cipher	Encryption (seconds)	1.900900
	Decryption (seconds)	0.486881

EXPERIMENTAL RESULTS AND DISCUSSIONS

The security for the data has become highly important and the user's data privacy across the network is a central question. In this paper we come with new design of encryption and decryption algorithm, modified RSA(using five prime numbers) whose output have been compared with Hill cipher using MATLAB. When the cipher text is decrypted with the help of private key, same plain text has been observed. After analysing modified RSA and Hill cipher, it is found that the proposed algorithm increases the security of the system as it reduces the computation time. This shows that accuracy of modified RSA cryptographic algorithm using dynamic keys is good.

CONCLUSION

Security is considered the most important requirement for the success of electronic commerce, which is built based on the security of hash functions, encryption algorithms and pseudorandom number generators. Use of cryptographic techniques to secure data across networks is gaining more importance and with more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. By studying various encryption algorithms it can be concluded that bigger key size means, harder to crack. Key length is directly proportional to security and inversely proportional to performance. Therefore hacking time is reduced which indicate that the time available for the hacker has been reduced. In current scenario there are number of ways, which guarantee for the safety and security of the network but it cannot be said that they will be everlasting. Network security is a continuous process and demands regular network analysis, testing and maintenance. Furthermore there is a prominent need for continuously upgrading the security protocols, policies, mechanisms and their dynamic adaptation to cope with the evolving security threats.

REFERENCES

1. Khushdeep Kaur and Er.Seema, "Hybrid Algorithm with DSA, RSA &MD5 Encryption Algorithm for wireless devices", (IJERA) ISSN: 2248-9622, www.ijera.com Vol. 2, Issue 5, September-October 2012, pp. 914-917.

2. Dr. Atul M. Gonsai and Lakshadeep M. Raval, "Evaluation of Common Encryption Algorithm and Scope of Advanced Algorithm for Simulated Wireless Network", International Journal of Computer Trends and Technology (IJCTT) – volume 11 number 1 – May 2014.

3. Quentin Galvane Baptiste Uzel, "Cryptography - RC4 Algorithm", February 2012.

4. Radu Terec, Mircea-Florin Vaida, Lenuta Alboaie, Ligia Chiorean, "DNA Security using Symmetric and Asymmetric Cryptography", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 34-51. The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).

5. William Stallings, "Cryptography and network security", 2nd edition, Prentice Hall publications.

6. Tarun Narayan Shankar & G.Sahoo, "Cryptography by Karatsuba Multiplier with ASCII Codes", 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 12.

7. Shikha Kuchhal and Ishank Kuchhal, "Data Security Using RSA Algorithm In Matlab", International Journal of Innovative Research and Journal, ISSN: 2278 – 0211 July, 2013Volume 2 Issue 7.

8. Menezes, et.al., "Handbook of Applied Cryptography", CRC Press, 1996.Results of comparing tens of encryption algorithms using different settings- Crypto++ Benchmark Retrieved, 2013.

9. Nagesh Kumar et.al., "Performance Analysis Of Symmetric Key Cryptography Algorithms: DES, AES and BLOWFISH" International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 1, Issue 2, 2011.

10. http://etheses.dur.ac.uk/738/,11-05-2018

11. Amogh Mahapatra and Rajballav Dash, "Data encryption and decryption by Using hill cipher technique and self repetitive matrix", Department of Electronics & Instrumentation Engineering National Institute of Technology Rourkela 2007.

12. Mamatha et.al. "Use of Digital Signature with Diffie Hellman Key Exchange and Hybrid Cryptographic algorithm to Enhance Data Security in Cloud Computing", International Journal of Scientific and Research Publications, Volume 5, Issue 6, June 2015 ISSN 2250-3153.