ISSN 2278-3091

Volume 6, No.3, May - June 2017

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse06632017.pdf

DEVELOP A HYBRID METHOD TO ENCODE DATA

Naincy Aggarwal[1], Bhanu Pratap[2]

[1]M. Tech Scholar, Department of Comp. Sci. and Engg., DCET, Sunderpur, Saharanpur, India
[2]Asst. Prof., Department of Comp. Sci. and Engg., DCET, Sunderpur, Saharanpur, India

[1]naincyaggarwal@gmail.com
[2]bhanu8909@gmail.com

ABSTRACT

In the current time, communication becomes important among people through internet. It is used as a tool for ecommerce so that the security of our data becomes a very important issue to deal with many unauthorized accesses over the internet. Internet is widely used for uploading many web pages and many other documents online. Transferring of various data like e-banking, e-shopping, tenders etc. need special authenticated medium for providing security in highly complex manner. For this purpose we develop a hybrid method to encode data. In this paper we are working on developing an algorithm which will hide the data of user in highly complex manner with more security and accuracy by using multilevel and hybridization of two cryptographic algorithms that are RSA and ECC. By developing hybrid approach or algorithm we can develop more secure method for protecting our data in complex manner.

Keywords: **Cryptography, RSA, ECC, Security, Applications.**

1. INTRODUCTION

Cryptography is a way to hide the plain text. Through this we can disguise message in such a way that an unauthorized user cannot change the data without the permission of actual user. Communication among people becomes an important in current time over the internet. So it is very important to provide security among various communication medium over the internet. It makes secure communication over the unsecure channel. Various files are transfer over the internet. So there is a need to provide security to these files. For this purpose, various cryptographic techniques are widely used for converting original data into unreadable form. Secret key cryptography and asymmetric key cryptography are widely used for hiding information. So that, no unauthorized user can modify or use data for his benefit without the permission of user.

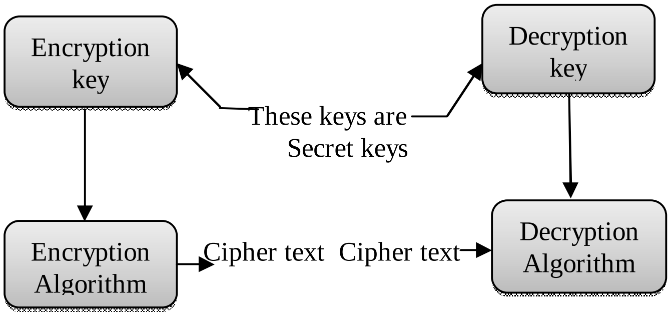


Figure 1.1: Process of Encryption and Decryption

In secret key sender and receiver of data uses the same key for encryption and decryption. AES and DES are example of secret key cryptography. And in asymmetric key two key are used i.e. public key and private key. In this one key i.e. private key is kept by receiver and other key i.e. public key is announced to public. This algorithm is highly complex. This algorithm takes a long time to calculate secure text from original text. RSS and ECC are example of this cryptography. RSS is widely used asymmetric key algorithm. This is used in various e-commerce applications. This algorithm provides security of various files in highly complex manner. This algorithm is very safe to use. RSA provide a very good security since it uses very long prime numbers and their product is so large that an attempt to break the code using even the fastest computer shall require a few years. ECC is also a type of asymmetric key cryptography like RSA. It is different from PKC in its faster evolving capacity. It uses smaller key in comparison to non-ECC cryptography to provide same kind of security. We used this cryptography in various factorization algorithms. Hybridization of RSS and ECC algorithm can provide more security and accuracy to data in highly complex manner. So that it is impossible for unauthorized user to intercept the data without the permission of user.

The three major reasons for using the cryptosystems are as under:

- To maintain privacy and to prevent an unauthorized person from extracting information from the communication channel. The process of extracting information from the channel is called eavesdropping.
- To enable authentication for preventing unauthorized persons from injecting information into the channel. The process of injecting information is called spoofing.
- Sometimes, it is essential to provide the electronic equivalent of a written signature in order to avoid or settle any dispute between the transmitter and the receiver about what the transmitted message is.

2. LITERATURE SURVEY

A) Enhancing Cloud Data Security Using Elliptic Curve Cryptography: Cloud computing is [1] one of the hottest technology of the IT trade for business. Cloud computing security has changed into a popular topic in sector and academic research. Cloud computing is a conceptual service based technology which is used by many companies widely these days. ECC algorithm provides secure communication integrity and authentication, along with nonrepudiation of communication and data confidentiality. ECC (Elliptic Curve Cryptography) is known as a public key encryption technique based on elliptic curve theory that can be used to create speedy, tiny and more efficient cryptography key for encryption of data. It has three protection point; authentication, key generation and encryption of data. This paper will create cloud security data security of cloud in cloud computing by creating digital signature and encryption with elliptic curve cryptography.

B) Secure Communication using Elliptic Curve Cryptography on Android Devices: SMS (Short Message Service) is being used in many daily life applications. When send [2] a message from one device to another, the message is transmit as plain text. Sometimes, this message may be confidential, and it is a major disadvantage to send such through message while the traditional message service does not provide encryption to the information before its transmission. We purpose an efficient and secure application called ECCSMS (Elliptic Curve Cryptography Short Message Service). To prevent attack, a secure digital scheme is needed. Each signature is signed using key signature scheme of ECC to increase complexity of brute force attacks.

C) Survey on Security Architecture Based [3] on ECC (Elliptic Curve Cryptography) in Network: Cryptography is the technique of hiding message in some unintelligible format so that the message lies hidden in plain sight of an unintended person. Public key cryptography offers a wide range of security over the various mode of transferring data, especially over Internet. Countermeasures against these attacks should be considered during cryptosystem design. Side channel attacks allow an attacker to retrieve secret key with far less effort than other attacks. The main aim of this paper to introduced ECC to implement an efficient and secure network with high speed as compared to current standards by using various techniques and algorithms.

D) Certificate less Public Key Cryptography: Certificate less public key cryptography is a model of public key cryptography that, while similar, avoids the escrow of identity-based public key cryptography while not relying on the use of certificates [4] to guarantee the authenticity of keys. The intent of this paper is to explore some algorithms for certificate less public key cryptography and to determine their benefits and disadvantages.

E) An Efficient Many-Core Architecture for Elliptic Curve Cryptography Security Assessment: Elliptic Curve Cryptography (ECC) is a popular tool to construct public-key crypto-systems. The security of ECC is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP). Implementing and analysing the [5] performance of the best known methods to solve the ECDLP is useful to assess the security of ECC and choose security parameters in practice. We present a novel many-core hardware architecture implementing the parallel version of Pollard’s rho algorithm to solve the ECDLP. This architecture results in a speed-up of almost 300% compared to the state of the art and we use it to estimate the monetary cost of solving the Certicom ECCp-131 challenge using FPGAs.

F) Implementation of Elliptic Curve Cryptography for Audio Based Application: [6] Recently 3G technology has grown rapidly and is becoming a medium of choice for communication. All elements of multimedia (text image audio and video) are used. In this era, network security has become an issue of importance, on which a lot of research is going on. This paper presents the implementation of ECC (Elliptic Curve Cryptography) by first transforming the audio file into an affine point on the Elliptic Curve (EC), over the finite field GF (p). In ECC we normally start with an affine point called Pm (x , y) which lies on the elliptic curve. In this paper we illustrate the process of encryption/decryption for audio file. It is almost infeasible to attempt a brute force attack to break the cryptosystem using ECC.

G) File Encryption and Decryption Using Secure RSA: In this paper we have introduced secure RSA for secure file transmission. There are many cases where we need secure file transmission for example in banking transactions, e-shopping etc. In this paper we present modified RSA [7] algorithm for secure file transmission. RSA algorithm is asymmetric key cryptography also called public key cryptography. Two keys are generated in RSA, one key is used for encryption and other key which is only known to authenticated receiver can decrypt message. Every communication party need just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he/she can communicate with anyone else. RSA is well known public key cryptography algorithm and was one of the first great advances in public key cryptography. Even if it is efficient algorithm it is vulnerable to attackers. With the help of all brute force attacks hacker can obtain private key. Many improvements has been done to improve RSA like BATCH RSA, Multi Prime RSA, Multi Power RSA, Rebalanced RSA, R Prime RSA etc. As craze of internet is increasing exponentially, it is used for email, chatting, transferring data and files from one end to other. It needs to be a secure communication among the two parties. This paper focuses on file transfer using secure RSA, which eliminates some loopholes of RSA that might prevent a hacker from stealing and misuse of data. This paper also presents comparison between RSA file transfer and Secure RSA file transfer.

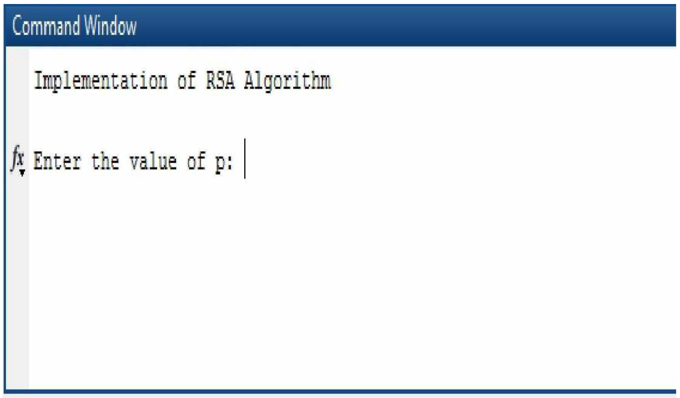
3. PROBLEM FORMULATION

The idea that the technology is moving beyond the personal computer to everyday devices with embedded technology and connectivity, as computing devices become progressively smaller and more powerful, is called ubiquitous computing or pervasive computing. The ubiquitous computing is growing trend of embedding computational capability, goes beyond the realm of personal computers: it is the idea that almost any device, from clothing to tools, appliances, cars, homes, and even human body, can be placed with chips to connect the device to an infinite network of other devices. The main objectives of this computing merges the current network technologies with wireless computing, voice recognition, internet capability and artificial intelligence to create an environment where the connectivity of various devices is set in such a way that the connectivity is unobtrusive and always available. So there is need for such an algorithm which will do the secure connections to each other, to ensure that the information they provide remains confidential and that only those authorized to control these devices can do so. Providing security in such environment will be a critical task.
For that there is need for such an algorithm which is more secured, providing more accuracy and has fast cryptographic property along with fast encoding.

4. IMPLEMENTATION OF RSA ALGORITHM USING MATLAB SOFTWARE

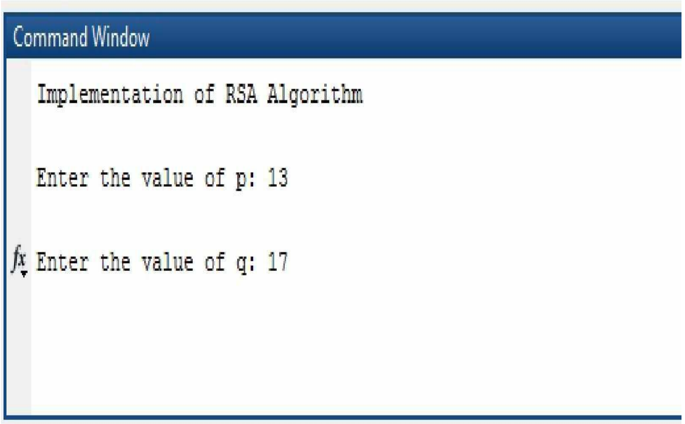
Step 1: Run rsa.m Matlab code in Matlab software.

Step 2: It ask prime value of p and q as shown in figure:



```
Implementation of RSA Algorithm

Enter the value of p:
```

Figure 3.1: Implementation of RSA algorithm for value of p

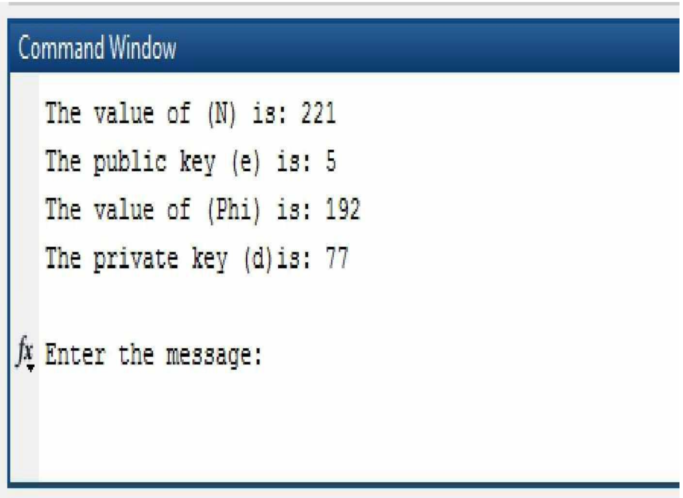


```
Implementation of RSA Algorithm

Enter the value of p: 13

Enter the value of q: 17
```

Figure 3.2: Implementation of RSA algorithm for the value of p and q

Note: Take any large prime value of p and q.

Step 3: After putting values press enter then it shows calculated public and private keys for RSA as shown in figure:

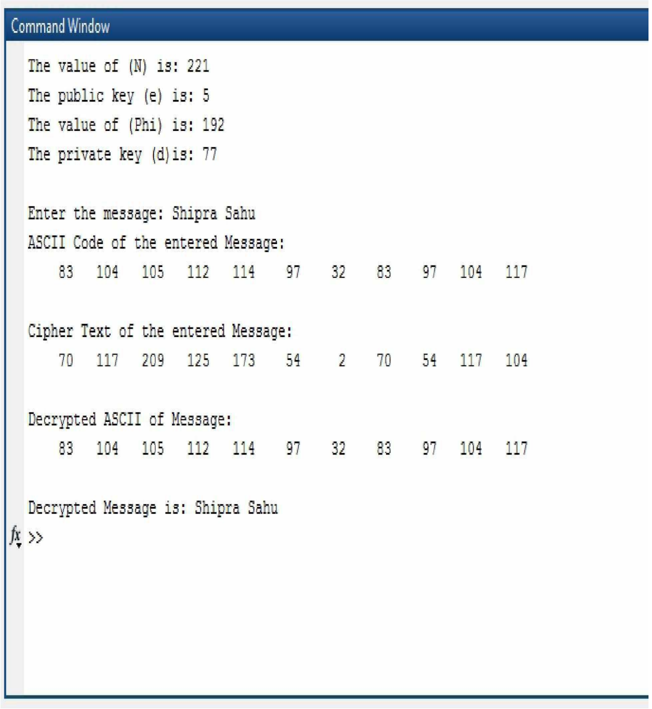


```
The value of (N) is: 221
The public key (e) is: 5
The value of (Phi) is: 192
The private key (d)is: 77

Enter the message:
```

Figure 3.3: Calculated values of public key and private key

Step 4: In figure 3 it also ask for enter the message, then we write any text here like “ShipraSahu” for encryption and decryption.

Now press enter after writing message it shows the ASCII code of entered message, cipher text ASCII message, decrypted ASCII message and finally shows decrypted message as entered message, as shown in figure 4:



```
The value of (N) is: 221
The public key (e) is: 5
The value of (Phi) is: 192
The private key (d)is: 77

Enter the message: Shipra Sahu
ASCII Code of the entered Message:
    83   104   105   112   114    97    32    83    97   104   117

Cipher Text of the entered Message:
    70   117   209   125   173    54     2    70    54   117   104

Decrypted ASCII of Message:
    83   104   105   112   114    97    32    83    97   104   117

Decrypted Message is: Shipra Sahu
fx >>
```

Figure 3.4: ASCII Code and Decrypted Message

5. PROPOSED METHODOLOGY

The proposed methodology implemented here is based on the concept of hybridization of RSA and ECC algorithm for encoding data in complex manner.

5.1 Algorithm

5.1.1 RSA Algorithm

(1) First select two prime numbers such that:

$$P = 13,\ Q = 17$$

(2) Then calculate the value of N and T,

$$N = P * Q = 13 * 17 = 221$$

$$T = (P - 1)\ (Q - 1) = 12 * 16 = 192$$

(3) Then, we evaluate D and E.

E (public key) should not have any factor other than 1 in common with T i.e. 192.

Thus, $192 = 2 * 2 * 2 * 2 * 2 * 2 * 3$

Hence, we can select E = 5

Now, we evaluate D (private key) with the help of following expression:

$$D = E^{-1} \bmod T$$

Therefore, $D = 5^{-1} \bmod 192$

Now, D can be calculated as under:

Next, we find the (multiple of 192 + 1) which is divisible by 5. Then, we divide that number by 5 and select the quotient of this division as D.

Therefore, (192 * 1) + 1 = 193 not divisible by 5

(192 * 2) + 1 = 385 is divisible by 5.

Therefore, 385/5 = 77

Or D = 77

(4) For encryption process calculate the cipher text from plaintext as follow:

Let, letter F is to be sent so M = 6 as F is the sixth alphabets.

Hence, Cipher text $C = M^E \bmod N$

Or, $C = 6^5 \bmod 221$

Hence, C = 41

This number is sent to the receiver.

(5) Now for decryption process calculate the plaintext from cipher text as follow:

$$\text{Plaintext } M = C^D \bmod N$$
$$= 41^{77} \bmod 221$$
$$= 6.$$

Thus, the original number is obtained.

5.1.2 Elliptic Curve Cryptography Algorithm

ECC is type of asymmetric key cryptography like RSA. It is different from PKC in its faster evolving capacity. It uses smaller key in comparison to non-ECC cryptography to provide same kind of security. We used this cryptography in various factorization algorithms.

We used ECC cryptography to hide message, digital signature and other cryptography techniques.

Elliptic curve is a plane curve over a finite field which consists of the points satisfying the equation –

$$Y^2 = X^3 + AX + B$$

Certain chosen number a and b, typically the number are integer, it can also work on principle of real number. Curves do not have an elliptic shape. For example a = -4 and b = 0.67 gives the elliptic curve with equation $y^2 = x^3 - 4x + 0.67$

If equation x + ax + b contains no repeated factors, or if 4a + 27b is not 0, then the elliptic curve can be used to form group. A group is simply a set of points on the curve. For the purpose of cryptographic, an elliptic curve algorithm must have only points with all coordinates whole number in the group.

Generating an Elliptic Curve public key:

AI = As * F

AI is public key

As is secret key

The above process is same for other user or receiver.

5.2 Flow diagram using the hybridization of RSA and ECC Algorithm

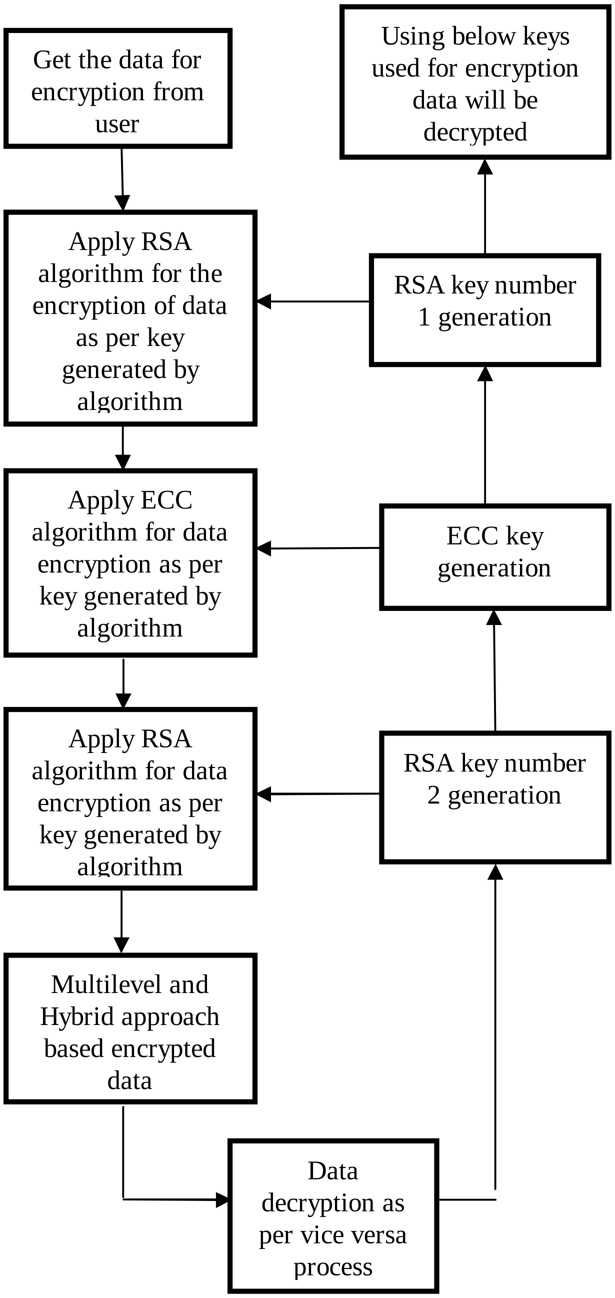

Get the data for encryption from user
Using below keys used for encryption data will be decrypted
Apply RSA algorithm for the encryption of data as per key generated by algorithm
RSA key number 1 generation
Apply ECC algorithm for data encryption as per key generated by algorithm
ECC key generation
Apply RSA algorithm for data encryption as per key generated by algorithm
RSA key number 2 generation
Multilevel and Hybrid approach based encrypted data
Data decryption as per vice versa process

Fig 5.2: Flowchart Using the Combination of RSA and ECC Algorithm

6. CONCLUSION

In this paper we develop a hybrid method to encode data for providing great level of security. For this purpose we deeply study two cryptographic algorithms that are RSA and ECC. This work include multilevel and hybridization of RSA and ECC algorithm. Thus, this approach provides more security so that only the authenticated user can access the data or files over Internet. This method also provides secure transmission of files like banking transaction, e-shopping, tenders etc. over the Internet. As a future work multiple file encryption and decryption can be possible. It has broad development prospects. Great level of security is achieved using the hybridization of these algorithms for preventing unauthorized user from injecting information into the channel.

REFERENCES

[1] Ms. Nikita N Chintawar “Enhancing Cloud Data Security Using Elliptic Curve Cryptography” International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, pg. 94-97, 2016.

[2] Ramkumar S “Secure Communication using Elliptic Curve Cryptography on Android Devices” South Asian Journal of Engineering and Technology, Vol. 2, pg. 11-16, 2016.

[3] Mrs Sweta Nigam “Survey on Security Architecture Based on ECC (Elliptic Curve Cryptography) in Network” International Journal of Computer Science and Mobile Applications, Vol. 3, pg. 17-23, January- 2015.

[4] Rachel silva, “Certificate less Public Key Cryptography”, Vol. 1, pg. 1-6, May 2015.

[5] Andrea Miele, “An Efficient Many-Core Architecture for Elliptic Curve Cryptography Security Assessment”, Vol. 2, 2015.

[6] Rahul Singh, “Implementation of Elliptic Curve Cryptography for Audio Based Application”, Vol. 4, January 2014.

[7] Rajan S. Jamgekar “File Encryption and Decryption Using Secure RSA”, Vol. 1, 2013.

[8] Tanu, “A Hybrid Geometric Cryptography Approach to Enhance Information Security”, Journal of Network Communications and Emerging Technologies (JNCET), Vol. 3, pg. 16-20, July 2015.

[9] Vaishali P. Bhoge, “New Secure Authentication and Key agreement Scheme for Session Initiation Protocol using Elliptic Curve Cryptography”, International Journal of Computer Trends and Technology, Vol. 30, pg. 200-205, December 2015.

[10] Nivedita Bist, “A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, pg. 1028-1031, March 2015.

[11] Sharvari Dixit “Public Key Cryptography based Lossless and Reversible Data Hiding in Encrypted Images” Vol. 6, pg. 3551-3558, 2016.

[12] Fathima Nizar “RSA Based Encrypted Data Embedding Using APPM”, Vol. 1, 2014.