ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Comparative Analysis of RSA and ECC

Kumari Archana[1], Vibhuti Sikri[2]

P.G. Student, Department of Computer Science & Engineering, Bahra University, Shimla Hills, H.P, India[1]

Assistant Professor, Department of Computer Science & Engineering, Bahra University, Shimla Hills,H.P,India[2]

ABSTRACT: Cryptography is the study of techniques which ensures the secrecy and authentication of the information. For this, an appropriate cryptographic algorithm needs to be selected and used based on security and performance attributes. This paper aims at study of the two asymmetric-key algorithms i.e. Rivest-Shamir-Adlemann(RSA) and Elliptic-Curve cryptography(ECC).A comparative analysis of both the algorithms was done on the basis of results obtained. The analysis showed that ECC takes less time for encryption and decryption and also provides key of smaller size as compared to RSA.

KEYWORDS: Cryptography, authentication, RSA, ECC, asymmetric-key.

I. INTRODUCTION

Cryptography is an art of converting a message into an encoded unreadable form so that only the intended receiver can read and process it. The main aim of the cryptography is to provide security to the data from unauthorised access. The cryptography involves encryption and decryption. The transformation of original message into the format that is almost impossible to read without the appropriate knowledge is called encryption.Decryption is the reverse process of encryption.It is the conversion of encrypted message back into original readable format.The encryption and decryption both require the use of some secret information i.e. key.

Cryptography involves two main approaches:

- Symmetric-key cryptography.
- Asymmetric-key cryptography.

Symmetric-key cryptography: Same secret key is used for both encryption and decryption.
Asymmetric-key cryptography: Two different keys are used i.e. one for encryption and other for decryption.
In this paper, the two algorithms- RSA and ECC which are believed to be most secured ones are studied and compared.

RSA:

This asymmetric cryptographic algorithm was developed in 1977.RSA is based on the use of two large prime numbers according to the mathematical fact that it is easy to find to large prime numbers but difficult to factorize their product.RSA generates two keys: Public key for encryption and Private key for decryption.

The public key consists of public-key modulus and public-key exponent. The private-key consists of private-key modulus and private-key exponent.

Algorithm:

1. Take two prime numbers, p and q.
2. Calculate, n = p*q.

n is called the modulus of both public and private keys.

3. Calculate, $\varphi(n) = (p-1)(q-1) = n - (p + q - 1)$, where φ is Euler's toient function and its value is kept secret.
4. Choose an integer e, $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.e and $\varphi(n)$ are coprime.

e is called the public key exponent.

5. Calculate, $d \equiv e^{-1} \pmod{\varphi(n)}$.d is called the private key exponent.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Encryption:
Sender sends his public key(n,e) to the receiver and keeps the private key (d) confidential.He converts the message into an integer m and computes cipher text as

$$C = M^e \bmod n$$

Decryption:
The receiver can recover the original message by using his own private key.

$$M = C^d \bmod n$$

ECC:
ECC was discovered by Victor Miller (IBM) and Neil Koblitz in 1985.ECC is based on the algebraic structure of elliptic curves over finite fields.ECC provides the same level and the type of security as RSA does but with shorter key length. So the encryption and decryption by ECC is fast as compared to RSA.

Algorithm:
The public key is generated using the following equation:

$$Q = d * P$$

d is the random number generated within range(1,n-1).P is the point on curve on which the original message is mapped. Consider m on the point M on the curve. Select k randomly from range (1, n-1).
The cipher text will be generated as:

$$CT1 = k * P$$
$$CT2 = M + k*Q$$

To get back the original message,

$$PT = CT2 – d*CT1$$

II. RELATED WORK

Vivek B. Kute et.al (2009) This paper focused on performance attribute of public key cryptosystems. The algorithms studied and compared are RSA, ECC. Implementation of these algorithms in Java in order to perform software tests is done.
Vivek Katiyar et.al. (2010) This paper provided an introduction to ECC and presented a survey on the current use of ECC in the pervasive computing environment.
D. Sravana Kumar et.al. (2012) The principal attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size, thereby reducing the processing overhead. This paper introduced a new encryption algorithm using Elliptic Curve over finite fields.
Bafandehkar.M (2013) This paper introduced the comparison of elliptic curve cryptography (ECC) algorithm with Key size of 160-bit and Rivest-Shamir-Adleman (RSA) algorithm with key size of 1024-bit.

III. IMPLEMENTATION RESULTS

A. Performance comparison of RSA and ECC as per graphs generated:

1. Encryption time graphs:

RSA encryption time: The graph corresponding to the time taken by RSA to perform encryption on given text is as follows:

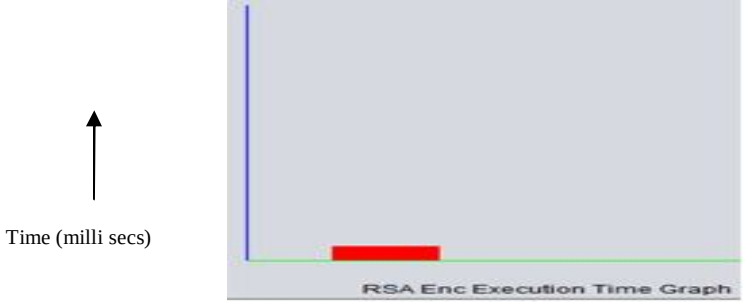

Figure1.1: RSA encryption time

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

ECC encryption time: The graph corresponding to the time taken by ECC to perform encryption on given text is as follows:

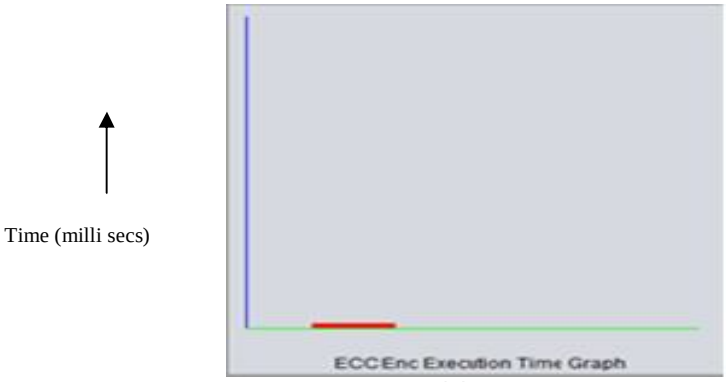

Figure1.2: ECC encryption time

Observation: From both the encryption time graphs, it is clear that RSA takes more time for encryption than ECC.

2. Decryption time graphs:

RSA decryption time: The graph corresponding to the time taken by RSA to perform Decryption on RSA encrypted text is as follows:

Figure1.3: RSA Decryption time

ECC decryption time: The graph corresponding to the time taken by ECC to perform decryption on ECC encrypted text is as follows:

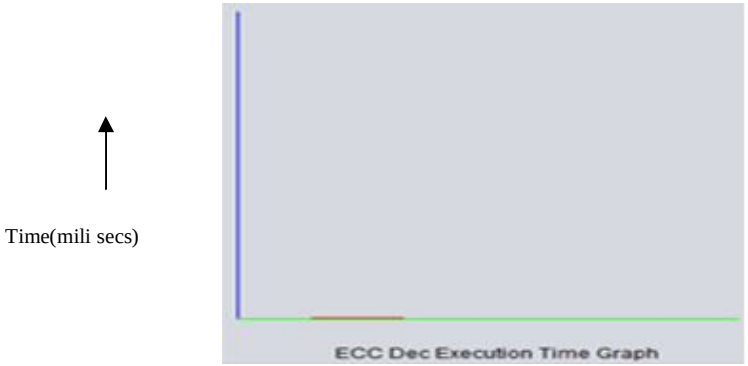

Figure1.4: ECC decryption time

Observation: From both the decryption time graphs, it is clear that RSA takes more time for decryption than ECC.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

3. Key length graphs:

RSA generated key length: The graph corresponding to key generated by RSA for the given text is as follows:

Figure1.5: RSA key length

ECC generated Key length: The graph corresponding to key generated by ECC for the given text is as follows:

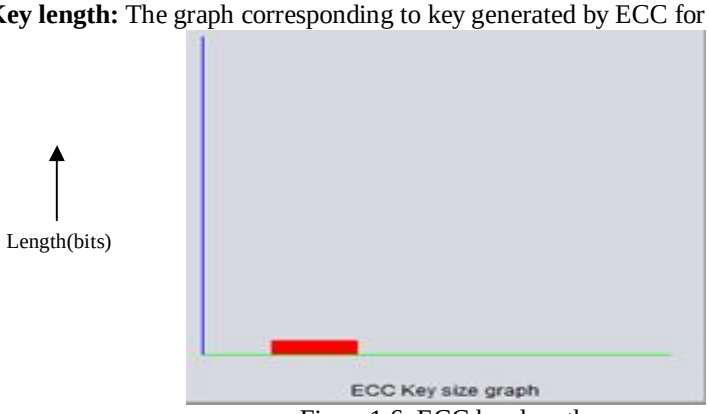

Figure1.6: ECC key length

Observation: From both the key length graphs, it is clear that RSA generates key of larger size than ECC.

B. Table : Performance comparison of RSA and ECC

C.

Algorithm	Original Data	Encryption time (milli secs)	Decryption time (milli secs)	Key- Length (bits)
RSA	Hiiii....What are you doing..???	More	More	Large
ECC	Hiiii....What are you doing..???	Less	Less	Short

IV. CONCLUSION AND FUTURE WORK

In today's world the internet is used for the secure communication.So the strong algorithms are required to provide the security to the data. The comparison table of RSA and ECC shows that ECC takes less time for encryption as well as decryption and also generates key of smaller size than RSA. So it can be concluded that ECC is more efficient than RSA. In future, comparison of other cryptographic algorithms can be done and efforts can be done to reduce the execution time of RSA.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

REFERENCES

[1] Alfred J.Menezes and Scott A. Vanstone, "Elliptic Curve Cryptosystems and their implementations",1993
[2] Ch. Suneetha,Dr. Sravana Kumar and A. Chandrasekhar, "Secure key transport in symmetric cryptographic protocols using elliptic curves over finite fields",November 2011
[3] Fathima Nizar, " RSA Based Encrypted Data Embedding Using APPM",2014
[4] Gajendra Singh Chandel , "A Review: Image Encryption with RSA and RGB randomized Histograms",2011
[5] K. Naga Divya, " A Routing-Driven elliptic Curve cryptography Based Key Management Scheme for Heterogeneous Sensor Networks",2012
[6] Lekha Bhandari, " Speeding up Video Encryption using Elliptic Curve Cryptography (ECC)",2013
[7] Rajan.S.Jamgekar, "File Encryption and Decryption Using Secure RSA",2013
[8] Vivek B. Kute, " A software comparison of rsa and ecc",2009
[9] Vivek Katiyar, " A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment",2010
[10] William Stallings, " A text book of cryptography and Network security",2007