Survey paper comparing ECC with RSA, AES and Blowfish Algorithms

A Arjuna Rao[1], K Sujatha[1], A Bhavana Deepthi[1], L V Rajesh[1]
[1] *Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagram, India*

Abstract: Data Security is primary concern for every communication system. There exist many frauds in real time through online in each and every aspect, in order to overcome those frauds which means to keep one's images and personal information secure, there should be some security algorithms which helps in reducing the frauds. In general, there are many encryption algorithms that can be used to reduce the real time frauds. These encryption algorithms can be classified into two types. One is symmetric encryption and the other one is asymmetric encryption. Symmetric encryption algorithms are used earlier for the purpose of providing security such as AES and Blowfish algorithms. In AES algorithm, the processing time is more and requires more rounds of communication when compared to the remaining algorithms and it is not highly secured. In case of blow fish algorithm, uses a lot of memory and has a relatively long key setup time and it was only designed for software. In order to provide more security the asymmetric algorithms are used such as RSA algorithm and Elliptic Curve Cryptography (ECC) algorithm. When compared to ECC, RSA algorithms is little slow and uses larger key or message in size. So, now the most efficient ECC algorithm came into the picture in order to provide high security over the existing credit frauds. This proves the efficiency and the less memory usage after the implementation of elliptic curve cryptography.

Keywords: *Data Security, Symmetric and Asymmetric algorithms, AES, Blowfish, Elliptic Curve Cryptography (ECC).*

*****

1. INTRODUCTION

Encryption is a process which is used to modify the data that is given as input and protects that data from unauthorized users or attackers. It not only protects the data but also prevents data losses. The following are the issues that are caused when the data that want to be keep as secure is not encrypted. So, by this the encryption plays a major role in securing the data.

There are several types of data encryption:

- File and folder encryption: It is also called as "desktop encryption", which allows users to encrypt files stored in their PCs, laptops or portable storage devices and other media.
- E-mail encryption: It protects e-mail messages from unauthorized access as more number of frauds can be caused over in corporate networks.
- Full-disk encryption: Instead of encrypting the individual files oe messages it encrypts the entire hard disk drive and is popular for laptops used by mobile workers.
- Mobile data encryption: It encrypts the data which is stored on devices such as PDAs and smart phones.
- Application encryption: It encrypts the data stored within a custom application such as a payroll system

2. SECURITY ALGORITHM

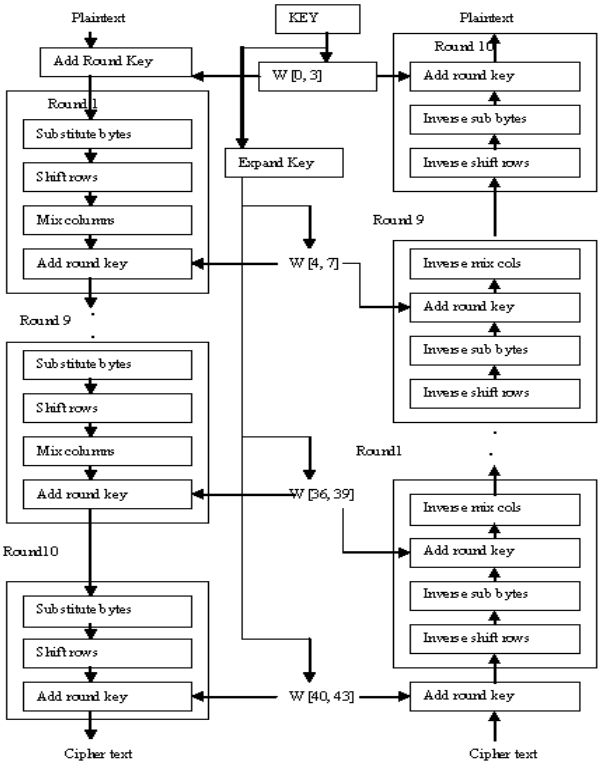
AES Algorithm:

It is a symmetric encryption algorithm which uses 128-bit blocks of data. Lengths of 128, 192, and 256 bits are standard key lengths used by AES Algorithm. The algorithm consists of four stages that make up a round which is iterated 10 times for a 128-bit length key, 12 times for a 192-bit key, and 14 times for a 256-bit key. In AES, we have a set of round keys called as derived keys which are applies along with another application which holds one block of data exactly. The steps which are included in the process of performing operations using AES algorithm has involved the following types of operations:

- Sub Bytes
- Shift Rows
- Mix Columns
- XOR Round Key

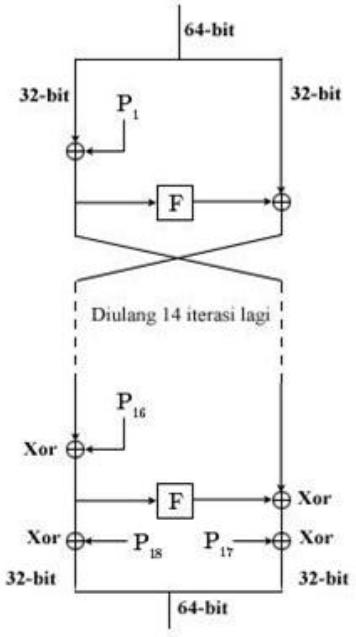
Structure of AES algorithm is as follows:

 ISSN: 2321-8169
44 – 47



Blow-Fish:

Blowfish is another algorithm to replace DES which splits messages into blocks of 64 bits and individually encrypts them. It has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits and has 16 rounds. Each round consists of a key dependent permutation, and a key- and data-dependent substitution. The structure of Blow-Fish algorithm as follows:



RSA Algorithm:

At the time of electronic email arising soon, RSA has implemented the following way:

- Public Key Encryption: In RSA, keys used for encryption are public, while the keys used for decryption are not, so the person who has the correct decryption key can only decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key.

The following steps are involved in RSA Algorithm in order to encrypt and decrypt the data:

(i) Select any two integers say p and q where p,q should be the prime numbers but p should not be equal to q.

(ii) Now calculate n=p*q

(iii) Calculate r=(p-1)(q-1)

(iv) Select an integer e for encryption and gcd(r,e)=1; 1<e<r

(v) Calculate d where $d=e^{-1}$ (mod (r))

(vi) Public Key PU = {e,n} and Private Key PR = {d,n}

Elliptic Curve Cryptography (ECC):

Elliptic Curve Cryptography (ECC) is a public key cryptography developed independently by Victor Miller and Neal Koblitz in the year 1985. In Elliptic Curve Cryptography we will be using the curve equation of the form

$$y2 = x3 + ax + b \quad (1)$$

 ISSN: 2321-8169
44 – 47

which is known as Weierstrass equation, where *a* and *b* are the constant with

$$4a3 + 27b2 = 0$$

Point addition:

The two point $P(x1, y1)$ and $Q(x2, y2)$ are distinct. $P + Q = R(x3, y3)$ is given by the following calculation.
Figure 1(a) shows graphical representation of Point Addition operation.

$$x3 = \{\lambda 2 - x1 - x2\} \bmod p \quad (2)$$

$$y3 = \{\lambda(x1 - x3) - y1\} \bmod p \quad (3)$$

where $\lambda = y2 - y1$

$$x2 - x1 \bmod p$$

Point Doubling:

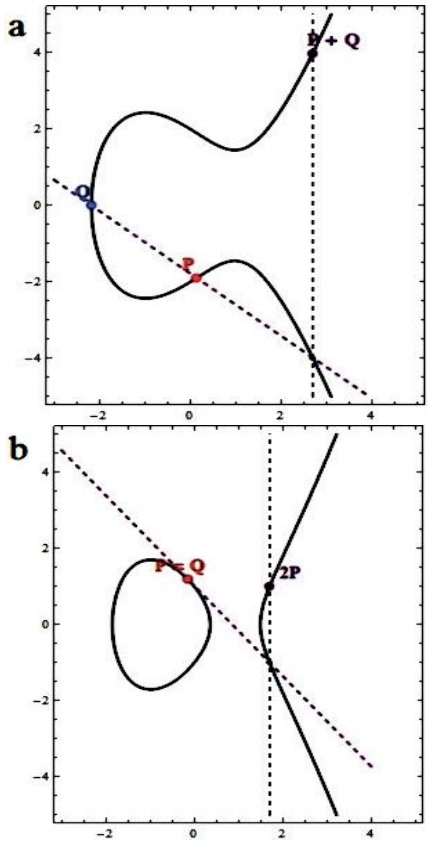
The two point $P(x1, y1)$ and $Q(x1, y1)$ overlap. $P + Q = R(x3, y3)$ is given by the following calculation.

Figure 1(b) shows graphical representation of Point Doubling operation.

$$x3 = \{\lambda 2 - 2x1\} \bmod p \quad (4)$$

$$y3 = \{\lambda(x1 - x3) - y1\} \bmod p \quad (5)$$

where $(3x21 + a)/ 2y1 \bmod p$

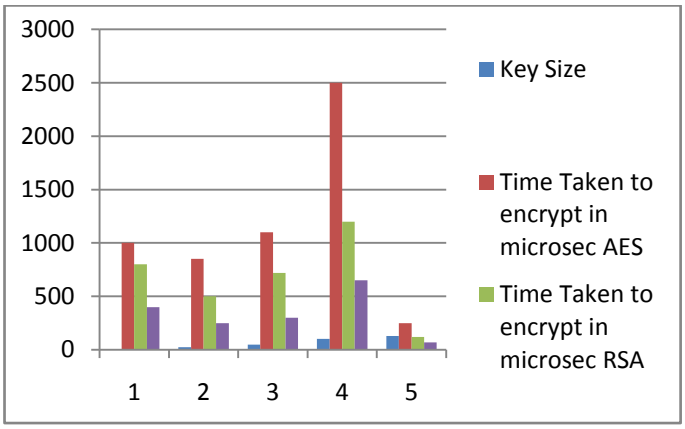


3. RESULTS:

Comparison between symmetric and asymmetric algorithms such as between AES, RSA and ECC are shown below. This compares the time taken to encrypt using these algorithms. This analysis shows that ECC is comparatively better than AES and RSA.

Key Size	Time Taken to encrypt in microsec		
	AES	RSA	ECC
6	1000	800	400
25	850	500	250
48	1100	720	300
102	2500	1200	650
128	250	120	70

The graph for these values is shown as below:



4. CONCLUSION

When compared to symmetric algorithms such as AES and Blow fish, asymmetric algorithms such as RSA and ECC are secure as they maintain two keys where one is secret and the oter is shared. They can be used for authentication, confidentiality, key exchange. ECC is better than RSA as this provides equal security at smaller key length. This can be implemented in any applications that requires security such as Image Encryption, banking applications, online exchanges, e-commerce.

References

[1] Text Book: "Cryptography and network security, Principles and practices", by William Stalling, Retrieved on 8 December 2006.
[2] Adari Bhavana Deepthi, Gandham Venkata Himaja, U.V.Chandra Sekhar M.TECH(PH.D), "
[3] A Novel security techniques based on watermarking and encryption for LSB digital Images"

[4] Bruce Schneier, "The Blowfish encryption algorithm", Dr. Dobb's Journal of Software Tools, 19(4), p. 38, 40, 98, 99, April 1994

[5] Xinmiao Zhang ; Parhi, K.K., "Implementation approaches for the Advanced Encryption Standard algorithm", Circuits and Systems Magazine, IEEE , Vol 2,Issue: 4 , pp 24

[6] Neal Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, Vol 48. Number 177, Jan I987. pp 203-209

[7] Victor S. Miller, "Use of Elliptic Curves in Cryptography", LNCS, Advances in Cryptology — CRYPTO '85 Proceeding, Sec V, pp 417-426, 1986, Springer Berlin Heidelberg.