iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4503

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Comparative Analysis of various Cryptographic Algorithms with ECC

Aman Verma (m. Tech, cse)[1], Sarita Soni (m. Tech, cse)[2]
[1]*M.Tech Student, BBAU, Vidya Vihar Raibareily Road Lucknow*
[2]*Assistant Professor, BBAU, Vidya Vihar Raibareily Road Lucknow*

Abstract: ***In today's generation, internet has been the main source of data communication. In a pervasive computing environment, ECC has been preferred because of its suitability to the devices and having limited battery power, bandwidth, less memory and less computational resources. This paper provides various cryptographic algorithms, its encryption, decryption and general computational approach. Security being the major issues in today's life so the data protection over the communication is very important.***
Index terms: Comparison, Encryption, Decryption, ECC, Operation.

I. INTRODUCTION

An Original message is called Plain Text and a Coded message is called Cipher text. The process of converting the plain text into cipher text is called encryption and the process of retrieving the plain text from cipher text is called decryption. Breaking the code is called cryptanalysis. Together the cryptanalysis and cryptography are called cryptology. Encryption can be divided into Symmetric and Asymmetric. AES (128/192/256 bits), Blow Fish, Two Fish, DES, 3DES, RC4 are all Symmetric whereas Diffie-Hellman Key Exchange, RSA, SHA-224/256/512 and SHA-3 uses asymmetric encryption. ECC is having the quicker evolving capacity and provide an attractive way in cryptographic algorithm [3].

Algorithm	Key	Advantage	Disadvantage	Bit length (in bits)	Attacks
DES	Symmetric	No impact of Brute force attack	Weak in the design of ciphers and Initial/Final Permutations is confusing.	56	Brute Force attack
AES	Symmetric	Secure, Fast in both hardware and Software.	All blocks are ciphered in the same way.	128,192,256	Side Channel attack
Diffie-Hellman Key Exchange	Symmetric	The sender and Receiver have no prior information about each other.	No authentication of participants and exponential operations are used.	2048	Man in the Middle attack
RSA	Asymmetric	Fast, easy to implement and simple encryption.	Slow key generation and decryption.	1024-2048	Brute Force and Side Channel Attacks
Elgamal Encryption	Asymmetric	Discrete Logarithm problem and similar to DH.	Require more bit length than the original plain text.	1024-2048	Chosen cipher text attack
Elliptic Curve	Asymmetric	Fast key generation and shorter key pair.	Complex mathematical descriptions are used.	160-256	Pollard's Rho Method.

Table 1: Comparison between Various Cryptographic Algorithms

II. RELATED WORK

A. Implementing Elliptic Curve Cryptography [1] -This paper shows that the because of shorter keys and efficient algorithm ECC is more future oriented application. This paper gave a short overview of Elliptic Curve Cryptography. Introduced the software framework, which allows transparent replacement of data and algorithms. Also discussed about standardized encoding and interoperability problem that could occur.

B. Theory and Implementation of Elliptic Curve Cryptography [2] -This paper described the mathematics that was needed to implement ECC. Its functionality, challenges and advantages over other cryptographic algorithms. Also, compared various cryptographic algorithms based on efficiency, key size to attain the level of security. Its present and future attacks, including its prevention techniques, which shows the reliability of ECC.

C. Research on Elliptic Curve Cryptography [3] -As there are many drawbacks in current encryption algorithm with respect to security, performance and so on. ECC plays a major role or an alternative for RSA with key size and higher security.

D. Literature Survey on Elliptic Curve Encryption Technique [6] -This paper presents the literature survey on Elliptic curve cryptography and focused on the security while communicating as data is sensitive and ECC plays a major role as it provide encryption, digital signature and key exchange.

III. GENERAL APPROACH OF DES (DATA ENCRYPTION STANDARD)

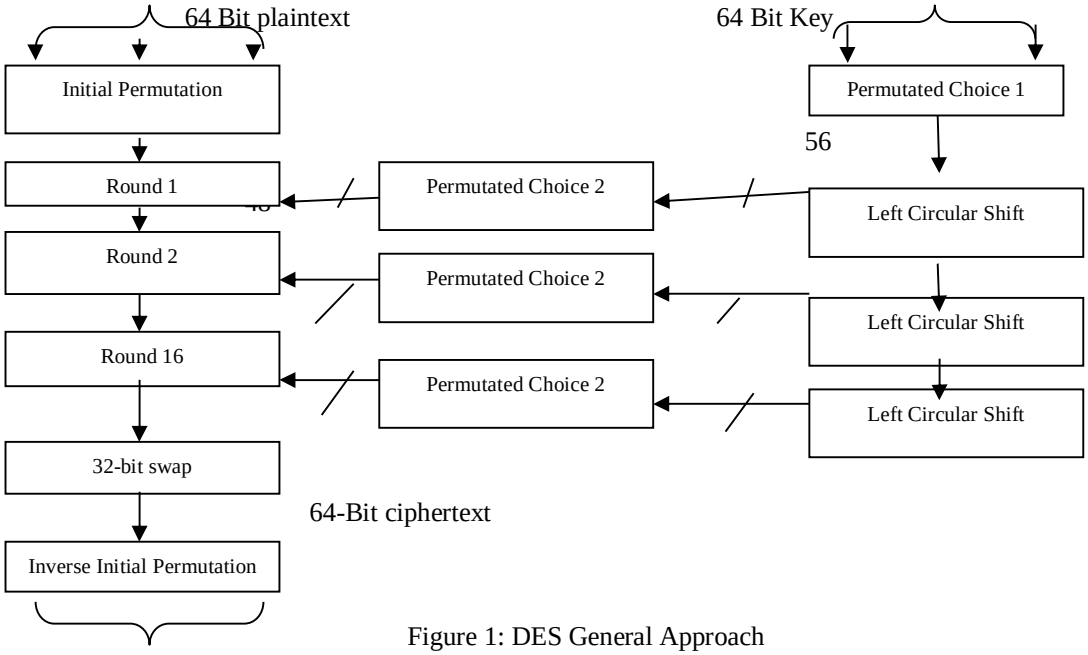


Figure 1: DES General Approach

IV. ELLIPTIC CURVE ARITHEMATIC

ECC offers equal security when compared to RSA. ECC reduces processing overhead by having smaller key size.

A. Elliptic Curve over Real Numbers

Elliptic curve are not ellipses, they are defined by two variables with coefficients. They are named because it is using cubic equations. Weierstrass equation: $y^2 + axy + by = x^3 + cx^2 + dx + e$

Where a, b, c, d are real numbers. $Y^2 = x^3 + ax + b$

B. Geometric Description of Addition

1) Let 0 as the additive identity so 0 = -0 for all P on Elliptic Curve and P+0=P

2) P+(-P) = P-P = 0, P=(x,y) and –P=(x,-y). These two points join on vertical line.

3) P+Q=-R, P+Q is the mirror image of the third point of intersection.

4) P+ (-P) =0

5) Q+Q=2Q=-S

P and Q are different x-axis coordinates, drawing a straight line between them and finding the third point of intersection that is R.

Symmetric Key Algorithm	Diffie Hellman Digital Signature Algorithm	RSA (Size of n in bits)	ECC (Modulus size in bits)
80	L=1024 N=160	1024	160-223
112	L=2048 N=224	2048	224-255
128	L=3072 N=256	3072	256-383
192	L=7680 N=384	7680	384-511
256	L=15,360 N=512	15,360	512+

Table 1: Comparative Key Size of Various Algorithm, L= Size of Public Key and N= Size of Private Key.

C. Algebraic Description of Addition

$$P= (x_p, y_p)$$

$$Q= (x_q, y_q)$$

$$\Delta= (yq - yp)/(xq - xp)$$

As, R=P+Q

$$Xr=\Delta^2 - xp - xq$$

$$Yr=-yp+\Delta\ (xp - xr)$$

operation heirarchy of ecc (kovtun et al 2012) [5]

Cryptographic Transformations	Encryption/Decryption	Digital Signature generation and verification	Key Exchange		
Arithmetic in Elliptic Curve Point Group	Scalar Multiplication of Elliptic Curve Point				
	Point Addition		Point Doubling		
Arithmetic in Finite Field	Multiplication	Addition	Subtraction	Squaring	Inversion
CPU Commands	Mov.mul.shr.add.sub….				

D. Ecc operation Hierarchy is Divided into Various Levels

1) Cryptographic Transformation
2) Arithmetic Operation
a) Elliptic Curve Point Group
b) Finite Field & CPU Commands
3) Scalar Multiplication
a) Addition

b) Doubling

Software Implementation of ECC gives moderate speed and maximum accuracy but still have limited storage and physical security.

V. GENERAL APPROACH OF RSA

In 1977, RSA was developed by Ron Rivest, Adi Shamir, and Len Adleman at MIT and was first published in 1978.

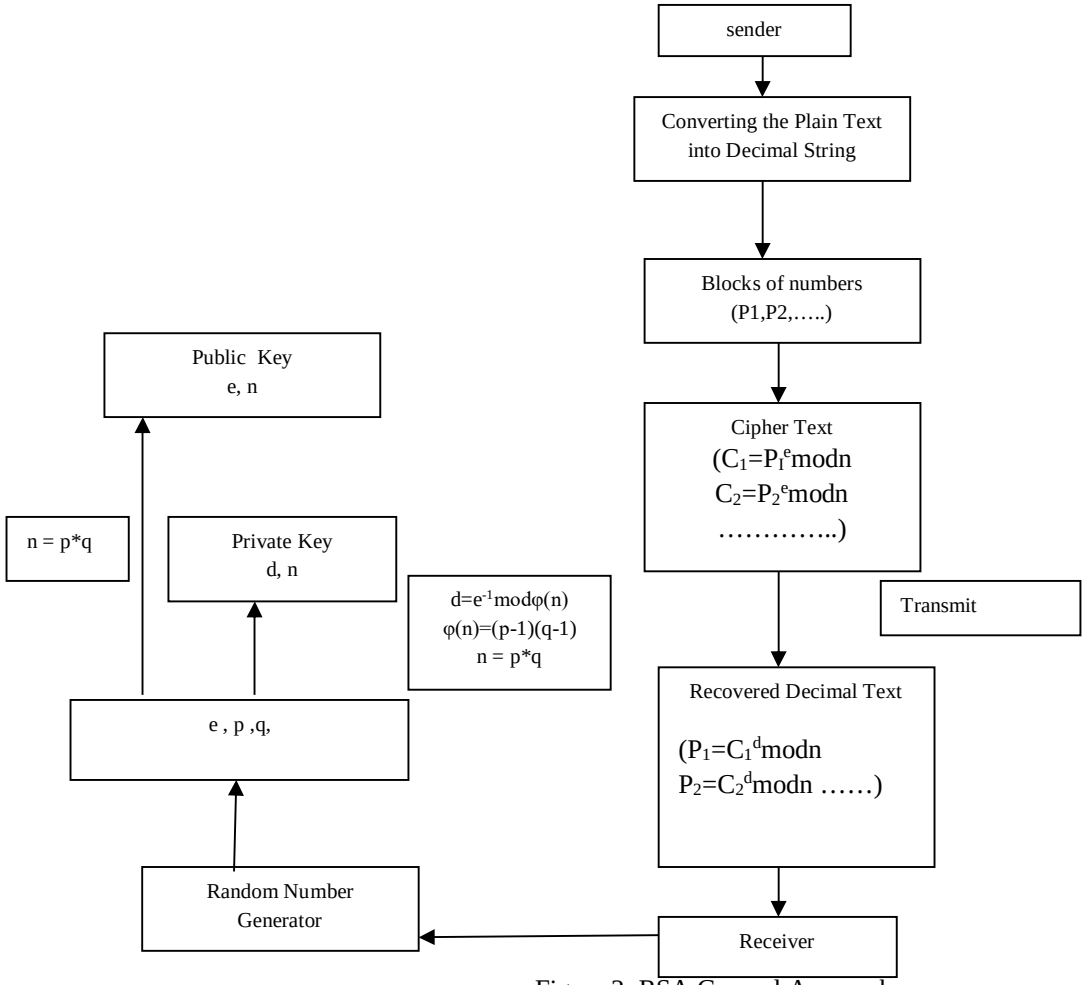


Figure 2: RSA General Approach

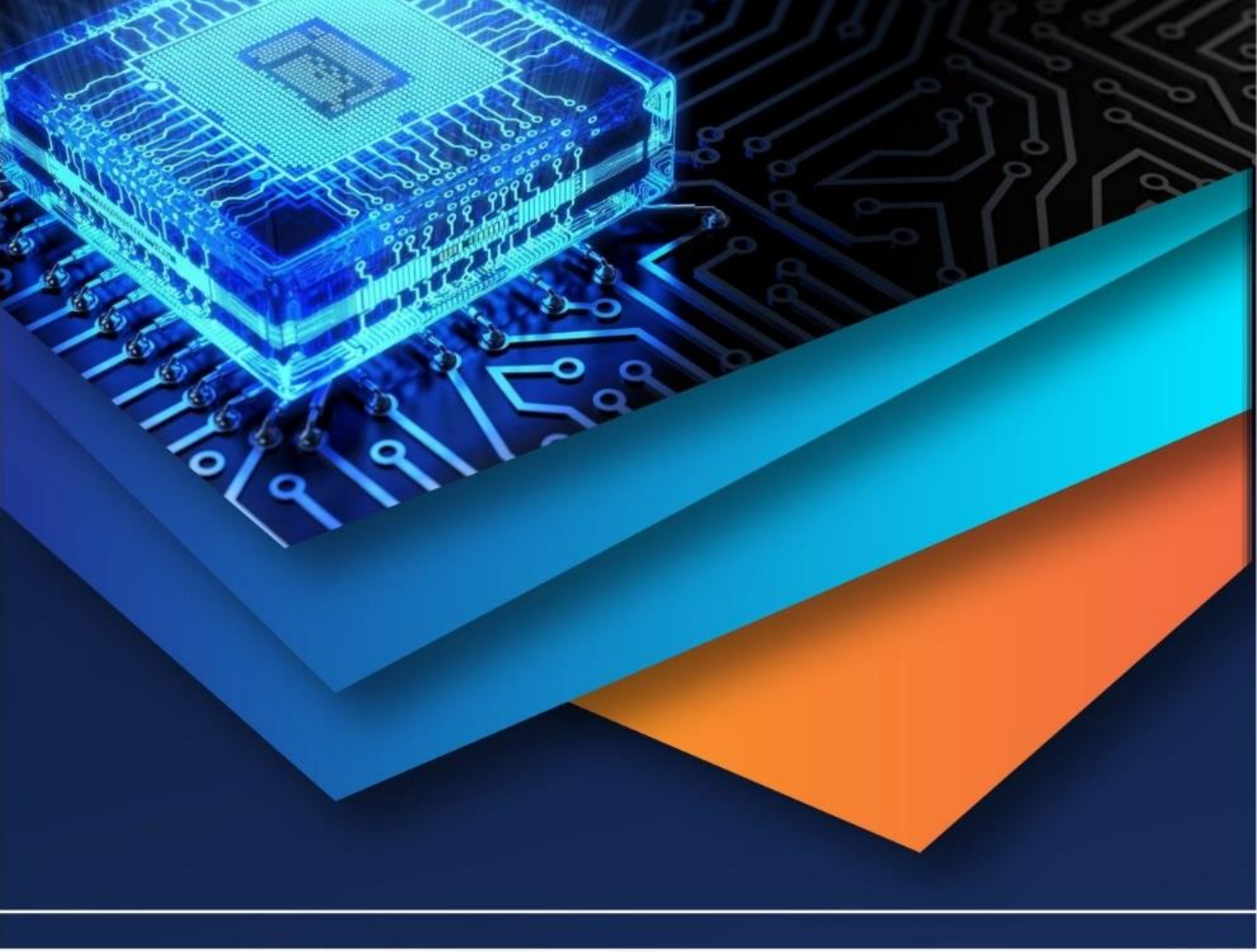
VI. CONCLUSION AND FUTURE SCOPE

As wireless devices are dependent on security features and ECC provide more secure and efficient performance. Hence, ECC provides shorter key size, fast generation of system, smaller space requirement and efficient implementation techniques [7]. ECC can be used in applications such as Smart Card, Pagers and cellular telephones. For portable mobile devices, low power applications and the integration with cloud services, ECC makes an ideal choice.

REFERENCES

[1] Bauer, W. (2002) Implementing Elliptic Curve Cryptography. In: Jerman-Blažič B., Klobučar T. (eds) Advanced Communications and Multimedia Security. IFIP — The International Federation for Information Processing, Vol 100. Springer, Boston, M
[2] Sharad Kumar Verma and Dr. D.B. Ojha, "A Discussion on Elliptic Curve Cryptography and Its Applications", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012 ISSN (Online): 1694-0814 www.IJCSI.o
[3] Fatima Amounas, El Hassan El Kinani, "Secure encryption scheme of Amazigh alphabetic based ECC using finite state machine", Security Days (JNS3) 2013 National, pp. 1-4, 2013.
[4] Shodhganga.inflibnet.ac.in/bitstream/10603/24003/7/07_chapter2.pdf

[5] Ruchika Markan, Gurvinder Kaur, "Literature Survey on Elliptic Curve Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 9, September 2013 ISSN: 2277 128
[6] Samta Gajbhiye ,Dr. Sanjeev Karmakar,Dr. Monisha Sharma, Dr. Sanjay Sharma,Dr. M K Kowar, "Application of Elliptic Curve Method in Cryptography": A Literature Review, Samta Gajbhiye et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012,4499 – 4503, ISSN- 0975-9664
[7] Ms. Priyanka Sharda, "Providing Data Security in Cloud Computing Using Elliptic Curve Cryptography", International Journal on Recent and Innovation Trends in Computing and Communications, volume 3, Issue: 2, ISSN- 2321-8169 413-417.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY