International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
International Conference & workshop on Advanced Computing 2014 (ICWAC 2014) – www.ijais.org

Security Enhancement Algorithm for Data Transmission using Elliptic Curve Diffie - Hellman Key Exchange

Shaikh Ammarah P.
Thakur College of Engg. & Technology
Maharashtra, mumbai

Vikas Kaul
Thakur College of Engg. & Tech.
Maharashtra, mumbai

S K Narayankhedkar
MGMCET
Navi mumbai

ABSTRACT

Data Security for end-end transmission is achieved by many different symmetric and asymmetric techniques for message confidentiality, message authentication and key exchange using transport layer security.

This paper presents the combination of two symmetric algorithms AES and Blowfish to enhance security. AES is enhanced by modifying the S-boxes columns, and then combination of enhanced AES and blowfish is used for data confidentiality. Message digest 5 is used for authentication. Key exchange is done using ECDHA, Elliptic Curve Diffe Hellman algorithm. ECDSA is used for digital signature.

Performance of this system is evaluated for text file, image file, audio file and video file on the basis of encryption/decryption processing time and throughput.

Keywords

Symmetric encryption, AES, Blowfish, enhanced AES, Elliptic Curve Cryptography, ECDH, MD5 and ECDSA.

1. INTRODUCTION

Network security [1] involves methods or practices used to protect a computer network from unauthorized accesses, misuses or modifications. Data encryption is important for improving database security, preventing the data from theft and tampering. The data encryption algorithms are broadly classified into two categories a) symmetrical encryption algorithm (Private-Key-Cryptography) [2] and b) asymmetrical encryption algorithm (Public-Key-Cryptography) [3]. The symmetrical encryption algorithms are DES, IDEA, Blowfish, RC4, RC5, RC 2, 3DES and AES. Asymmetric key encryption algorithms are RSA, Robin, ElGamal and Elliptic Curve.

The classification of cryptography techniques is shown in Figure 1.

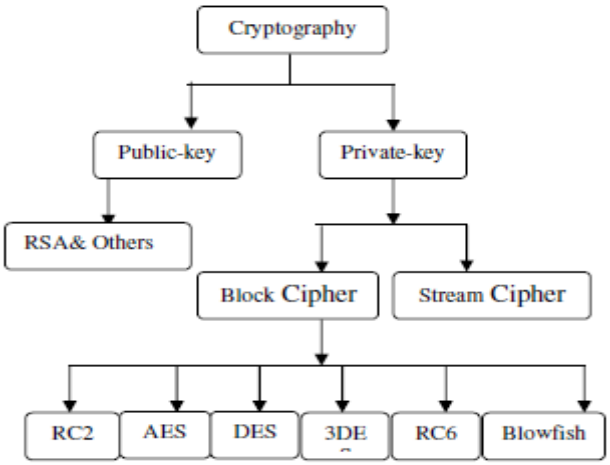


Figure 1. Classification of Cryptography techniques

2. SYMMETRIC ALGORITHMS

In this proposed system two symmetric algorithms, Blowfish and AES, are used.

2.1 Blowfish Algorithm

Blowfish algorithm was developed in 1993. Blowfish [4], is a symmetric encryption algorithm with a variable-length key block cipher. It is a Feistel network, iteration with the encryption function up to 16 times. The size of block is 64 bits and the key lies at any length up to 448 bits. [5] When implemented on 32-bit microprocessors with large data caches which is significantly faster than DES.

The algorithm as shown in Figure 2 consists in two parts.

First is key-expansion part and other is data- encryption part. Key expansion converts a 448 bits key into several sub-key arrays of 4168 bytes in total. Data encryption is done through 16-rounds. Each round performs an permutation depending on key and substitution depending on data using XOR operation and addition on 32bit words.

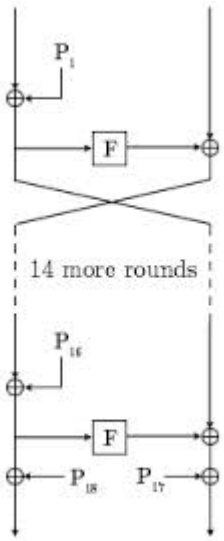


Figure 2. Blowfish Algorithm

2.2 Advance Encryption Standard

AES was developed in 1999. AES was announced by National Institute of Standards and Technology (NIST). AES is a block cipher symmetric algorithm with block length 128 bits and key lengths of 128, 192 or 256. The key size of the algorithm depends on the number of rounds in algorithm. The algorithm is as shown in Figure 3.

In AES, there are four transformations for one round

1) SubBytes - It's a nonlinear substitution, here each byte is replaced by another fix bytes.
2) ShiftRows - each row is rotating according to row position from right to left. Like 0^{th} row rotate for 0times, 1^{st} row rotates for 1 time, 2^{nd} row rotates for 2 times and 3^{rd} row rotates for 3 times.
3) MixColumns - performs mixing operation on columns with constant and data.
4) AddRoundKey - combining data's bytes column with a key's byte column.

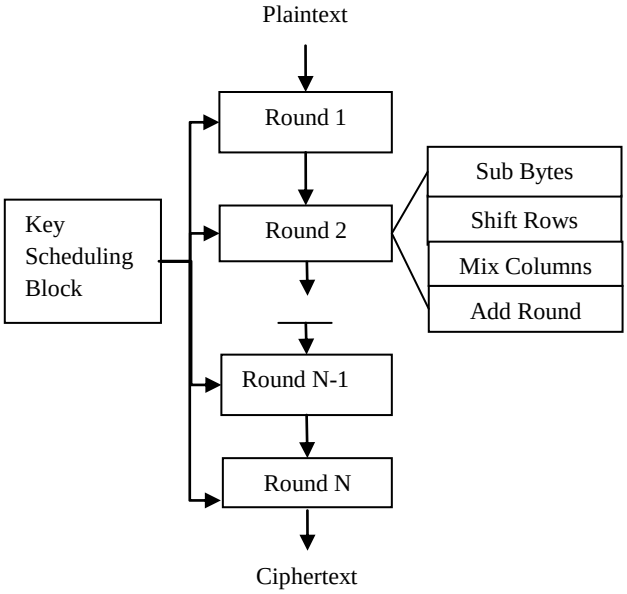


Figure 3. AES Algorithm

AES Algorithm

1) Key expansion - It derives the keys for each round.
2) Initial round before 1st round - Only perform Add round key.
3) N-1 Rounds - Perform all four transformations.
4) Final Round Nth round - Only MixColumns transformation is absent in this round.

Improved AES get by changing the column of S-Boxes in the standard S-Boxes.

3. ASYMMETRIC ENCRYPTION ALGORITHMS

There are many asymmetric algorithms used for encryption. In symmetric-key cryptography, symbols are either permuted or substituted but in Asymmetric-key cryptography, numbers are manipulated. In this system the concept of Elliptic Curve is used.

3.1 Elliptic Curve Cryptography

Elliptic Curve Algorithm is standardized IEEE P1363 for public key cryptography [6]. ECC offers equal security compared to RSA with small key size [7]. ECC is difficult to understand than RSA. The ECC over GF(p) or GF(2^n) is shown in Figure 4.

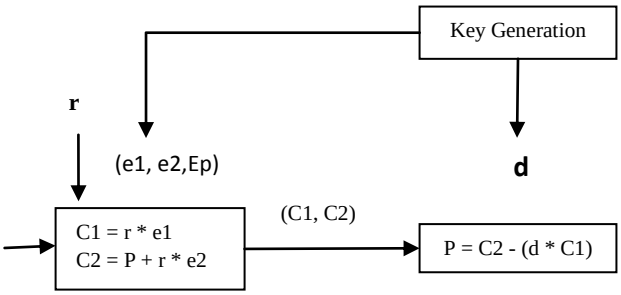


Figure 4. Elliptic Curve Cryptosystem

d - private key

Ep - set of points on curve

e1 and e2 - two points on curve as a public key

P - plaintext

C1 and C2 - ciphertext

r - random number

ECC Algorithm

Key generation (Public and Private):

1) Find points Ep(a,b) on Elliptic curve with proper square root with an Elliptic curve over GF(2^n).

2) Choose point on curve, e1(x1,y1).

3) Choose an integer d.

4) Calculate e2(x2,y2) = d*e(x1,y1) (Binary method for point multiplication [17])

5) Announce E(a,b), e1(x1,y1) and e2(x2,y2) as a public key.

Encryption:

C1 = r * e1

C2 = P + r * e2

Decryption:

P=C2 - (d * C1)

4. SYMMETRIC AND ASYMMETRIC ENCRYPTION ALGORITHMS

The performance evaluation of symmetric algorithm was done by Nadeem, A. and Javed, M.Y in 2006 [8]. They implemented it on JAVA and evaluated the performance by time required for encryption/decryption. They compared the symmetric encryption techniques like DES, Triple DES, AES and Blowfish.

Results shows that Blowfish has no known security weaknesses and also Blowfish algorithm gives more throughput as compared to other symmetric encryption algorithms [8]. Blowfish has not any known security weak points, which makes it an excellent standard encryption algorithm.

AES is considered as a Standard algorithm, the Brute force attack is possible on it, but the AES gives more security then other algorithms. The throughput of AES is less as compare to the Blowfish but when we are more concerned about security AES is best. AES can also be used in a Bluetooth communication by hybrid AES and RSA [9]. If data types are changing like text to image then the other algorithms like RC2 and RC6 are time consuming and Blowfish shows better performance [10].They have shown the results in both CBC and ECB mode of operation. The throughput of ECB was more than the encryption in CBC mode but CBC is preferable because of its security. Blowfish algorithm can be used in software applications but its key size may be a cause of concern.

RSA, Rabin, ElGamal and ECC are asymmetric cryptosystems. An asymmetric key cryptosystem is faster and it also consumes less power than the symmetric key cryptography but the symmetric key gives more security. Triple DES and RSA hybrid can also be done to enhance the security for wireless communication [11]. The features of both the cryptosystems can be gathered by combining both. Symmetric key cryptography can be used for encryption/decryption and asymmetric cryptography for Key Management.

5. KEY MANAGEMENT

Keys are used in cryptography to achieve confidentiality or data integrity.

Key management process is the set of processes, which are required to establish the key and distribute the same to authorized parties. The processing of sharing the key between more than one parties, called Key Distribution [12].

In symmetric key agreement, the shared key is established between two parties without using any Key Distribution Centre (KDC). There are two methods for symmetric key agreement/key exchange; Diffie-Hellman key agreement and station to station key agreement. DH is not an encryption/decryption algorithm.

6. MESSAGE AUTHENTICATION/ ENTITY AUTHENTICATION AND DIGITAL SIGNATURE

Message integrity can be achieved by cryptographic hash functions. Hashing algorithms are MD2, MD4, MD5 and SHA1. SHA1 and MD5 are the best algorithms for hashing. Authentication and non-repudiation security goals are achieved by doing digital signature.

A hashed code is a fixed-size fingerprint of a variable-sized message. Hash code is known as message authentication code (MAC).

7. LITRATURE SURVEY

Evaluating the six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6 was done. A comparison was based on different sizes of data blocks, different data types and battery power consumption with different key sizes and finally encryption/decryption speed. Concluding Blowfish had a better performance than other algorithms. Also AES gave poor performance compared to other algorithms since it needs more processing power. Using CBC mode had added extra processing time and overall it is relatively negligible for certain applications especially which require more secure encryption to relatively large data blocks [20].

The proposed architectures with Mixcolumn and pre-process InvMixcolumn were integrated together to perform Mixcolumn/InvMixcolumn transformation to have more area efficiency than previous related work [21]. Evaluated encryption speed and power consumption for their performance showed that Blowfish algorithm runs faster than DES algorithm while both of them consume almost the same power. Blowfish algorithm maybe more suitable for wireless networks with small size packets exchanges [5]. Hardware implementation of the AES had the advantage of increased throughput and offers better security. Used search based S-box architecture to reduce the constraint in the hardware resources. Hardware implementation gives faster speed and better security when compared to software models [22]. Differential power analysis (DPA) is effective on the ECC on devices. The zero-value point attack could be resisted if randomized the scalar. Randomize not only the base point but also the secret scalar [23]. Experiment over the standard elliptic curves, found that many non-standard exceptional points even though the standard addition formula over the curves has no remarkable point. Whenever a new addition formula is to be developed, one should be cautious about the proposed attack [24]. The proposed scan-based attack namely timing and leakage analysis

that allows finding out data related to the secret key among the bits observed through the Design-for-Testability (DfT) structures. Setup allows full automation of the proposed scan attack on designs including DfT configurations. Require around 8 chosen points to implement the attack for retrieving a 192-bit scalar [25]. The analysis and computational comparison to the randomized methods showed that the combinatorial approach has clear advantages: a) it increases the probability of a pair of sensor nodes to share a key, and b) decreases the average key-path length while providing scalability with hybrid approaches [26]. Mix of improved AES and ECC encryption algorithm, can not only enhance the speed of data encryption and decryption, but also solute the problem of key distribution and authentication. It has high computing speed and anti-attack capability, which improved the security of data transmission process effectively [27]. The algorithms are AES, DES, and 3DES, RC6, Blowfish and RC2. According to changing the size of packet, it has been concluded that Blowfish has a better performance than other common encryption algorithms used, followed by RC6. It also shows 3DES still has low performance compared to algorithm DES, RC2 has disadvantage over all other algorithms in terms of time consumption and they conclude AES has comparatively better performance than other symmetric algorithms (RC2, DES, and 3DES). In aspects of audio and video files the result is the same as in text and document. Finally the case of changing key size - higher key size leads to clear change in the battery and time consumption [28]. The image distortion is very low and that the achieved capacity is enough to embed reliability proof as well as some other data. Joint watermarking/encryption system is slower than simply encrypting the image but it provides reliability control functionalities [29].

8. HYBRID SYMMETRIC AND ASYMMETRIC ENCRYPTION ALGORITHMS

First we use two symmetric encryption algorithms AES and Blowfish. Combination of these two algorithms will increase the run time for encryption/decryption. The total time required for hybrid algorithms will be the addition of both the algorithm's run time (processing time). Blowfish requires less time as compared to others algorithms, Blowfish algorithm adds the additional time for processing but it will enhance the overall security. The combination of enhanced AES and Blowfish is as shown in Figure 4.

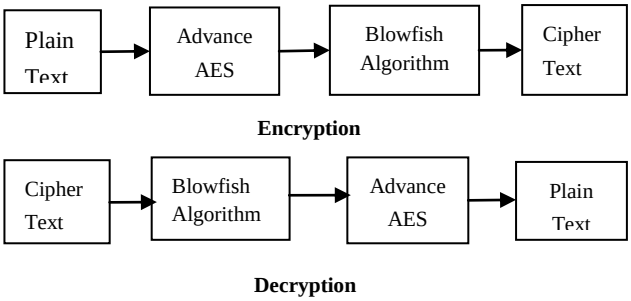


Figure 4. Hybrid AES and BF

Public keys will be distributed by the symmetric key agreement protocol [13]. Here, for key management ECC (Elliptic Curve Cryptography**)** concept is used instead of RSA. RSA can also be combined with AES [14]. ECC gives same security as compare to the RSA algorithm but with small key size. ECC requires less computational power, low bandwidth and minimum memory. Here the secret key is created by the ECC algorithm and then applied to DH for key exchange [15]. Combining the two algorithms ECC and DH is called Elliptic Curve Diffie-Hellman Key Exchange (ECDH) [16][17].

For integrity MD5 hashing algorithm is used. Authentication is done by ECDSA (Elliptic Curve Digital Signature Algorithm). ECC digital signature is better than the RSA digital signature [18]. For the model of proposed system see Figure 5 and Figure 6.

Here we use the same key for Advance AES and Blowfish algorithms. The key is encrypted by the ECC algorithm with the help of public key generated by ECC key generator. ECDH performs key management between two parties. Hashing is done by MD5.

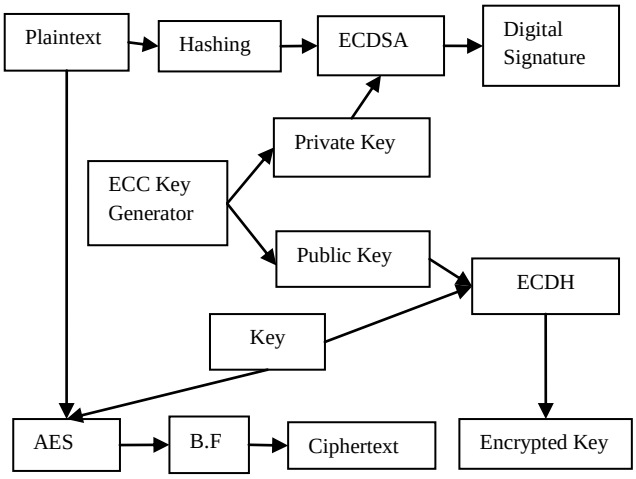


Figure 5. Sender's System Architecture

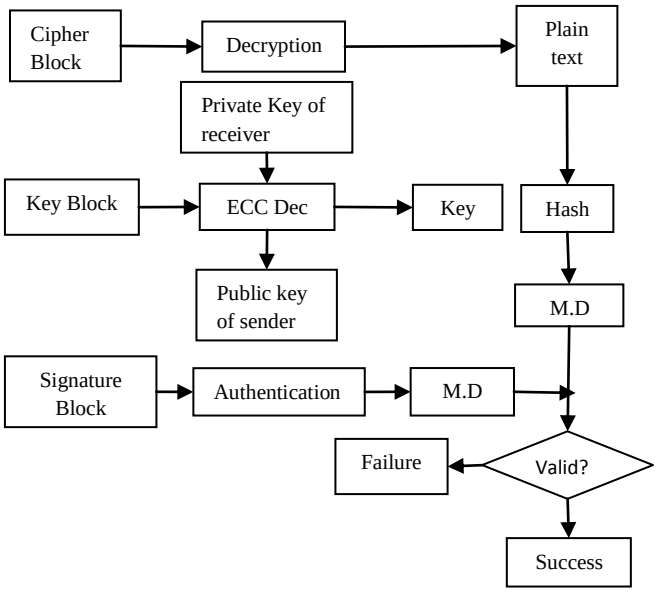


Figure 6. Receiver's System Architecture

9. RESULTS BASED ON RUNTIME AND THROUGHPUT

Both the algorithms are implemented on JAVA and tested on AMD Phenom (tm) II P 960 Quad configurations.

Algorithms:-
Encryption/Decryption: Enhanced AES and Blowfish
Key Management: ECDH
Hashing: MD 5
Digital Signature: ECDSA
Computer Configuration: AMD Phenom (tm) II P 960 Quard Processor: Core Processor 1.7GHz.
Run Time: Millisecond.
Throughput: bits Per Second.
Result analysis is done on different type of inputs such as document, image, audio and video, shown in Table 1.

Table 1. Data inputs Files

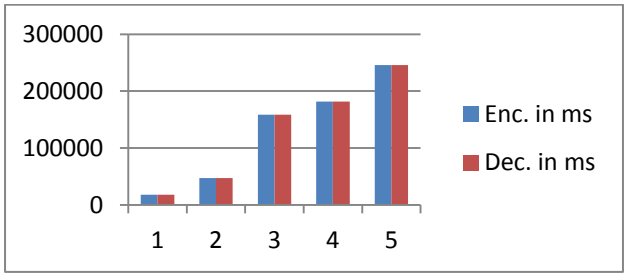
Sr.	File name with extension	File Size in bits
1	File1.jpeg	81182
2	File2.mp3	212992
3	File3.mp4	714342
4	File4.doc	819200
5	File5.pdf	1105920

9.1 Result based on Runtime

Enhanced AES encryption and decryption runtime in millisecond are shown in Table 2 and Graph 1.

Table 2. Enhanced AES enc./dec. runtime

Sr. No.	Data Bits	AES Enc. in ms	AES Dec. in ms
1	81182	18599	18543
2	212992	49535	48991
3	714342	158589	158850
4	819200	181665	180920
5	1105920	247219	245593

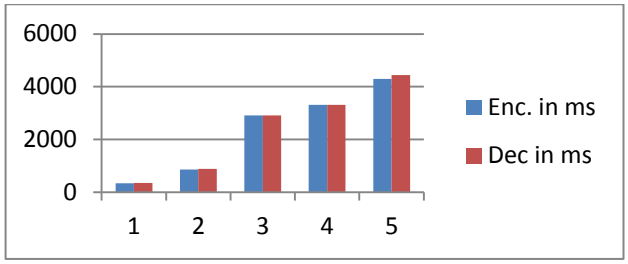


Graph 1. Enhanced AES enc./dec. runtime

B.F encryption and decryption runtime in millisecond are shown in Table 3 and Graph 2.

Table 3. Blowfish enc./dec. runtime

Sr No.	Data Bits	B.F Enc. in ms	B.F Dec in ms
1	81182	341	348
2	212992	856	883
3	714342	2907	2915
4	819200	3315	3314
5	1105920	4301	4439

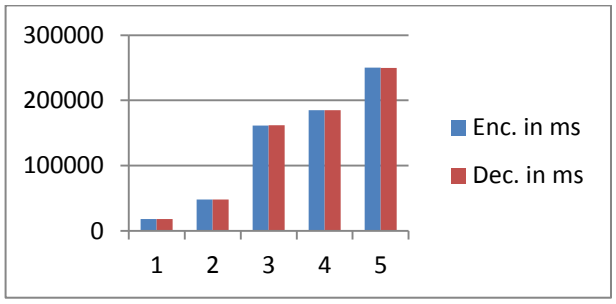


Graph 2. Blowfish enc./dec runtime

Hybrid of enhanced AES and BF algorithm runtime are shown in Table 4 and Graph 3.

Table 4. Hybrid enhanced AES and BF enc./dec. runtime

Sr. No.	Data Bits	AES + BF Enc. m.s	AES + BF Dec. m.s
1	81182	18940	18891
2	212992	50391	49874
3	714342	161496	161765
4	819200	184980	184234
5	1105920	251520	250032



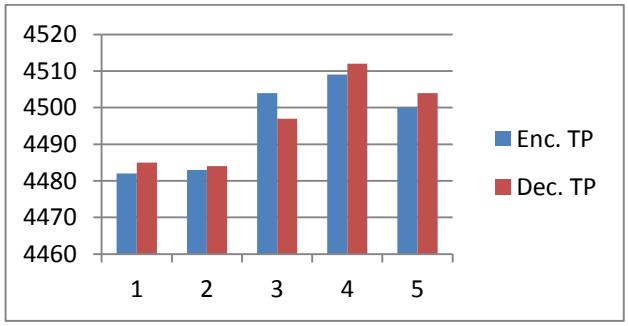
Graph 3. Hybrid enhanced AES and BF enc./dec. runtime

9.2 Result based on Throughput

The enhanced AES encryption and decryption throughputs are shown in Table 5 and Graph 4 and BF encryption and decryption throughputs are shown in Table 6 and Graph 5.

Table 5. Enhanced AES enc./dec.Throughput

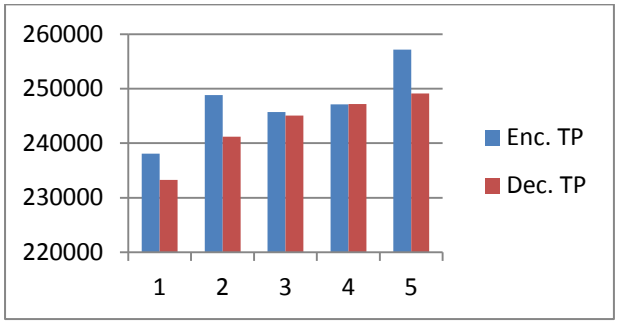
Sr. No.	Data Bits	AES Enc. TP	AES Dec. TP
1	81182	4482	4485
2	212992	4483	4484
3	714342	4504	4497
4	819200	4509	4512
5	1105920	4500	4504



Graph 4. Enhanced AES enc./dec. Throughput

Table 6. BF enc./dec. Throughput

Sr. No.	Data Bits	B.F Enc. TP	B.F Dec. TP
1	81182	238070	233281
2	212992	248822	241214
3	714342	245731	245057
4	819200	247119	247193
5	1105920	257130	249137

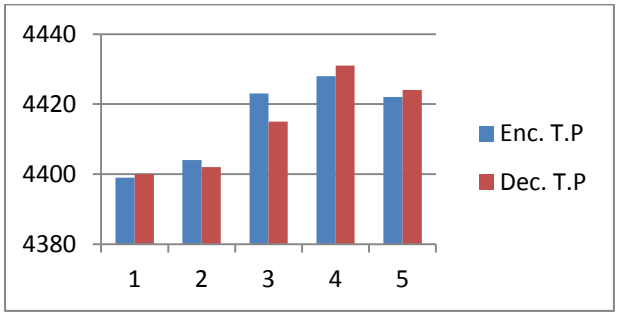


Graph 5. BF enc./dec. Throughput

The hybrid enhanced AES and blowfish throughputs are shown in Table 7 and Graph 6.

Table 7. Hybrid enhanced AES and BF enc./dec. Throughput

Sr. No.	Data Bits	AES + BF Enc. T.P	AES + BF Dec. T.P
1	81182	4399	4400
2	212992	4404	4402
3	714342	4423	4415
4	819200	4428	4431
5	1105920	4422	4424



Graph 6. Hybrid enhanced AES and BF enc./dec. Throughput

10. SUMMARY AND CONCLUSION

Experiment results show that the average encryption throughput for Blowfish is 247374 bps and the average decryption throughput is 24316 bps. The average throughput for enhanced AES is 4495 bps and the average decryption throughput is 4496 bps. After combining these two algorithms the resultant throughput for encryption is 4415 bps and throughput for decryption is 4414 bps.

AES is more secure than the Blowfish algorithm, and Blowfish is secured than the other algorithms. Blowfish gives high throughput as compared to others. The hybrid of AES and Blowfish algorithm has characteristics of both the algorithms and it makes the algorithm strong against vulnerabilities. This hybrid structure of enhanced AES and Blowfish provides more security. Better key exchange provided by ECDHA with authentication.

11. FUTURE WORK

The processing time can be reduced by running both the algorithms simultaneously instead of one after another. Blowfish can be replaced by Twofish symmetric algorithm. SHA1 can be used instead of MD5 for Message Digest. This work can be realised for 4G/5G networks where there is a need for Next Generation Encryption.

12. REFERENCES

[1] "Network Security", Cisco system, ISOC NTW, 2000.

[2] Ayushi, 2010 "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15.

[3] Thorsteinson, 2003. "Asymmetric Cryptography", book Page 99 July 29.

[4] Bruce Schneier, 2008 "The Blowfish Encryption Algorithm".

[5] T. Nie, C. Song, X. Zhi 2010 "Performance Evaluation of DES and Blowfish Algorithms", Biomedical Engineering and computer Science International Conference, *IEEE*.

[6] N. Koblitz., 1987 "Elliptic curve cryptosystems", *Mathematics of Computation"*, 48, pages 203–209.

[7] M.J.B. Robshaw, Y. Lisa Yin, 1997. "Elliptic Curve Cryptosystems", an RSA Laboratories Technical.

[8] Nadeem, A., Javed, M.Y., 2005 "A Performance Comparison of Data Encryption Algorithms," *IEEE*, Information and Communication Technologies, *ICICT*, First International Conference, pp. 84- 89.

[9] K. Rege, N. Goenka, P. Bhutada, S. Mane, 2013, "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA", International Journal of Computer applications (0975–8887) Volume 71– No. 2.

[10] D. S. Abdul, Elminaam, H. M. Abdul Kader and M. M. Hadhoud, 2009 "Performance Evaluation of Symmetric Encryption Algorithms" Communications of the *IBIMA* Volume 8, ISSN: 1943-7765.

[11] A. C. Pamarthy, K. Rajasekha. 2012. " A Hybrid Encryption Algorithm Based on Triple DES and RSA", International Conference on Information Technology, Electronics and Communications (*ICITEC*).

[12] A. Menezes, P. van Oorschot, S. Vanstone, 1996, "Key Management Techniques," CRC Press.

[13] Malan, David J., M. Welsh, M. D. Smith, 2004 "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography". IEEE SECON 2004: 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks: SantaClara, California, 71-80. Piscataway, N.J. *IEEE*, 4-7.

[14] K. Rege, N. Goenka, P. Bhutada, S. Mane, 2013 "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA", International Journal

of Computer Applications (0975 – 8887), Volume 71– No.22.

[15] R. Ahirwal, M. Ahke 2013 "Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network", (*IJCSIT*) International Journal of Computer Science and Information Technologies, Vol. 4 (2), 363 - 368.

[16] A. Chandrasekar, V.R. Rajasekar, V. Vasudevan, "Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography", International Journal of Computer Science and Security (*IJCSS*), Volume (3), Issue (4).

[17] H. Brar, 2010 "Performance analysis of Point multiplication methods for Elliptic curve".

[18] N. Jansma, B. Arrendondo 2004 "Performance comparison of elliptic curve and RSA digital signatures".

[19] G. M. Bertoni, F. Roberto, L. Breveglieri, F. Regazzoni, 2006 "Speeding Up AES By Extending a 32 bit Processor Instruction Set", Application-specific Systems, Architectures and Processors, *IEEE*.

[20] Abdel-Karim, Al Tamimi 2006, "Performance Analysis of Data Encryption Algorithms ".

[21] Yu-Jung Huang, Yang-Shih Lin, Kuang-Yu Hung, Kuo-Chen Lin 2006 "Efficient Implementation of AES IP", *IEEE*.

[22] Subashri T, Arunachalam R, Gokul Vinoth Kumar B, Vaidehi V 2010, "Pipelining Architecture of AES Encryption and Key Generation with Search Based Memory"**,** International journal of VLSI design & Communication Systems (VLSICS) Vol.1, No.4.

[23] T. Akishita, T. Takagi 2003 "Zero-Value Point Attacks on Elliptic Curve Cryptosystem".

[24] Izu, T. Takagi, 2003 "Exceptional Procedure Attack on Elliptic Curve Cryptosystems".

[25] I. Verbauwhede, B. Rouzeyre, M. Flottes, G. Di Natale, A. Das and J. Rolt, 2005 "A scan-based attack on Elliptic Curve Cryptosystems in presence of industrial Design-for-Testability structures".

[26] Seyit A. 2007 "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", *IEEE*.

[27] X. Li, J. Chen, D. Qin, W. Wan**,** 2010**,** "Research and Realization based on hybrid encryption algorithm of improved AES and ECC", *IEEE*.

[28] D. Salama Abdul Minaam, H. M. Abdual-Kader2, M. Mohamed Hadhoud 2010, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", *International Journal of Network Security*, Vol.11, No.2, PP.78-87.

[29] D. Bouslimi, G. Coatrieux, 2012, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", *IEEE*.