An Efficient Steganography Encryption using Hybrid Cryptography

Dr S Selvi[1], Dr M Gobi[2]
[1]Professor,PSG College of Arts and Science, Coimbatore,TamilNadu,India
[2]Chikkanna Govt.Arts College,Tripur,TamilNadu,India

Abstract*-Data Security these days is turning into an essential worry for any correspondence procedure particularly when it is having classified data and needs to go through an uncertain medium of correspondence. There are numerous methods to shield the information from unapproved get to. Techniques like Symmetric Encryption makes utilization of a mystery key which is utilized by the sender and the beneficiary for scrambling and unscrambling the substance separately. Strategies, for example, lopsided encryption makes utilization of two distinctive keys to do a similar undertaking. The previous technique is quicker when contrasted with the last mentioned however needs as far as security. The last technique makes utilization of an open key framework to make the encryption procedure open however decoding private henceforth expanding the general intricacy. The best known symmetric figure AES[11] makes utilization of 256 piece keys to do the encryption. Exceptionally notable awry strategy RSA[12] makes utilization of 1024 piece keys to do a similar occupation, in this manner expanding the time and space intricacy at the cost of expanded security. Another awry partner ECC[13] makes utilization of a totally unique approach by changing over the characters into relative purposes of an elliptic bend. It makes utilization of 160 piece keys and delivers a similar outcome at a greatly improved pace when contrasted with RSA. In this paper a novel proficient model of Hybrid Encryption including AES and ECC is advanced which scrambles any interactive media information i.e. content, picture, sound, video, and so on. The benefits of both AES and ECC are used to make an all the more intense half and half figure to cross over any barrier of speed and security. With the assistance of lesser estimated keys the time figure required to do the encryption is diminished. The outcomes gotten after execution mirrored a 100 % precision and a colossal speed increase over the current symmetric and hilter kilter innovations. The execution is completed in the Java condition by making separate keys and using them to do the encryption.*

Keywords-ECC, Hybrid Encryption, Steganography Multimedia Encryption, Cryptography, Symmetric Encryption, Asymmetric Encryption

I. INTRODUCTION

An Encryption assumes an exceptionally essential part with regards to ensure the substance of any secret information. The historical backdrop of encryption goes back to the antiquated Civilizations where information was kept mystery by concealing it or securing it by scrambling the substance of the message to make it disjointed. The extremely essential Caesar Cipher[14] establishes the framework for now's cutting edge modern calculations. The idea of substitution is utilized as a groundwork to outline the calculations that we know today. We have a variety of symmetric [15] calculations accessible, for example, AES and DES which give a fast scrambling up of the information utilizing a solitary key. Though awry [15] calculations, for example, RSA, Blowfish, ECC [16] and so on utilize 2 keys to do a similar undertaking however give better security. Both having their equivalent offer of favorable circumstances and burdens, however with regards to encoding mixed media information, for example, pictures, sound and video, the current calculations confront a precarious test, for example, memory and time contemplations, throughput, the measure of keys to be utilized and the space required to store the scrambled document.

In this paper a cross breed of AES and ECC calculation is planned and executed in Java runtime utilizing Flexi-Core Cryptographic libraries. The calculation makes utilization of productively arranged arrangement of keys which inevitably decreases the unpredictability of sparing a bigger key. AES is picked as the symmetric.

partner since it gives the outcome quicker and superior to anything DES though ECC is picked as the awry key partner since it does the encryption by utilizing less number of keys when contrasted with RSA and at a considerably speedier pace[1][2][3].

The crossover calculation is intended to scramble any interactive media document, for example, sound, video, pictures and content by changing over it into a content proportionate to lessen the general time requirement. Keeping every one of the restrictions of the overall advancements as a top priority and detecting the need of a superior encryption show for media information, as far as security, memory and time, a framework is composed, which addresses the issues.

II. PROBLEM STATEMENT

Key Size: The Symmetric figures utilize just a solitary key for encryption and decoding, henceforth the span of the key ought to be sufficiently substantial with the goal that it can't be effectively speculated by any enemy utilizing the animal constrain assaults. Lopsided figures then again utilize 2 keys for doing likewise which impacts the memory antagonistically yet gives better security.

Time Complexity: Complex plan approaches mean the time multifaceted nature and straightforward ones give better time many-sided quality at the cost of security. Thus an exchange off between the two should be set up.

Memory Efficiency: Text encryption frameworks offer a superior memory adequacy when contrasted with interactive media encryption frameworks however need as far as assortment, though sight and sound encryption requires a considerable measure of free memory space to store the keys, input documents, figured records and the yield documents. Henceforth, again an exchange off amongst assortment and memory should be set up.

Types of Inputs bolstered: All the frameworks considered and investigated were all single worked, i.e they all bolster encryption for content sources of info straightforwardly from the client or as records containing literary data or even instant messages as SMS's. With regards to high necessity sight and sound data sources, for example, pictures, sound, video, graphical substance, and so forth the current frameworks need in execution due to issues, for example, high memory prerequisite and time required to scramble/unscramble them.

III. DESIGN METHODOLOGY

The cross breed encryption model depends on blended encryption worldview [4] where media information is subjected to an essential pressure known as Base64 Encoding [5]. This Base64 encoded organize document changes over the mixed media source record into an a little bit at a time message variant of the underlying organization. This Base64 configuration is a standard organization which regardless of the arrangement of the source media creates a content adaptation of the same. This stances as the underlying level of encoding. This Base64 organize document then goes about as the underlying Plaintext (P.T) which is additionally subjected to an ECC encryption taken after by AES Encryption to yield the last Ciphertext. The current AES calculations utilize keys going from 128, 192 and 256 bits relying on the quantity of rounds i.e either 10, 12 or 14 separately. The current ECC keys utilize at least 160 piece keys for the encryption. The Table 1 clarifies the keys prescribed by NIST [6] through a point by point depiction about the proportionality between the key lengths among various encryption calculations. For correlation reason an AES calculation of 192 bits is chosen which compares to a 7680 piece RSA figure and a 384 bits ECC calculation. In the planned half and half technique an ECC calculation of 160 bits and relating AES calculation of 128 bits is picked which would give a similar level of security to the information however under a diminished time interim. The half breed calculation would make utilization of 128 + 160 = 288 piece keys for the encryption and unscrambling. This further decreases the multifaceted nature for putting away the keys.

Table 1. NIST recommended key sizes [7]

Symmetric Key Size(bits)	RSA and Diffie-Hellman Key Size(bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

The overall encryption methodology is as shown in the figure 1 below.

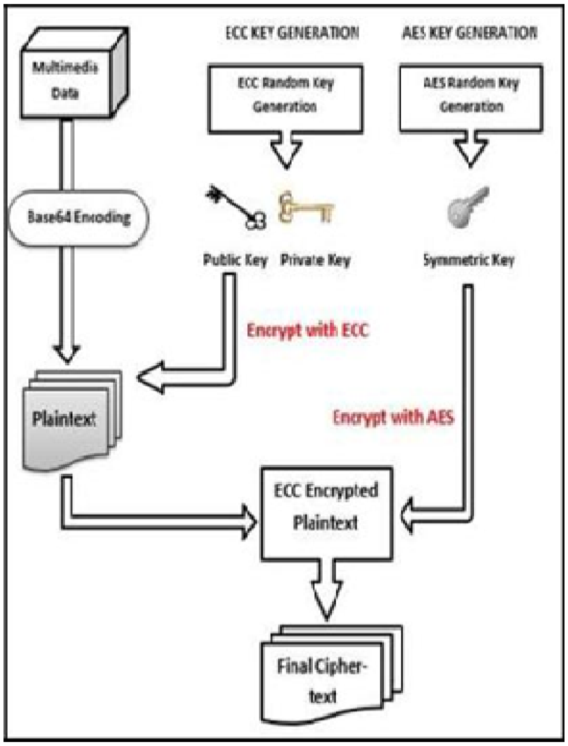


Figure 1. Encryption Process in Hybrid Cryptography

The Overall encryption process can be separated as takes after:

- Base64 Encoding
- Key Generation
- Encryption with ECC
- Encryption with AES

The Encryption stage starts with scrambling the plaintext with the ECC open key created haphazardly. In this examination work a key of size 160 bits is utilized as an open key.

This key is created utilizing Flexi-center supplier's Brainpool160P [8] cryptographic library. The comparing Ciphertext is again subjected to an AES encryption with 80/128 piece keys. The keys are created haphazardly at the earliest reference point independent of the encryption procedure being serial. The key era stage devours the most extreme measure of time. Here the AES strategy utilized as a part of the half and half calculation utilizes 128 piece keys rather than 192 and ECC utilizes 160 piece keys rather than 384 piece keys which intensely enhances the general time productivity of the whole procedure. The general unscrambling procedure is as demonstrated as follows:

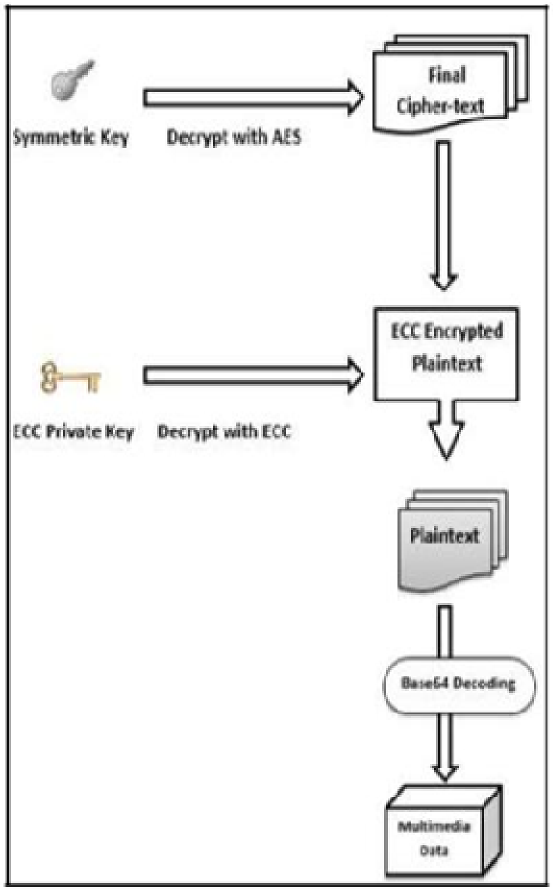


Figure 2. Decryption Process in Hybrid Cryptography

The Overall unscrambling procedure can be separated as takes after:

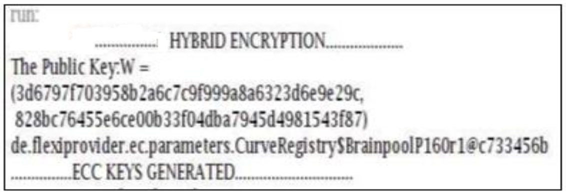
- Decryption with AES
- Decryption with ECC
- Base64 Decoding

The unscrambling procedure is precisely inverse of that of the encryption procedure and takes after a switch arrange. the keys for which were at that point produced before the encryption procedure ,Unscrambling by AES taken after by ECC. After effective unscrambling the Base64 decoded arrangement is acquired which ought to coordinate with the Base64 encoded design. In the event that there's no blunder actuated, then a relating mistake free sight and sound document is created.

IV. IMPLEMENTATION

The usage is completed in the Java runtime condition utilizing the cryptographic libraries given by FlexiCore suppliers. The ECC keys are given by FlexiCore's BrainPool160P library.

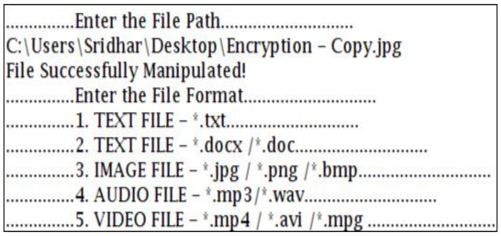
The AES keys and ECC keys are produced utilizing the KeyProviders keeping up the limitations of the key details. The Implementation depictions are as given beneath:



```
run:
              ................ HYBRID ENCRYPTION...................
The Public Key:W =
(3d6797f703958b2a6c7c9f999a8a6323d6e9e29c,
 828bc76455e6ce00b33f04dba7945d4981543f87)
de.flexiprovider.ec.parameters.CurveRegistry$BrainpoolP160r1@c733456b
...............ECC KEYS GENERATED.............................
```

Figure 3. ECC Key Generation

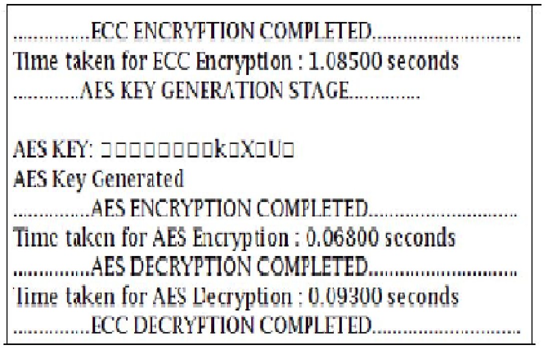
The execution starts with creating the keys required for the encryption procedure. As ECC stage starts preceding AES, the comparing ECC open key is created as appeared in Figure 3. The following stage starts with perusing the mixed media source document from the nearby File framework as appeared in Figure 4 beneath.



```
...............Enter the File Path.............................
C:\Users\Sridhar\Desktop\Encryption – Copy.jpg
File Successfully Manipulated!
...............Enter the File Format............................
...............1. TEXT FILE – *.txt............................
...............2. TEXT FILE – *.docx /*.doc............................
...............3. IMAGE FILE – *.jpg / *.png /*.bmp............................
...............4. AUDIO FILE – *.mp3/*.wav............................
...............5. VIDEO FILE – *.mp4 / *.avi /*.mpg ............................
```

Figure 4. File Processing Phase

In the wake of entering the source record organize vis txt, doc, docx, jpg, png, bmp, mp3, wav, mp4, avi, mpg and so forth the document is brought from the registry and controlled utilizing the ECC open key to create an outcome record which is then scrambled utilizing the AES key to yield the Final Ciphertext File. The Decryption stage starts with the Final Ciphertext record as the information, which is then subjected to an AES Decryption utilizing a similar key to yield a middle of the road document which is again subjected to a last decoding utilizing the ECC Private key as appeared in Figure 5.

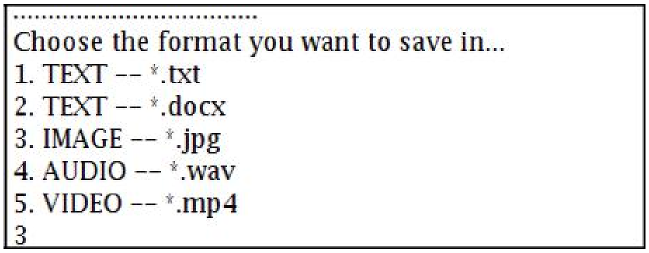


```
...............ECC ENCRYPTION COMPLETED............................
Time taken for ECC Encryption : 1.08500 seconds
.............AES KEY GENERATION STAGE.............

AES KEY: □□□□□□□□□k□X□U□
AES Key Generated
...............AES ENCRYPTION COMPLETED............................
Time taken for AES Encryption : 0.06800 seconds
...............AES DECRYPTION COMPLETED............................
Time taken for AES Decryption : 0.09300 seconds
...............ECC DECRYPTION COMPLETED............................
```

Figure 5. Encryption/Decryption Phase

The Final step is concerned with converting the ECC decrypted file back to the original source format file by Base64Decoding as shown in Fig 6 below.



```
...................................
Choose the format you want to save in...
1. TEXT -- *.txt
2. TEXT -- *.docx
3. IMAGE -- *.jpg
4. AUDIO -- *.wav
5. VIDEO -- *.mp4
3
```

Figure 6. Base64 Decoding to get the Original File

V. RESULTS AND CONCLUSION

The correlations are done between the current symmetric and uneven calculations. Similar informational collections are utilized as contributions for the correlation reason.

Table 2. Data Set used for Text Encryption

S.No	Format	Size(in Kb)
1	.txt	118
2	.docx	153
3	.docx	196
4	.doc	312
5	.txt	868

Txt Files

The informational indexes utilized for the execution procedure is according to Table 2. The nearest contender to the half and half (proposed) strategy regarding symmetric key encryption methods is AES which makes utilization of 128-256 piece keys relying on the quantity of rounds. The nearest rival as far as time is ECC which makes utilization of least 160 piece keys.As specified before the keys are suggested by the NIST. The examinations are finished with a 192 piece AES figure and comparing a 384 piece ECC. RSA utilizes 7680 piece keys to play out the encryption settling on it the slightest basic decision. The Hybrid strategy makes utilization of the slightest conceivable quantities of keys to give similar outcomes rapidly. It makes utilization of 128 piece AES and 160 piece ECC making it a sum of 288 keys to play out a similar errand which takes around 7680 piece keys by RSA. This settles on it a potential decision of encryption. The table underneath gives a relative synopsis of the different techniques utilized.

Table 3. Comparison of Existing and Proposed Method [9]

Size	**Time (In Sec)**				
(In Kb)	**AES**	**DES**	**RSA**	**ECC**	**HYBRID**
118	1.7	3.2	10	1.202	1.135
153	1.6	3	7.3	1.042	0.808
196	1.7	2	8.5	1.235	1.03
312	1.8	3	7.8	1.243	0.917
868	2	4	8.2	1.162	0.937
Average Time	**1.76**	**3.04**	**8.36**	**1.1768**	**0.9654**
Average Size	**329.4**				
Throughput	**187.16**	**108.36**	**39.41**	**279.92**	**341.21**

Img Files

The accompanying tables highlights the correlation between the current and the half breed technique.

Table 4. Execution time comparisons of image encryption algorithms

Size	**[10]**		**Hybrid Method**	
	Encryption (in sec)	**Decryption (in sec)**	**Encryption (in sec)**	**Decryption (in sec)**
256 by 256	0.29	0.30	0.75	0.16
512 By 512	0.79	0.60	0.87	0.29
1024 By 1024	2.47	1.58	0.88	0.50

We can see from Table 4 that the encryption time of the current strategy is marginally lower than the cross breed strategy yet it likewise should be seen that as the determination of the picture builds, a similar strategy sets aside significantly greater opportunity to execute the encryption procedure when contrasted with the mixture system so the previous technique will neglect to give better effectiveness if the picture quality is better, while the proposed method gives an adjusted execution time towards pictures of various resolutions. A striking distinction is found in the decoding times. The half breed strategy gives a considerably speedier outcome when contrasted with the current procedure which settles on it a superior decision.

Audio Files

The outcomes acquired in the wake of applying the half and half calculation to sound documents are as per the following:

Table 5. Audio Files Encryption

Input File Size	Encrypted File Size	Encryption Time	Decryption Time
1.29 Mb	4.27 Mb	1.091 Sec	0.799 Sec

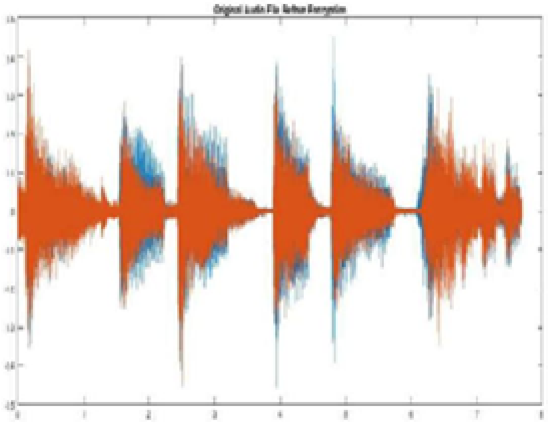


Figure 7. Audio File Before Encryption

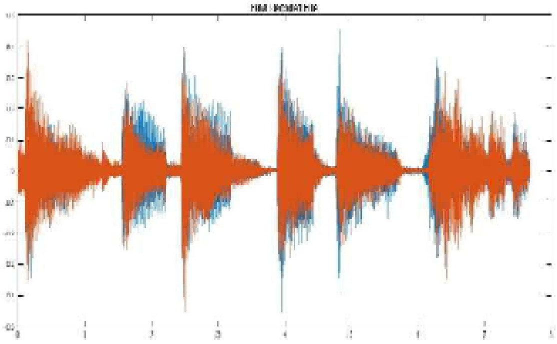


Figure 7. Audio File After Encryption

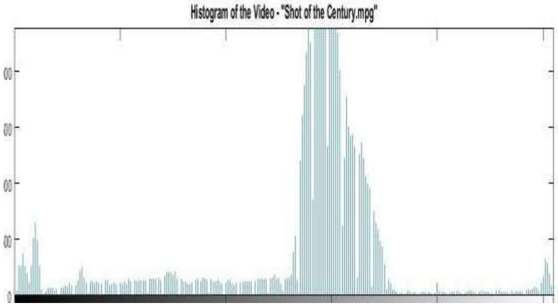
The histogram plots are created utilizing MATLAB R2015a Professional License release. The Final_Encrypted_File.mp3 record is gotten after the encryption procedure. This document experiences an unscrambling procedure to at long last yield the decoded or unscrambled adaptation of the source record. As obvious, the histograms of the sound document previously, then after the fact the encryption and unscrambling procedure are precisely indistinguishable and no misfortune is experienced amid the procedure.

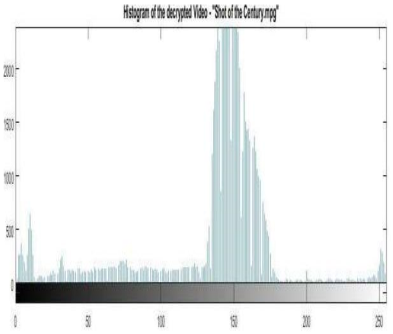
Video Files

The outcomes gotten subsequent to applying the mixture calculation to video records are as per the following:

Table 6. Video Files Encryption

Input File Size	Encrypted File Size	Encryption Time	Decryption Time
820 Kb	2708 Kb	0.805 Sec	0.714 Sec





VI. DISCUSSIONS AND CONCLUSION

The use of the talked about effective cross breed encryption strategy to the different large number of record configurations, for example, content, sound, video and pictures brought about a yield with 100 percent precision with no loss of data. To finish up, one might say that the present usage has been tried on different sight and sound records and the outcomes acquired so far are extremely persuading a result of the speed increases over the current systems. The present content usage is 1.8 times speedier than AES, 3.15 times quicker than DES, 8.66 times speedier than RSA and 1.21 times quicker than ECC. Additionally a 1024 by 1024 determination picture encryption brought about a speed pick up of 2.8 times over its closest rival. Video and Audio encryption was likewise done utilizing the novel calculation as specified in the past areas. The general procedure decreases the overhead of profoundly complex picture and video handling calculations yet getting the coveted outcomes with no loss of imperative data.

VII. FUTURE SCOPE

The present execution considers an independent framework where the Client and Server live on a similar system. A similar framework could be utilized as a part without bounds to give an encryption of information over the web by sending the encoded records and scrambled keys through messages, by sending the keys through QR Codes or installed in instant messages as OTP's. Numerous usage are conceivable in view of the idea given in this examination article.

REFERENCES

[1] Hafid Mammass and Fattehallah Ghadi, “Implementation of Smartcard Personalization Software,” International Journal of Future Generation Communication and Networking 2012; vol 5(4), p.39-54

[2] F. Amounas and E.H. El Kinani, “A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin ½ Matrice,”International Journal of Information & Network Security (IJINS) 2013; vol 2(3),p. 190-196

[3] Md.Zaheer Abbas, Dr.JVR Murthy, Authenticated And Policy - Compliant Source Routing. International Journal of Engineering Research and Applications (IJERA) 2012; vol 2(3),p.1347-1352.

[4] Sridhar C. Iyer, R.R. Sedamkar, Shiwani Gupta, “A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach,” 7th International Conference on Communication, Computing and Virtualization-2016 (ICCCV-2016), Procedia Computer Science; Vol 79, p.293-298, ISSN:1877-0509.

[5] The Base16, Base32, and Base64 Data Encodings. IETF. October 2006. RFC 4648. Retrieved March 18, 2010.

[6] www.csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf; (1999).

[7] NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General, original version 2005, Table 4.

[8] www.ecc-brainpool.org/download/Domain-parameters.pdf; (2005)

[9] B. Padmavathi, S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique," International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064; Volume 2 Issue 4, April 2013;p.170-174

[10] L.D.Singh and K.M.Singh, "Image Encryption using Elliptic Curve Cryptography," Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015),Procedia Computer Science 54 (2015);p.472 – 481.

[11] Daemen, Joan, Rijmen, Vincent, "AES Proposal: Rijndael," National Institute of Standards and Technology 2003; p. 1. Retrieved 21 February 2013.

[12] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" Communications of the ACM 1977; p. 120-126

[13] Christof Paar, Jan Pelzl, "Elliptic Curve Cryptosystems",Chapter 9 of "Understanding Cryptography, A Textbook for Students and Practitioners". Springer, 2009.

[14] Luciano, Dennis, Gordon Prichett ,"Cryptology: From Caesar Ciphers to Public-Key Cryptosystems". The College Mathematics Journal 18; p.2–17.doi:10.2307/2686311

[15] Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," International Journal of Emerging Technology and Advanced Engineering Dec 2011; vol 1(2); p.6-12

[16] S.M.Celestin ,V.K.Muneeswaran, "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography," IEEE International Conference on Advanced Computing Dec 2009; p. 82-85.