A

Thesis Report

On

Efficient Key Management for Data Security using AES

Submitted towards the partial fulfillment of requirement for the award of degree of

Master of Engineering

In

Electronics and Communication

Submitted by:

NITISH KANSAL

Roll No: 801361018

Under the Guidance of:

Dr. Ajay Kakkar

Assistant Professor

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

(Established under the section 3 of UGC Act, 1956)

PATIALA – 147004 (PUNJAB)

DECLARATION

I hereby declare that the work which is being entitled **"Efficient Key Management for Data Security using AES "** in fulfillment of the requirements for the award of degree of Masters of Engineering in Electronics and Communication Engineering submitted at Electronics and Communication Engineering Department of Thapar University Patiala, is an authentic record of my own work carried out under the guidance of **Dr. Ajay Kakkar (Assistant Professor),** Electronics and Communication Engineering Department and refers others research's work which are duly listed in reference section.

The matter presented in this dissertation has not been submitted in any other University/ Institute for the award of degree.

Date: 15/7/15

Nitish Kansal

Roll No: 801361018

This is to certify that the above statement made by the student is correct to the best of my knowledge and belief.

Date: 15/7/15

Dr. Ajay Kakkar

Assistant Professor, ECED

Thapar University

Countersigned By:

Dr. Sanjay Sharma

Head of Department

ECED, Thapar University

Dr. S.S. Bhatia

Dean of Academic Affairs

Thapar University

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to **Dr.Ajay Kakkar**, **Assistant Professor,** Electronics and Communication Engineering Department, Thapar University Patiala for his patient guidance and support throughout this report. I am truly very fortunate to have the opportunity to work with him. I found this guidance to be extremely valuable. I am also thankful to our Head of Department, **Prof. Dr. Sanjay Sharma** and P.G. Coordinator, **Dr. Amit Kumar Kohli**. I would like to thank the entire faculty and staff of Electronics and Communication Engineering Department and then friends who devoted their valuable time and help me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work.

Lastly, I would like to thanks my parents for their years of unyielding love and encourage they have always wanted the best for me and I admire their determination and sacrifice.

Nitish Kansal
ME (ECE)
80136108

TABLE OF CONTENTS

ABSTRACT

Secured and timely transmission of data is always an important aspect for an organization. In the encryption process the failure rate of keys and processing time are directly related with the security of cryptographic model. The use of strong encryption algorithms almost make it impossible for a hacker to get access of node. It helps to ensure the privacy of a user from others. Secured and timely transmission of data is always an important aspect for an organization. Keeping in view the importance of keys for secure data transmission, this work incorporates the use of efficient key management in AES. This work is focused on the use of key in an efficient manner to achieve more data security. Various techniques employed for the data security with their merits and demerits have been critically analyzed. Literature survey has been carried out by considering key papers related with data security and encryption algorithms. From these papers few observations have also been drawn, which are used to formulate the problem. Finally objectives have been drawn in which key has been efficiently used. Simulation results have been achieved using MATLAB, encryption time has been reduced which makes the cryptographic model more secured in comparison to AES. Finally, comparison of the proposed scheme has been done with AES in terms of encryption and decryption time.

LIST OF ABBREVIATIONS

DES	Data Encryption Standard
IBM	International Business Machines
TDES	Triple Data Encryption Standard
IDEA	International Data Encryption Algorithm
RSA	Ron Rivest, Adi Shamir and Len Adelman
DSA	Digital Signature Algorithm
MIT	Massachusetts Institute of Technology
PGP	Pretty Good Privacy
PKI	Public Key Infra Structure
AES	Advance Encryption Standard
ISO	International Organization for Standardization
ANSI	American National Standards Institutes
IEEE	Institute of Electrical and Electronics Engineers
GPS	Global Positioning System
WSN	Wireless Sensor Network
CRC	Cyclic Redundancy Check
SEU	Single Even Upsets
FRR	False rejection ratio
FAR	False Acceptance Rate
APE	Average Pixel Expansion
GDC	Generalized Digital Certificate
HOFT	Homomorphic One-Way Function Tree
CED	Concurrent Error Detection
GNSS	Global Navigation Satellite Space
PKC	Public Key Cryptography
IBC	Identity Based Cryptosystem
ANN	Artificial Neural Network
CPA	Chosen Plaintext Attacks
CCA	Chosen Ciphertext Attacks

IBSDDS	Identity-Based Secured Distributed Data Storage
FPGA	Field Programmable Graphic Array

LIST OF FIGURES

LIST OF TABLES

LIST OF PUBLICATIONS

1. N. Kansal, A. Kakkar, "Secured data using RSA", *Proceedings of National conference on Role of Information Technology in Management and Engineering*, pp. 54-57, March, 2015.

2. G. Puri, N. Kansal, A. Kakkar, "Key Generation in Encryption Algorithm for Data Security," *4th International Conference on Eco-friendly Computing and Communication Systems*, Sponsored by Elsevier, 7-8th December, 2015, NIT, Kurukshetra, Haryana, India. (Communicated)

Chapter 1: Introduction

In modern world, there is a lot of problems arises with the security of documents, files and important data. Hence, there is a need to have a procedure to protect the documents and which makes secure the documents from unauthorized access. Data security is an essential component of an organization [2]. There are various procedures which are used to provide security and privacy to documents. The distinct procedure of cryptography is in figure1.1.

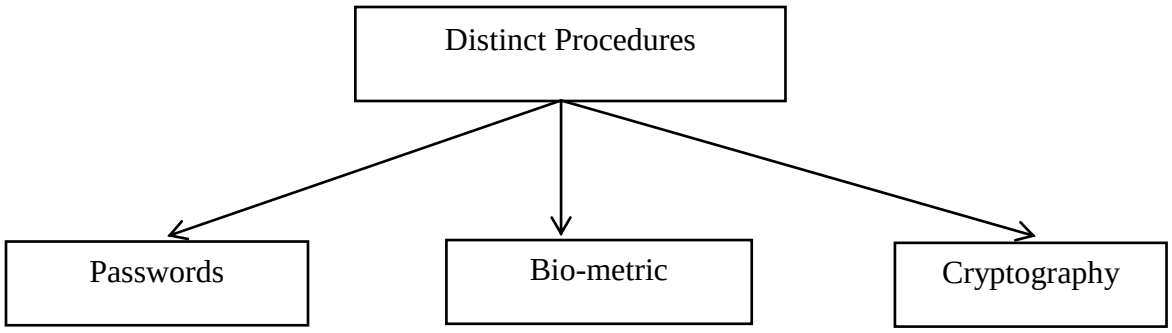

Figure 1.1 Distinct procedures of cryptography

Passwords have low entropy and thus not that so much advantageous for data security. Biometrics produces some harmful effects on the human beings and it is too costly. But all the above problems can be overcome by cryptography. It is the best solution for data security. It is all about designing and resolving code that overcomes the effect of an enemy and which is related to information security in many ways [2]. It is an art of secret writing. Modernized cryptography is heavily based on mathematical theory and computer science method. Cryptographic algorithms are constructing in such a way that it become difficult to crack in method by any attacker. It is theoretically possible to crack such a scheme but it is futile to do so by any known proficient means. Functions of cryptography include ATM cards and computer passwords. The course of encryption and decryption is called cryptology and cryptography is the study of them. Encryption is the procedure of designing a cipher-text from a plain-text and decryption is the converse procedure of encryption, where cipher-text is changed into plain-text. The basic cryptography model is shown in Figure 1.2.

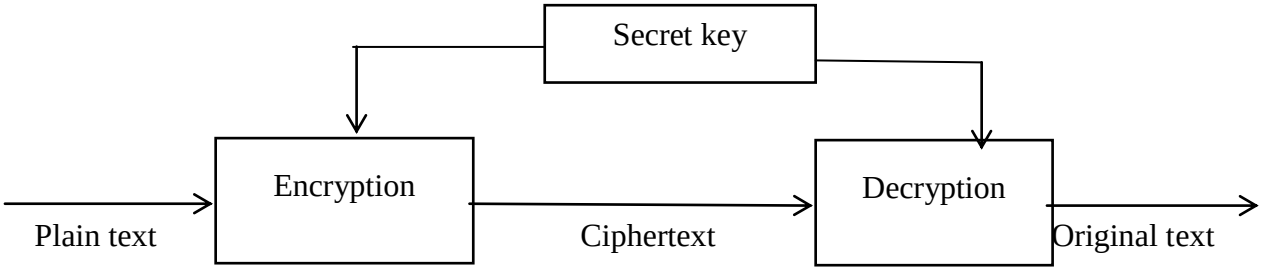

Figure 1.2 Basic cryptography model

1.1 Basic Terms

There are few basic terms related with cryptography and are explained as follows:

- Plain text is the original text before it is encrypted. Cipher-text is the encrypted text, it is a text obtained after encoding the data with the help of a key. The key is a word or value which is used to encrypt the plain text or decrypt the cipher text [2]. The method of converting the data into coded form with the help of key is called encryption. It is a method to lock information, so that, intruders cannot access it without a key. Decryption is the method of transforming the encoded data to the original form. A crypto analyst is a person who is an expert in analyzing and breaking codes. The main goals of cryptography are shown in Figure1.3.

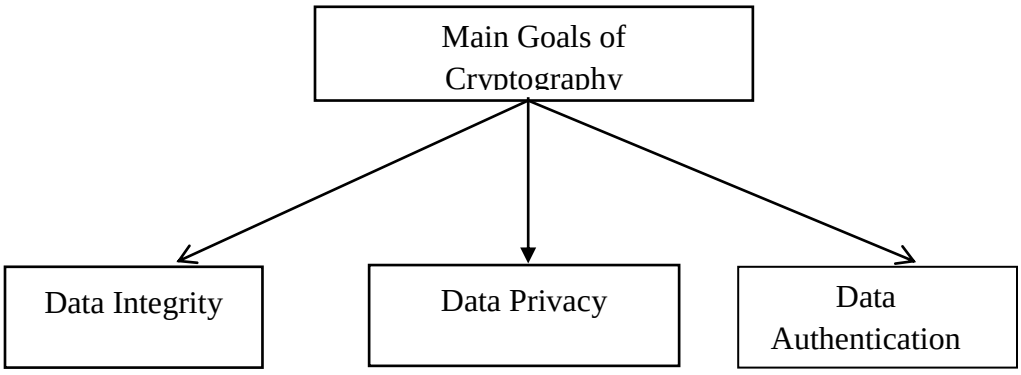

Figure1.3 Main goals of cryptography

- **Data Integrity**

It refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data. It is opposite of data corruption, which is a form of data loss [6].

- **Data Privacy or Confidentiality**

Confidentiality is most generally forward objective. The content of information is covered by ciphering it. The operator encrypts the content using a secret key. The acceptor decrypts the content using a cryptographic key that may or may not be the like as the one used by the operator [6].

- **Authentication**

A system can confirm their integrity to other who does not have particular awareness of their integrity. Kerberos is a general cryptographic verification scheme [6].

1.2 Types of cryptography

The types of cryptography are shown in Figure1.4.

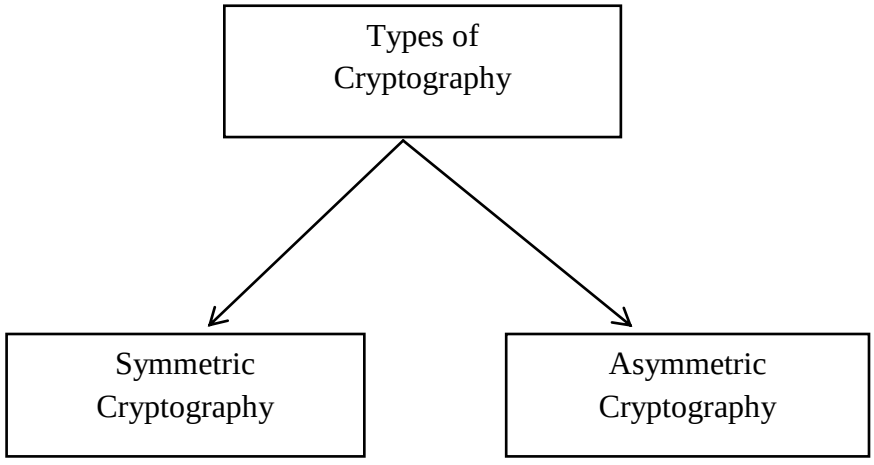

Figure 1.4 Types of cryptography

1.2.1 Symmetric Cryptography

Symmetric key cryptography refers to encryption methods in which both the operator and acceptor dividend the same key. It consists of two parts; a) The algorithm b) The Key. Private key is a method or encryption process where one key is used for both encryption and decryption. This is different from public key encryption where a distinct key is used for encryption and decryption [4]. Private key encryption process is fast and efficient, making it useful for large data transmissions. The types of symmetric cryptography are shown in figure1.5.

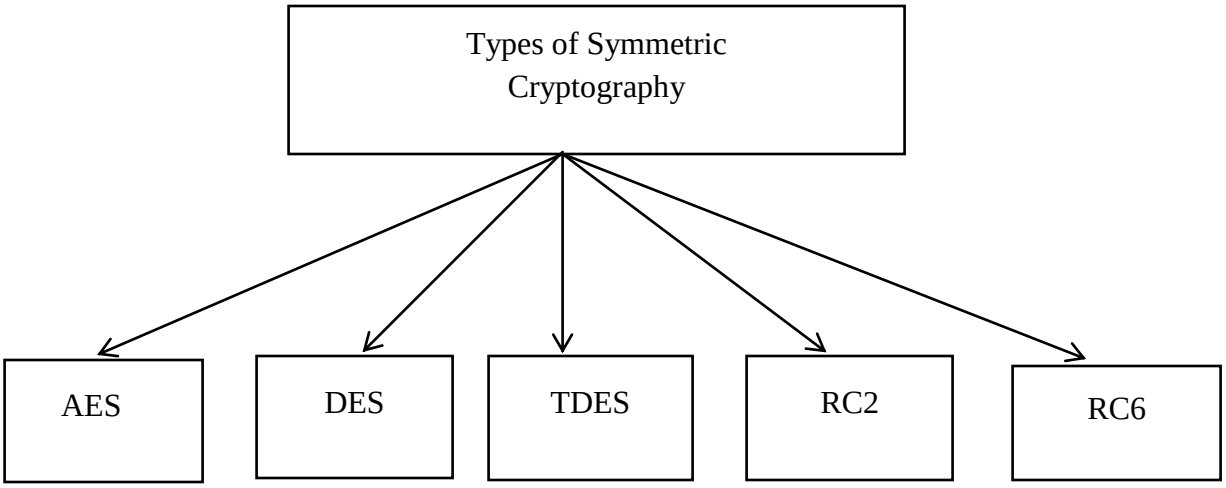

Figure 1.5 Types of symmetric Cryptography

- **Data Encryption Standard**

It is a symmetric algorithm with key size of 56 bits and block size of 64 bits [4]. It divides 56 bits block size into two 28 bits halves, each half of the key is shifted by one or two bits depending on the round. It has 8 bit parity which has to be detached from the key by subjecting to the key permutation.

- **Triple Data Encryption Standard**

It is a symmetric algorithm established in 1998. Triple DES has to undergo 3 iterations for effectively encrypting data with 168 bits key size. The process has three subparts where data is first encrypted with first 56 bits then decrypted with next 56 bits and finally, again encrypted with the 56 bits. Hence, TDES is an improved symmetric algorithm which provides secure information [4].

- **Advanced Encryption Standard**

It is a symmetric algorithm presented in 2001. It has 3 distinct key size which are as 128, 192, 256 bits which is 16, 24 and 32 bytes A number of AES criterion depend on its key size. It encrypts the data blocks of 128 bits in 10, 12 and 14 rounds depending on key size [4]. It has got encryption and decryption speed faster than DES and RSA Power consumption is less than RSA.

- **RC2**

In cryptography RC2 (is known as ARC2) a symmetric key block secret created by Ron Rivest 1987. RC2 is a 64 bit block cipher with a fluctuating size key. Its 18 rounds are form as a source heavy unstable Feistel network, with 16 rounds of one type of blend interrupt by two rounds of another type crush [4].

1.2.2 Public Key (Asymmetric) Cryptography

Public key cryptography is the encryption methods in which both the operator and acceptor use the different key. The basic structure of public key cryptography is shown in Figure1.6.

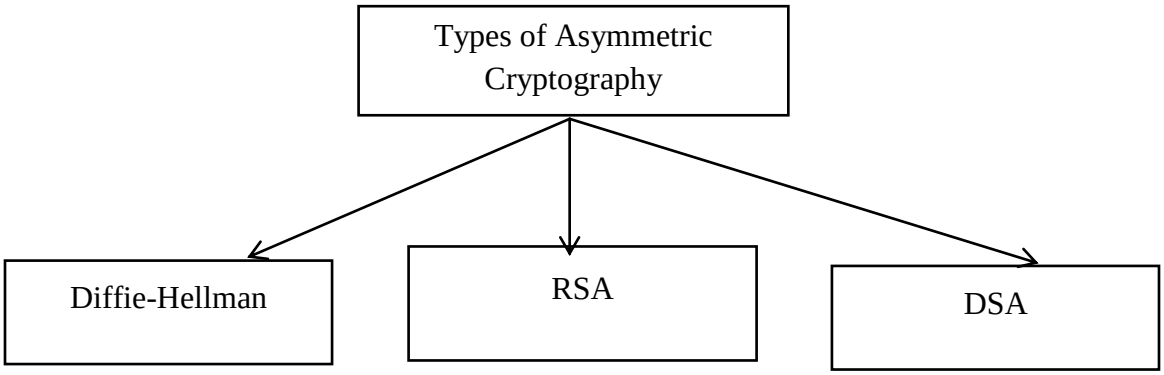

Figure 1.6 Asymmetric Cryptography

- **Diffie-Hellman**

Diffie–Hellman key exchange is a definite method of swapping cryptographic keys proposed in 1976. It has two parties that have no previous knowledge of each other to mutually create a common secret key over an anxious communications channel. This key is used to encrypt consequential communications using a symmetric key cipher [3].

- **RSA**

It was first announced in 1978 by Ronald Rivest, Adi Shamir and Leonard Adleman RSA algorithm uses the asymmetric key for providing the secure communication. It uses of public and private key for the encryption and decryption process. Stimulation speed in case of RSA is faster, as it uses equation editor to write equations. The security of RSA depends upon the product of two prime numbers. It requires keys of at least 1024 bits for secure communication. Block size should be minimum of 512 bits. Ciphering and deciphering key used are distinct from DES and AES [3].

- **Digital Signature Algorithm (DSA)**

A digital signature algorithm is a public key cryptographic algorithm designed for endorsing digital content. Content is signed by a secret key to produce a signature, and then this is verified against the content by a public key. Any party can verify the signatures but only one party with the secret key can sign the contents. A valid digital signature gives recipient logic to admit that the content was designed by a known operator [3].

1.3 Types of Attacks

Different types of attacks are shown in figure1.7

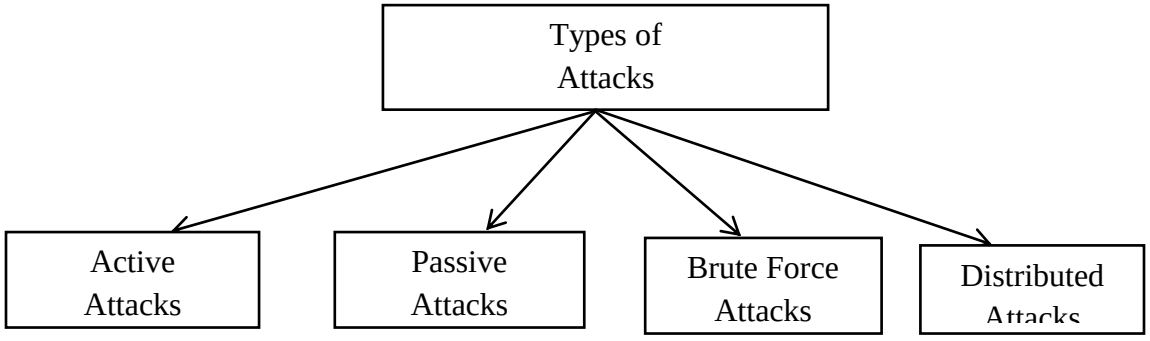

Figure 1.7 Types of attack

- **Brute Force Attack**

With a brute force attack, the attacker hardly achieves every possible key and employs it to the cipher text [2]. Any resulting plain-text that makes feel attempts a candidate for a certain key.

- **Passive Attack**

A passive attack auditor unencrypted service and attention for clear-text passwords and conscious information that can be used in other types of attacks Passive attacks contains service inquiry, monitoring of exposed communications, decrypting ailing encrypted service and grab certification data like passwords.

- **Active Attack**

In an active attack, the attacker effort to crack into assures systems. This can be done through stealth, viruses, worms, or Trojan horses [2]. Active attacks are seated against a chain determination. Active attacks result in the exposure of data files, or modification of data

- **Distributed Attack**

Distribution attacks focus on the nasty adjustment of hardware or software at the laboratory or in distribution event. These attacks offer nasty code such as a back door to a product to gain illegal approach to information or to a scheme function at a next date [2].

1.4 Organization of the thesis

The outline of the thesis is as follows:

Chapter1 discuss the introduction of cryptography and its types. A brief introduction about the security of the data has also been included. Chapter 2 includes the literature survey; it involves the work done by the various researchers in the field of cryptography. From the literature survey, few observations have also been drawn and the objectives are developed from these. Chapter 3 includes the analysis of the AES algorithm. Detailed description of AES is explained, it also includes the advantage, disadvantage and key related issues. Chapter 4 includes the detailed analysis of proposed work. Generation of 64 bit key has been used for the encryption and decryption process. Chapter 5 shows the results and discussion of the proposed work. Comparison of the proposed scheme has been done with AES in terms of encryption and decryption time. Chapter 6 details the conclusion of the proposed work and its future scope has been discussed.

Chapter 2: Literature Survey

This chapter involves the work done by the various researchers in the field of cryptographic algorithm for data security. From the literature survey various observations have been drawn and listed at the end of this chapter. From the observations various objectives have also been derived.

2.1 Literature survey

Daniyal M. Alghazzawi [1] *et al.* studied the advancement of cryptanalysis research on AES. It aimed at identifying specific vulnerabilities and threats against the communication application in the sensitive domain. The threat model of the sensitive presents quite highly equipped opponent and lot more critical conditions faced against the opponent in comparison to any commercial domain. Limitation of this research is that there is a need to work on the domain, so that it cannot access by unauthorized parties.

M. O. Neill [5] *et al.* worked on a low-cost GPS digital signature architecture, which combines an optimized GPS algorithm design. They also optimized SHA-1 design for low cost RFID tags. In the development of emerging mobile and ubiquitous computing applications RFID tags were integral part. This architecture could be used for device authentication to avert tag cloning and to provide data authentication to prevent transmission counterfeit. The design offers significant enhancements over previous work on RFID digital signature architectures in terms of area and power. The hardware structure of this scheme was very complex. So, it is not easy to implement and system cost was also very high.

Salasiah Sulaiman [7] *et al.* produced a new key schedule algorithm, an enhancement from the Rijndael key scheduling, which follows the standard of secure cipher by Shannon, where the new key schedule must satisfy the bit confusion and diffusion properties for security purpose. After both keys from schedule algorithms were analyzed, the results proved that the proposed satisfies the requirement that set by Shannon [61] in achieving both the properties**.** Limitation of this algorithm is that it requires large memory size for data, thus takes more time to compute the output as compare to other algorithms.

Yanchao Zhang [8] *et al.* operated on location based compromise-tolerant security mechanisms for WSN. They worked on the idea of location based keys by tying private keys of individual nodes to both their IDs and geographic locations. They also developed LBK-based neighborhood authentication scheme to localize the impact of compromised nodes to their vicinity. The conclusion was that they presented a comprehensive set of location based compromise tolerant security mechanisms for WSNs. Limitation of this WSN is that protocol are not adaptable by future techniques, therefore compatibility of protocol still a issue.

Monjur Alam [9] *et al.* presented a reconfigurable architecture of the AES (AES-Rijndael) cryptosystem. The suggested reconfigurable architecture was capable of handling all possible combinations of standard bit lengths (128,192,256) of data and key. Less hardware complexity is ensured by the fully rolled inner-pipelined architecture ensures. Main limitation of this architecture is that system gets delayed output.

Yukio Mitsuyama [10] *et al.* worked on a new cipher mode, particularly for the high performance implementation of AES and other next generation 128-bit block cipher algorithms. In comparison with the conventional modes, the burst mode attains a considerable increase in the throughput by employing a novel stream cipher mechanism it encrypt, 64 bit plain-text blocks through 16 invocations of the block cipher encryption operation. Limitation of this algorithm is that because of burst mode if there is an error in few bits, it is difficult to find the error; therefore, probability of removing whole blocks of data.

Chih Hsu Yen [11] *et al.* worked on error-detection schemes. These schemes are based on the $(n, n+1)$ cyclic redundancy check (CRC) over GF (2^8). Symmetry also benefits the implementation of this scheme to achieve that the encryption process and the decryption process caused share the same error detection hardware. These schemes were also suitable for encryption and decryption only. Error detection for the key schedule in AES was also proposed and based on the derived results in the data procedure of AES. Since, computation

of parity bits through polynomial division seems complicated and relationship between bits and polynomial provides the mathematical limitation also.

Omer K. Jasim Mohammad [12] *et al.* worked on the development on the generation of dynamic quantum S-Box (DQS-Boxes) based quantum cipher key, instead of the ordinary used static S-Boxes. Moreover, they also introduced the integration between the developed AES based DQS-Boxes, and the specific selected secret key generated from the QKD using two distinct modes (online and off-line). Limitation of this generation is that algebraic degree is low as compare to others and in this approach linearity of component is also high but for good S-Box there should be non linearity in component functions.

Francesco Buccafurri [13] *et al.* worked to find a cheap practical procedure which was feasible and efficient to mitigate the vulnerability of digital signature because that vulnerability allows the attacker to sign documents and to exploit them without any intention of signature's owner. The other nice feature of their approach was that it relies on the usage of Java cards instead of firmware only programmable smart cards. Digital signature schemes used were not completely secured.

Spyros T. Halkidis [14] *et al.* worked on architectural risk analysis of software systems based on security patterns. They performed risk analysis of software systems based on the security patterns that they contain. The first step was to determine to what extent specific security patterns shield from known attacks. This information was fed to a mathematical model based on the fuzzy-set theory and fuzzy fault trees in order to compute the risk for each category of attacks. It gives same importance to all factors that are to be combined and fuzzy rules included in this pattern there were not robust and arbitrary and class assignments were difficult to choose for best results.

Roohi Banu [15] *et al.* addressed the encryption of satellite imaging data using five AES modes–ECB, CBC, CFB, OFB and CTR. A detailed analysis of the effect of Single Even Upsets (SEUs) on imaging data during on-board encryption using distinct modes of AES was carried out. The impact of faults in the data occurring during transmission to ground due

to noisy channels was also discussed and compared for all the five modes of AES. It takes more time to encrypt the image. The abrupt change in the upward and downward link speeds may affect the performance of the system.

Xiaojiang Du [16] *et al.* worked on routing driven Elliptic Curve Cryptography key management scheme for heterogeneous sensor networks They adopt heterogeneous sensor network model for better performance and security and provides a routing driven key management scheme and establishes a shared keys for neighbor sensors which communicate with each other. The performance evaluation and security analysis show that this key management scheme provides better security, storage space and energy consumption than other key management schemes. It uses heterogeneous network, it suffers from system complexity in protocols and all protocols were not routable.

Julita A. [17] *et al.* worked on online signature verification which is a process of verifying the writer's identity using signature verification system. An individual could sign on the digitizing tablet using the special pen regardless of his signature size and position. The signature was characterized as pen-strokes consisting x-y coordinates and the data was stored in the signature database in the form of a .txt file. These characteristics uniquely identify, a person and could not be stolen. The tight security that this software has will indirectly contribute towards the increased False Rejection Rate (FRR) but manage to lower down the False Acceptance Rate (FAR) where forgery signatures could be hardly verified as genuine signatures, makes the system more costly.

Panagiota Lagou [18] *et al.* evaluated the provision of non-repudiation in electronic transactions. Using digital signatures and biometrics. Non repudiation was required in many existing applications such as e-commerce, e-banking, and e-governance its successful provision could lead to the development and enhancement of many more, such as digital contract signing and access to confidential documents. Signature verification can caused the problem when multiple signatures changed over time and are not always consistent.

Bibhudendra Acharya [19] *et al.* proposed an involutory, permuted and reiterative key matrix generation methods to overcome the weakness of the hill cipher system. Involutory matrix generation method solves the key matrix inversion problem. This meant that same machinery could be used both for encryption and decryption of messages no additional hardware would be needed to figure out inverses before decrypting permuted and reiterative key matrix generation. Limitation of this scheme is that since the dimension of involutory matrix is large and so its mathematical analysis becomes difficult so it is difficult to modify the system according to the application

Feng Liu [20] *et al.* proposed the step construction of VCS for general access structure which improves the pixel expansion and contrast properties compared with many of the known results They also reduce APE (average pixel expansion) to minimum. Disadvantage of this visual cryptography is that the contrast of reconstructed image was not maintained and also perfect alignment of transparency was not upto the mark.

Mao-Yin Wang [21] *et al.* worked on single and multi-core configurable AES architectures for flexible security. Each AES processor provides block cipher schemes with a novel on the fly key expansion design for the original AES algorithm and an extended AES algorithm. In this multi core architecture, the memory controller of each AES processor was designed for the maximum overlapping between data transfer and encryption, reducing interrupt handling load of the host processor. Authentication process was very weak and provides maximum 128 bit authentication tag whereas other available algorithms that allows 256 bit authentication tag.

Mao Yin Wang [22] *et al.* worked on a mesh structured scalable internet protocols security processor used for protects the data over the Internet. They developed a parallel mesh structured internet protocols security processor and execute the protocols for Internet security applications. They also developed several areas where efficient cryptographic internet protocols security processor embedded in mesh structured internet protocols security processor. Mesh structured internet protocols security processor was suitable for

transport mode. Disadvantage of this protocol is that if access point is weak, it becomes easy to get all the information that is stored on the server.

Aqeel Khalique [23] *et al.* worked on a password authenticated key agreement scheme based on ECC using smart cards. It is one of the best public key procedures for its small key size and high security. It is also suitable for secure access of smart cards due to the implementation on smart cards. Limitation of above system is that although it is an authenticated system but it is not a authorized system in the sense that by knowing the password one can easily get information.

Jing Liu [24] *et al.* worked on collusion-resistant multicast key distribution based on homomorphic one-way function trees. They instantiate the general notion of one-way function tree to obtain a new cryptographic construction named HOFT (homomorphic One-Way Function Tree). They propose further idea to focus on the provable security of OFT-based protocols (especially the HOFT protocol). HOFT do not provide verifiable computing because cipher-text much larger than plain text.

Yi Sheng Shiu [25] *et al.* worked on physical layer security in wireless network for security of information. Security methods on cryptographic procedures employed at the upper layers of a wireless network known as physical layer. Physical layer security procedures could be classified into five major categories theoretical secure capacity, power, code, channel and signal detection approaches. Non repudiation and redundancy in physical layer remain an issue.

Lein Harn [26] *et al.* worked on the concept of Generalized Digital Certificate (GDC) that could be used to provide user authentication and key agreement. A GDC has information about user's public information, such as the information of user's digital driver's license. However, the GDC does not contain any user's public key. Since the user does not have any private and public key pair, key management in using GDC is much simpler than using public-key digital certificate. Authorities need to consistently update their certificate to protect users from unauthorized parties.

Nadia M.G. AL-Saidi [27] *et al.* worked on a novel digital signature protocol based on the iterated function system attractor. The idea behind this method is based on selecting a known fractal set and then finding the attractor of the affine transformation functions. The attractor was then used in the encryption and decryption of a hash function to ensure the protection of the document from eavesdropping and integrity during the transmission. The novel scheme utilizes the inherent advantages of a fractal attractor in terms of smaller key size and lower computational overhead compared with its counterpart public cryptosystems, such as the DSA and RSA. Its generation and verification require, considerable amount of time so, speed of communication will reduce.

Jjude H. moore [28] *et al.* worked on sub-collection of keys, those with a palindrome sequence of round keys, which are the weak keys, and those with an anti-palindrome sequence of round keys, which are part of the semi-weak keys. The results presented were used to identify the weaknesses of these keys. If two parties want to communicate they must agree to use same private key and this may impossible depending upon the circumstances.

Amid Jamshidi Jam [29] *et al.* designed a dynamic S-Box which depends on rounds keys for encryption in AES-128. The parameters of the dynamic S-Box have features equivalent to those in the normal algorithm AES. Static S-Box allows attackers to discover weak issues while using dynamic S-Box approach, it makes difficult and more complex for attacker to do any offline study of an attack of one particular set of S-Boxes. Limitation of this generation was that linearity of component is high but for good S-Box there should be non linearity in component functions.

Abdul Hamid M. Ragab [30] *et al.* introduced a new architecture and implementation for the proposed block cipher, which was an extension for the well-known block ciphers RC5 and RC6. Several design parameters of the algorithm were investigated among which is word size, number of rounds, and length of secret key. It requires more memory since they work on large chunks of data.

Zhiguo Wan [31] *et al.* worked on a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes. Limitation of this computing technique is that it is inflexible.

Shiva Murthy G [32] *et al.* worked on a secured node disjoint multipath routing protocol for WSN. The data packets were transmitted in a secured manner by using the digital signature crypto system. It is compared with an ad hoc on-demand multipath distance vector routing protocol. It shows better results in terms of packet delivery fraction, energy consumption, and end-to-end delay compared to the ad hoc on-demand multipath distance vector routing. Implementation cost was very high.

Ajay Kakkar [33] *et al.* worked on a new approach for generating keys from the available data. The analysis of various times, such as encryption, decryption, key setup, processing, and key shifting times, was done. The model takes minimum time to replace the faulty keys with the fresh keys. The security also increases if the key size is increased and the key shifting time (δ) was reduced; the above combination may be adopted for secure transmission. This work can be extended if more number of S-Boxes (64 and 128) was used for the same task, and the key length would be reduced with nominal processing time.

Kun Ma [34] *et al.* worked on a novel Concurrent Error Detection (CED) scheme to counter fault-based attack against RSA by exploiting its multiplicative homomorphism property. In order to achieve high performance, the proposed CED procedure requires successive contents to share the key. The CED scheme includes strong resistance to fault attacks and small time overhead. It was not time efficient and has added quantization noise which affects the performance of the system.

Bevan M. Bass [35] *et al.* worked on parallel AES encryption engines for many core processors. The smallest design requires only six processors and the fastest design achieves a throughput of 4.375 cycles per byte, which was 2.21 Gbps when the processors was

running at a frequency of 1.2 Ghz. The design on the fine grained many core achieves energy efficiencies approximately 2.9-18.1 times higher than other software platforms, and performance per area on the order of 3.3-15.6 times higher. Limitation of this scheme is that hardware implementation of this was very complex.

Todd E. Humphreys [36] *et al.* worked on detection strategy for cryptographic Global Navigation Satellite System (GNSS) anti-spoofing. The strategy was applicable both to military Global Positioning System (GPS) and enhanced civil GNSS signals, whose trustworthiness was increasingly an issue of national security. The detection strategy takes the form of a hypothesis test that accounts for the statistical profile of a replay-type spoofing attack. The simple navigation content authentication would be an effective protection against spoofing for civil GNSS signals. Implementation of this was practically very difficult because it has very complex structure. Limitation of this scheme is that this system could be affected by outages caused by insufficient tracked satellites.

Koji Nuida [37] *et al.* proposed novel ideas and procedures for evaluation of in distinguish ability between random and pseudorandom cases in PRG-based randomness reduction of cryptographic schemes. They also propose a further idea for improving the effect of the PRG-based randomness reduction. Due to periodicity there, were potential problems of regularity appearing in samples.

Peng Xu [38] *et al.* worked on public-key encryption with fuzzy keyword search a provably secure scheme under keyword guessing attack. They proposed the new primitive of PEFKS to resist KGA and formalized the SS-CKA and the IK-NCK-KGA securities of PEFKS, followed with a universal transformation from anonymous IBE to PEFKS. The scheme uses the third party to certify the reliability of public keys so security decreases.

OBV Ramanaiah [39] *et al.* operated on heavy computations such as generating RSA keys which were difficult to generate on mobile devices because the mobile device possesses limited resources. The well-known Rijndael cryptographic algorithm was used to secure the

communication between the mobile devices or mobile device with any conventional server**.** Limitation of this scheme is to make large prime number is a difficult process.

Zahir Zainuddin [40] *et al.* worked on the e-learning concept, data input of plain text that can be changed. Application of e-learning concept was not enough, if only simulation and animation process was used without explanation about the calculation process. Therefore, it needs e-learning concept to ease the user. Limitation of this is without routine structure of traditional class security may get lost.

Erfaneh Noroozi [41] *et al.* worked on the analysis of the security systems and the emphasis is on digital signature, hashed content algorithm. The proposed algorithm introduced a novel procedure for producing small sized output of digital signature as a result. The scheme was potentially practical; signing and verifying signatures were reasonably fast, and both speed and time were also improved. This hashing algorithm uses only one hash value for a record.

SK Hafizul Islam [42] *et al.* worked on a provably secure certificate less digital signature scheme using elliptic curve cryptography. Since the certificate less public key cryptosystem removes the complex certificate management procedure and the private key escrow problem of traditional Public Key Cryptography (PKC) and Identity Based Cryptosystem (IBC). The scheme was more efficient than IBC and PKC based signatures. Limitation of above system is that although it is a authenticated system but it is not an authorized system in the sense that by knowing the password one can easily get information.

William Stallings [43] worked on three digital signature algorithms that have been approved by the national institute of standards and technology and which have also been standardized by a number of other organizations, including ISO, ANSI, and IEEE. Two additional digital signature algorithms were also discussed.

S. Rashidi [44] *et al.* worked on an effective method for online signature verification. It covers two problems; comparison of functional features from the viewpoint of consistency and discrimination between genuine and forgery signatures. This system perhaps can

perform better in the verification phase. Limitation of online signature is that can be forged easily.

Othman O Khalifa [45] *et al.* worked on an offline signature verification schemes which considered as a highly secured procedure to recognize the genuine person's identity. It addresses the offline signature verification procedure using Artificial Neural Network (ANN) approach. They also highlighted the comparison among various approaches and challenges to develop the verification systems. The main benefit of using offline systems was identifying the right person and provides secure services. This scheme has large temporal variation and high intra class variability.

Ashok K. Bhateja [46] *et al.* worked on a robust online signature based cryptosystem to hide the secret by binding it with invariant online signature templates. The invariant templates of the signature were derived from artificial neural network. The scheme was highly robust as it works well for all kinds of signatures and was independent of the number of zero crossing and high curvature points in the signature trajectory. The results obtained with this scheme have a false rejection rate of 17.78% and a false acceptance rate of 2.22% on test signature samples. Limitation of online signature is that it could be forged easily.

Xinyi Huang [47] *et al.* presented a secure generic multi-factor authentication protocol to speed up the whole authentication process. Comparison with other generic design of multifactor authentication this design has significant improvements in computation and communication. It requires high level programming which was main limitation.

Chun-I Fan [48] *et al.* worked on arbitrary-state attribute-based encryption with dynamic membership. It was unnecessary for anyone else to update her/his private key when enrollment, leaving, or attribute updating occurs. These advantages will make an ABE service more efficient and flexible for practical applications.

Xiaofeng Chen [49] *et al.* worked on new algorithms for secure outsourcing of modular exponentiations. They proposed two outsource-secure and efficient algorithms for modular

exponentiations and simultaneous modular exponentiations, which were the most basic and expensive operations in many discrete logarithm cryptosystems. They also proposed the idea for all outsourcing algorithms, there was only one-round communication between the client and the servers. For each instance of an outsourcing algorithm, the communication complexity was only a few kilobytes, so that, it would not downgrade the overall performance. Disadvantage is that conversion of cipher text is time consuming.

Joseph K. Liu [50] *et al.* worked on linkable ring signature with unconditional anonymity. They proposed that it was possible to have a linkable ring signature scheme with unconditional anonymity. The scheme could provide strong anonymity under one of the interpretations. They also proposed further idea to shorten the size of the signature. Limitation is that signature increases linearly with size of the input. Such schemes are impractical for real use cases for sufficiently large number of users.

Xinqiang Luo [51] *et al.* worked on the software implementations based on 4 lookup tables and the AES accelerator on the radio chips could reduce the computation time significantly, the large storage overhead of the 4 lookup tables and the additional energy of the accelerators were still heavy burdens. A fast AES implementation 1-T based on a 2*256 bytes lookup table was presented**.** Limitation is that in this higher level protocols are used which limit key usage.

Joseph Soryal [52] *et al.* presented a distributed solution to detect and isolate the attacker in order to minimize the impact of the DoS attacks on the network. Detection algorithm enhances the Disk Copy Fast (DCF) firmware to enable honest nodes to monitor each other's traffic and compare their observations against honest communication patterns derived from a two-dimensional Markov chain. A channel hopping scheme was then used on the physical layer (PHY) to evade the attacker. Limitation of this is conventional distributed solutions need adequate protection in order to accommodate exchange of messages.

Bassem Bakhache [53] *et al.* worked on a new robust and fast chaotic encryption algorithm RFCA. This consists of a chaotic cipher composed of two perturbed maps piecewise linear

chaotic map. This algorithm was, adequate for data encryption in Zig-Bee networks where robustness and real time were both essential. A comparison between algorithm and the AES-CTR, the simplified AES, and the estream finalist candidates, was presented with regard to speed and robustness. This was done using correlation coefficients, unified average changing intensity, number of pixels change rate, and test of randomness for the generated bit sequences. Limitation is that there is no mortality and there are major complications.

Hassan Noura [54] *et al.* worked on a new kind of security system based on a cipher and authentication algorithm called EDCA was presented to ensure the necessary security requirements with low computation complexity. Furthermore, the cipher was based on a dynamic binary diffusion layer. The contents of packets was divided into many blocks, which were mixed together to produce the cipher blocks. Additionally, EDCA was evaluated by comparing it with AES, which was considered reliable and robust in several standards of sensor networks. Limitation is that, because of block ciphers there is wider attack than stream ciphers and also makes them harder to design.

Walid Y. Zibideh [55] *et al.* proposed a new encryption algorithm that uses an optimized framework for the throughput and security. Use of computer simulations to analyze the effect of the algorithm on the throughput was carried out. Moreover, evaluating the security of the algorithm in terms of its strength to applicable, well-known attacks. The algorithm performs the use of the same optimization framework over the variable length. Limitation is that it has got high complexity.

Jinguang Han [56] *et al.* worked on Identity-Based Secure Distributed Data Storage Schemes. They proposed two new IBSDDS schemes in standard model, a) The first scheme was only secure against the Chosen Plain-text Attacks (CPA), b) The second scheme was secured against the chosen Cipher Text Attacks (CCA). It was the first IBSDDS schemes where access permission was made by the owner for an exact file and collusion attacks could be protected in the standard model. The file owner in an IBSDSS scheme has less control on his secret key than that in other public key encryption schemes.

Joan Arnedo [57] *et al.* proposed a secure communication setup for peer to peer communications. They proposed a security framework for cryptographic data setup in order to secure juxtapose overlay communications. The main features were including a completely modular approach which may cater to a broad set of scenarios, an effective secure key distribution method, and a hybrid key authenticity scheme. Limitation is that it is very difficult to manage this type of computing.

Kirtiraj B hatele [58] *et al.* worked on design of new hybrid security protocol architecture for online transaction. This new security protocol for on-line transaction could be designed using the combination of both symmetric and asymmetric cryptographic procedures which was known as hybrid cryptography. This protocol serves three important cryptographic primitives, integrity, confidentiality and authentication. This hybrid security protocol architecture was could be easily upgraded and the protocol becomes more immune against the attacks. At the same time it becomes more time efficient. Limitation is that there is a scarcity in terms space and time.

V.A.Suryawanshi [59] *et al.* introduced an optimized hardware implementation of area and speed improvement for the block cipher Advanced Encryption Standard (AES-128) using Field Programmable Graphic Array (FPGA). As AES has four transformations among them sub-byte and mix-column transformation were key challenges to implement in terms of area and speed. The implementation suggested that new method cyclic shift method for implementation of mix-column transformation which uses logical shift and XOR operation were effective**.**

Gianluca Lax [60] *et al.* worked on the vulnerabilities of digital signature deriving from the unobservability of electronic documents. Possible mechanisms to contrast such vulnerabilities were also proposed, highlighting their positive and negative points under a perspective that does not ignore both practical and regulatory aspects. Disadvantage is that this complicates the sharing of documents.

2.2 Observations

From the above section few observations have been drawn and are as follows:

a) Asymmetric algorithms are much secured against the random attacks generated by the hackers, thus large and variable key size makes the system more secured.

b) Public key encryption is used to solve the problem of key distribution. Long key length requires more bandwidth and time require to transmit long keys is large.

c) If multiple keys are used, security level of cryptographic model is increased. However, processing time is also increased but it does not affect the model so much.

d) Whenever there is an increase in the users, the security level of cryptographic model tends to fall. Security level in such cases will be maintained, if more number of iterations is carried out.

2.3 Gap and Problem formulation

From the above observations, it has been found that transmission of long key takes large time. So there is a need to optimize the keys which requires less time to encrypt the data. Proposed work has been carried keeping in mind the observations; key has been generated and optimized using AES.

2.4 Objectives

From the above observation objectives have been derived objectives which are used to develop and are as follows:

- To analyze AES algorithm and study the performance meaning parameters of this algorithm.
- To improve the key management in AES algorithm in order to reduce encryption time.
- To compare the proposed scheme and compare with the existing algorithms.

Chapter 3: Analysis of AES algorithm

The Advanced Encryption Standard (AES) is a Federal Information Processing Standard (FIPS) which was declared after an encryption algorithm standard competition by National Institute of Standards and Technology [62]. AES is also named as Rijndael. The overview and algorithm of AES is described in this chapter.

3.1 AES Algorithm

AES is a symmetric algorithm introduced in 2001. It is essential to know that the unknown key can be of any size and AES uses three distinct key sizes: 128, 192 and 256 bits. A number of AES parameters depend on its key size. It encrypts the data blocks of 128 bits in 10, 256 bits in 12 and 256 bits in 14 rounds depending on key size.

→ **State f**

f 0,0	f 0,1	f 0,2	f 0,3
f 1,0	f 1,1	f 1,2	f 1,3
f 2,0	f 2,1	f 2,2	f 2,3
f 3,0	f 3,1	f 3,2	f 3,3

→ **Key p**

p 0,0	p 0,1	p 0,2	p 0,3
p 1,0	p 1,1	p 1,2	p 1,3
p 2,0	p 2,1	p 2,2	p 2,3
p 3,0	p 3,1	p 3,2	p 3,3

Figure 3.1 State matrix

The algorithm has been divided into four transformations that are repeated 10, 12 or 14 times depending on the key size been used. Currently, it is believed that no simplification of transformation will allow breaking the AES algorithm. It is a block cipher with a fixed block size of 128 bits and a variable key length. The distinct conversions operate on the transitional results, which are known as state. The state is a rectangular array of bytes and

since the block size is 128 bits, which is 16 bytes, the rectangular array of dimensions 4x4 matrix. The number of columns is the block size divided by 32 and denoted (Nb), the number of columns of the cipher key, denoted (Nk), is equal to the key length divided by 32 and the number of rounds which is function of Nk and Nb are fixed, is denoted with (Nr) [62]. Figure of state matrix is shown in figure 3.1. Here the cipher input bytes are charted against the state bytes in the order of f0,0, f1,0, f2,0, f3,0, f0,1, f1,1, f2,1, f3,1 ... and the bytes of the cipher key are charted against the array in the order p0,0, p1,0, p2,0, p3,0, p0,1, p1,1, p2,1, p3,1, the cipher output comes from the state by taking the state bytes in the same order AES uses a variable number of rounds, which are fixed: A key of size 128 has 10 rounds, a key of size 192 has 12 rounds, a key of size 256 has 14 rounds [62].

3.2 Algebraic Properties

The set of all integers denoted by Z is closed down the action of subtraction, addition and multiplication. Z is not closed down the division action since the answer of two integers (e.g. 1 divide by 2) is not an integer. The following is a lists some of the basic properties of multiplication and addition for any integers a, b and c. Closed: (a + b) or (a × b) is an integer [62].

Associative: (a + (b + c)) = ((a + b) + c) or (a × (b × c)) = ((a × b) × c)

Commutative: (a + b) = (b + a) or (a × b) = (b × a)

Existence of neutral element: (a + 0) = a or (a × 1) = a, neutral components have no effect on other components when combined with them.

Existence of inverse element: (a + (-a) = 0, inverse of an element reverses the effect that element.

Distributive: a × (b + c) = (a × b) + (a × c)

3.2.1 Galois Field (2^8)

The byte level operations in the AES algorithm is defined in the finite field (or Galois Field) GF (2^8). There are only a definite number of component in a definite field and this number of components is given as q^z, where q is a prime number and z is a positive integer. A finite field can be represented as polynomials of degree smaller than the

degree of the irreducible reduction polynomial. A byte polynomial representation is given below:

$\sum h_i x^i = h_7 x^7 + h_6 x^6 + h_5 x^5 + h_4 x^4 + h_3 x^3 + h_2 x^2 + h_1 x^1 + h_0 x^0$

The arithmetic operations in the finite field are distinct from standard arithmetic and they are explained in the following part. When these components are represented as polynomials, then the arithmetic operations are performed with modulo m. 'm' is an irreducible polynomial over the Galois field with the same degree [62]. For AES algorithm this irreducible polynomial is given by:

$m(x) = x^7 + x^5 + x^4 + x^2 + x + 1$

3.2.2 Euclidean algorithm

The Euclidean algorithm determines the greatest common divisor (gcd) of two integers. The greatest common divisor of two integers is the largest number that divides both integers, if both integers are not zero. For example gcd of 6 and 4 is 12. The continued Euclidean algorithm is a form of the Euclidean algorithm. Its input are two integers a and b then the algorithm figure out their greatest common divisor as well as integers x and y such that gcd, dx + ry = gcd (d, r). This works because the stride of Euclid's algorithm always deals with sums of multiples of d and r. The equation dx + ry = gcd (d, r) is especially helpful when d and r are co-prime. X is then the multiplicative inverse (reciprocal) of d modulo r. In modular arithmetic, the multiplicative inverse of x can also be defined: it is the number a such that (h × x) mod z = 1. However, the multiplicative inverse only exists if, h and z are co-prime. For example, the inverse of 5 modulo 11 is 3 because it is the solution to (5×x) mod11 = 4.The extended Euclidean algorithm may be used to figure out the multiplicative inverse modulo of a number [62].

3.2.3 Addition and Subtraction

The addition and subtraction of the polynomials in a finite field is a simple EXOR operation and same for both of addition and subtraction. The addition of two components in a finite field can be accomplished by adding the coefficients for the analogous powers in the polynomials for the two components [62]. The addition is achieved with the XOR operation

i.e 1 XOR1=0, 1 XOR 0=1, 0 XOR 1=0 and 0 XOR 0=0. In order to make it more clear there is an example for the addition polynomial:

$(x^7 + x^4 + x^2 + 1) + (x^6 + x^5 + x^2 + x) = x^7 + x^6 + x^5 + x^4 + x + 1$ (polynomial notation)

{10010101} XOR {01100110} = {11110011} (binary notation)

{43} XOR {80} = {c3} (hexadecimal notation)

Similarly, subtraction of polynomial is same to the addition of polynomials.

3.2.4 Multiplication

In this the multiplication of polynomial is an irreducible polynomial of degree 8. A polynomial is irreducible if its divisors are one and itself. For, the AES algorithm this irreducible polynomial is.

$m(x) = x^7 + x^5 + x^2 + x + 1$

For example: $(x^7 + x^5 + x^3 + x^2 + 1) * (x^6 + x + 1) = (x^{13} + x^{11} + x^9 + x^7 + x^5 + x^4 + x^2 + x + 1)$

3.2.5 Polynomials with coefficients in GF (2^8)

Polynomials of degree less than 4 that are representative of a 32 bit word in the internal state of the Rijndael can be defined with the coefficients that are finite field components. An example is, $(b_3x^3 + b_2x^2 + b_1x + b0)$ where the coefficient (b_3, b_2, b_1, b_0) each represent a byte in a 32 bit word. Finite field addition for these polynomials is achieved by adding the coefficients of power x., which is equivalent to exclusive ORing the corresponding bytes. As described in the FIPS standard 1997, multiplication is achieved by polynomial product and reducing the product modulo a polynomial of degree 4, so that the product is a polynomial of degree less than 4. For Rijndael algorithm, the polynomial x^4+1 is used as the 4 degree polynomial [62].

3.3 Conclusion

AES is a block cipher accepted as an encryption standard by the US government, and is normal to be used worldwide and consider broadly. The design and durability of all key lengths of the AES algorithm (i.e., 128,192 and 256) are acceptable to assure classified information up to the secret level. The implementation of AES in stock designed to assure national security schemes and/or information must be analyzed and authenticated by NSA

prior to their addition and use. The AES algorithm has been critically analyzed on the basis of round function, key utilization, block size, rounds, key length, computational speed, power consumption and memory usage. The development of modified key management in AES has been done in next chapter in order to optimize the encryption time.

Chapter 4: Proposed Work

In the past AES technique was used with 128,192 and 256 bit key. The biggest problem in this technique is that these keys require more time to encrypt and decrypt the message. So, the main aim is to reduce the key generation and transmission time which results decrease the processing time in encryption process. By improving the key generation process in AES, processing time for different file sizes has been reduced.

4.1 Shift Rows

In modified shift row the fourth row of the key matrix is changed to its binary form. The binary pattern is classified into 8 groups, each group having 4 bits starting from first bit as shown in the figure then b0 bits are XOR with the bits of b4 to generate a 4-bit binary result, E as shown below. Now we can obtain F, G and H are obtained from the groups of (b1, b5), (b2, b6), (b3, b7). In the E first two bits show the row number and they have to be cyclically left shifted. Now check out number of ones in F and for the row we have to calculate less than one ones in F. It gives that how much shift is in the E. Repeat the same process for G. figure of modified shift row is shown below in figure 4.1.

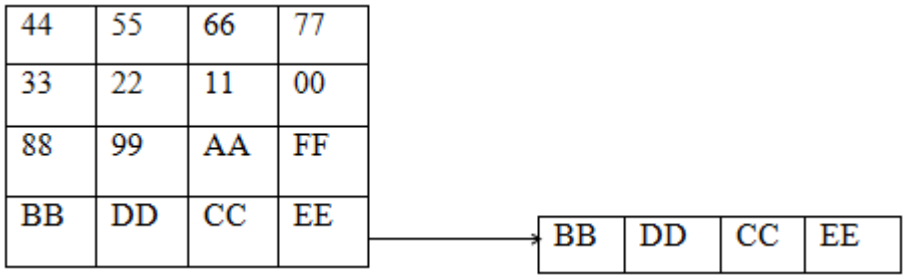

Figure 4.1 Modified shift rows

In this above diagram in the 4th row BB is written in binary form as b0= 1011, b1 = 1011 and next DD is written as b2= 1101, b3= 1101 and CC is written as b4= 1100, b5= 1100 and last EE is written as b6= 1110, b7= 1110.

b0 XOR b4 = 0111 = E

b1 XOR b5 = 0111 = F

b2 XOR b6 = 0011 = G

b3 XOR b7 = 0011 = H

4.2 Sub-bytes

Binary equivalent of second row of the key matrix is formed in process of modified Sub-bytes. Four patterns of binary equivalent are produced. In this process, first four bits of each binary pattern is separated out as explained in Figure. These bits are then grouped in 2- bit pattern and a1, a2 up to a8 is obtained. Further to carry encryption process, groups as (a1a8), (a2a7), (a3a6) up to (a4a5) is created. Substitution is carried out at data location H (a1, a8) from S-Box. Process of substitution is carried out following the original sub-bytes round of AES method. All the data locations wiz: (a2, a7), (a3, a6) and (a4, a5) are substituted. This explains the process of converting first row of cipher matrix, the entire process is repeated for second row too. Modified sub-bytes are shown in figure 4.2.

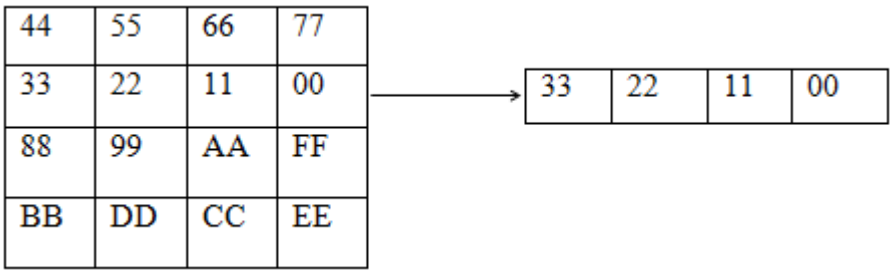

Figure 4.2 Modified sub bytes

Now 33 is written in binary form as 0011 and 0011 and 22 can be written as 0010 and 0010 same 11 can be written as 0001 and 0001 and lastly 00 can be written as 0000 and 0000. Now from we have to select 4-bit take 1st one from 33, 22, 11 and 00.

Now it becomes like 0011001000010000 after this we have to do grouping of it as 00= a1, 11= a2, 00= a3, 10= a4, 00= a5, 01= a6, 00= a7, 00= a8,

a1a8=0000

a2a7=1100

a3a6=0000

a4a5=0001

4.3 Mix columns

In these step elements of first row of cipher matrix is processed as shown in figure 4.3. Four groups are formed from the elements of first row. The groups are then converted into their respective decimal value. Modulus -4 operations is performed on decimal value obtained. As

it is a modulus-4 operation, the remainder will lie in range $0 \leq r \leq 3$ i.e.0, 1 ,2 and 3. The process of mix column as in original AES algorithm is carried out in this step on the selected column.

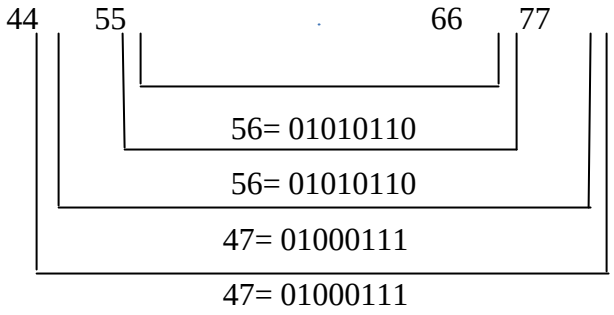

Figure 4.3 Modified mix columns

$56 = (86)_{10}$ and $47 = (71)_{10}$

86%4 = 2; Mix the 3rd column with state transition matrix

71%4 = 3; Mix the 4rd column with state transition matrix

4.4 Add Round Key Transformations

In this transformation, a round key is added to the State by a bitwise XOR operation. Each Round Key includes of Nb words from the key and is shown in figure 4.4. Those Nb words are each added into the columns of the state such that:

$[g0, g1, g2, g3] = [F0, F1, F2, F3] \text{ XOR } [p_{round * Nb+c}]$ for $0 < c < Nb$

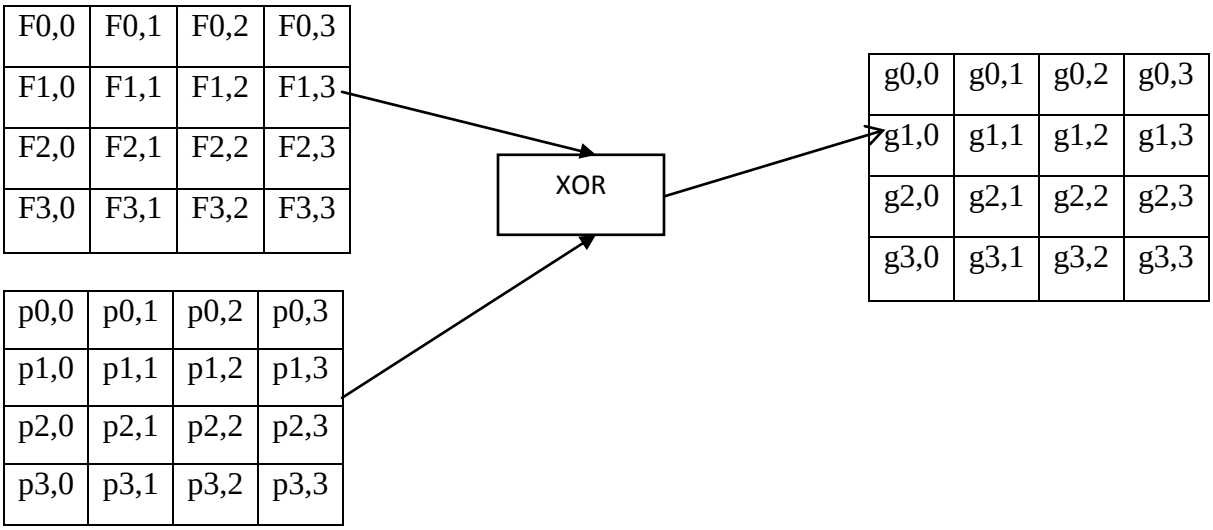

Figure 4.4: Add Round Key Transformations

4.5 AES Round Structure

The four transformations have been used followed by the sub bytes, shift rows, mix columns, add round key and a Sate which is used between the transformations used. All the four stages used in the AES rounds have been discussed above. Figure of aes round structure is shown in Figure 4.5.

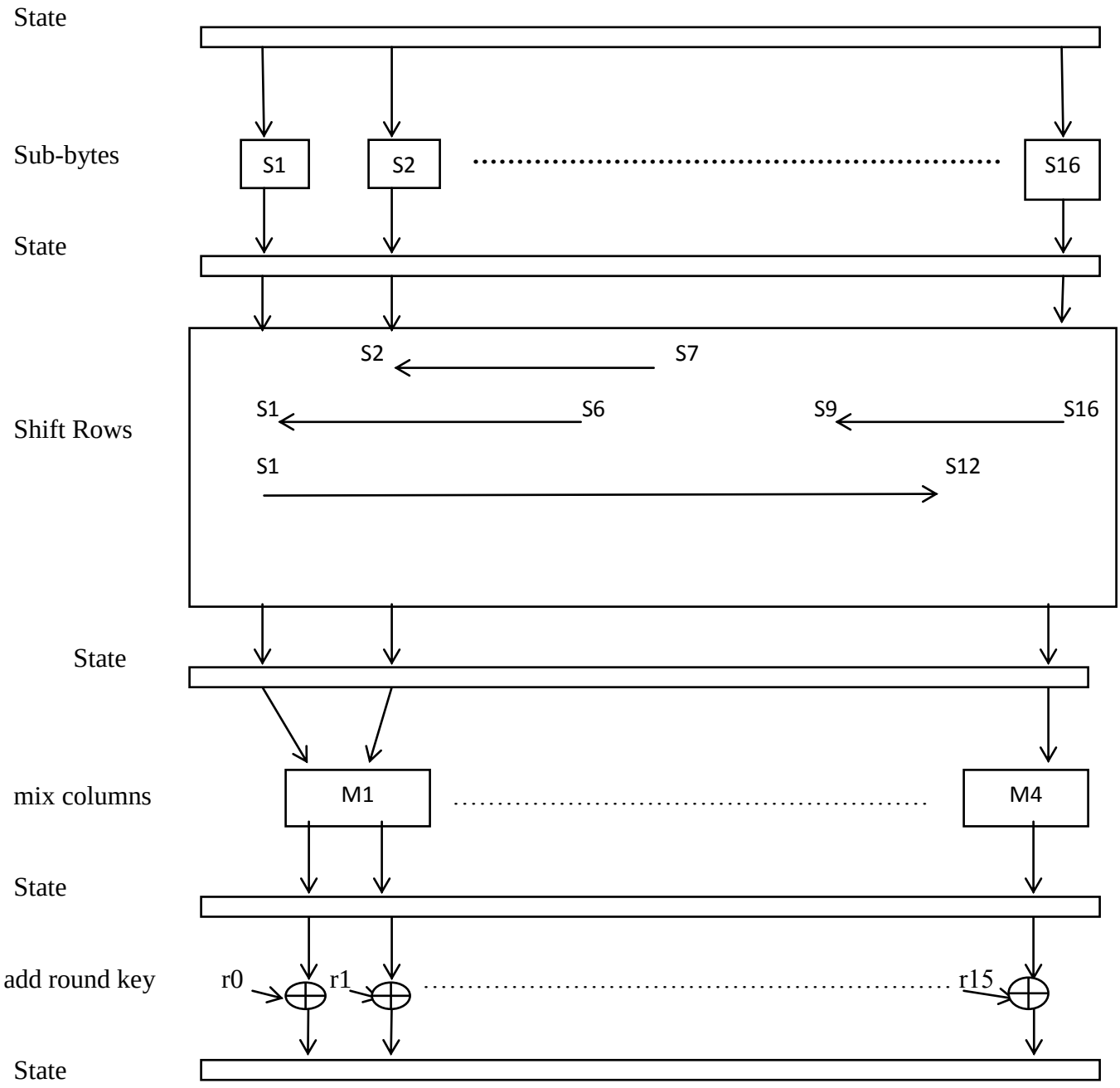

Figure 4.5: AES Round Structure

4.6 S-Box Implementation

The S-Box Implementation has been shown in the table 3. In this hexadecimal numbers are used in order to get the desired result by evaluating first ROWs and then COLUMNS. Through the substitution box we can get the number of results in matrix form which can be used for providing information security to the system.

Table 4.1 S-Box Implementation

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	Ab	76
1	Ca	82	c9	7d	Fa	59	47	f0	Ad	d4	a2	Af	9c	a4	72	c0
2	b7	Fd	93	26	36	3f	f7	Cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	Ed	20	Fc	b1	5b	6a	Cb	be	39	4a	4c	58	Cf
6	d0	Ef	Aa	Fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	Bc	b6	da	21	10	ff	f3	d2
8	Cd	0c	13	Ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	Dc	22	2a	90	88	46	Ee	b8	14	de	5e	0b	Db
A	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
B	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	Ea	65	7a	Ae	08
C	Ba	78	25	2e	1c	a6	b4	c6	e8	Dd	74	1f	4b	bd	8b	8a
D	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
E	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	Df
F	8c	a1	89	0d	Bf	e6	42	68	41	99	2d	0f	b0	54	Bb	16

4.7 Encryption Process

In this encryption process using sub bytes i am replacing every byte in state by another byte with the help of S-Box. Shifting every row in the array with some value to the left using shift rows is done. Using mix columns a linear transformation on the columns of the state is done. Lastly, each byte of a round key is added to the state by bitwise using XOR operation. Figure of encryption process is shown in Figure 4.6.

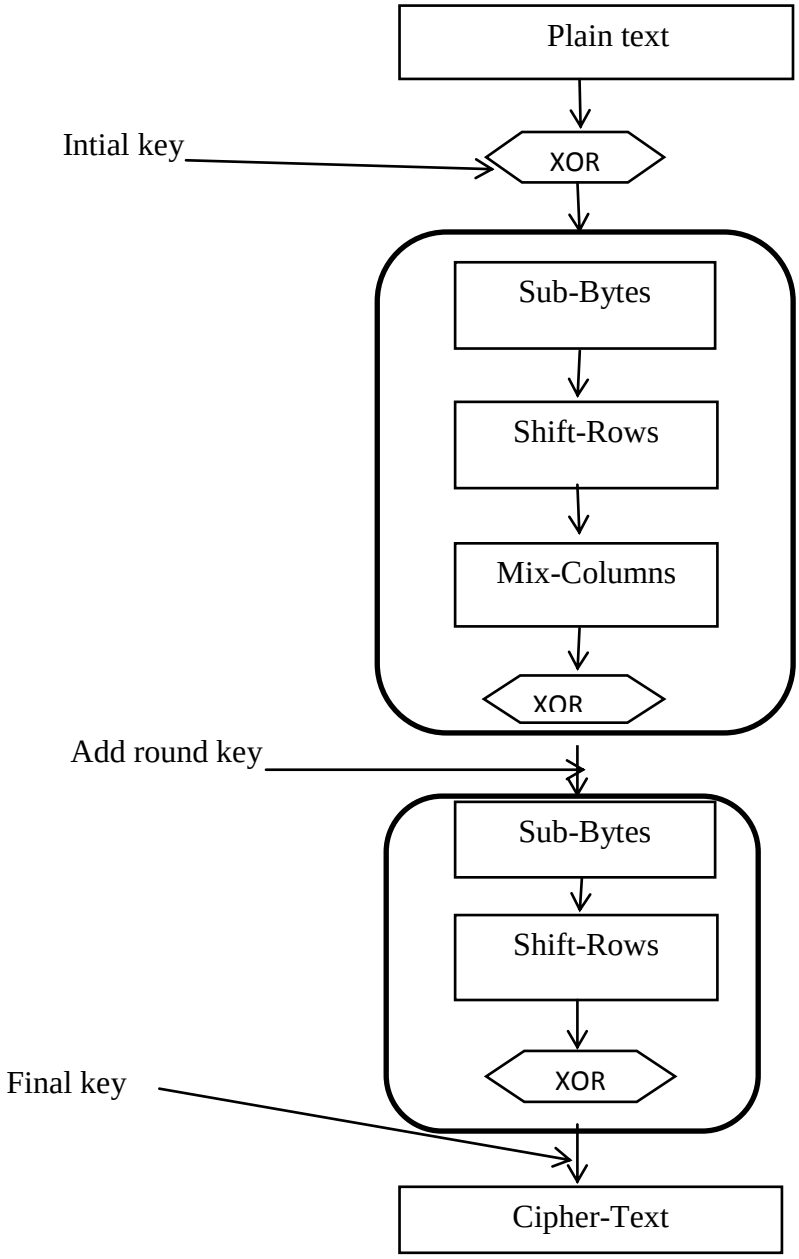

Figure 4.6: Encryption Process

4.7.1 AES Key Expansion

The Key agenda is responsible for developing a short key into a bigger key, whose parts are used during the distinct iterations. Each key size is developing to a distinct size; 128 bit key is developed to a 176 byte key; 192 bit key is developed to a 208 byte key, and 256 bit key is developed to a 240 byte key.

There is an affinity between the cipher key size, the number of rounds and the developed key size. For an 128-bit key, there is one initial Add Round-Key action plus there are 10 rounds and each round needs a new 16 byte key, therefore we require 10+1 Round Keys of 16 byte, which equals 176 byte. The same logic can be applied to the two other cipher key sizes. The general formula is that:

Developed Key Size = (number of Rounds+1) * Block-Size

The key is first transcribed into first four word of the developed key used. The remainder of developed key is filled with four words at a time. Each added word w[i] depend on the preceding words w [i-1], and the word four position back w [i-4]. In the three out of four only XOR is used for the key expansion

The function M consists of the following sub function:
i) Rot-Word: It performs the circular one byte left shift on a word. This means that the input word [h0 h1 h2 h3] is transformed into the [h1 h2 h3 h0].

ii) Sub-Word: In this it perform the substitution on each byte of the input word from the S-Box.

iii) The result of step 1 and step 2 is then XORed with the Round constant function RCON. In round constant the three right most bits are always '0' used.in the word. Therefore, the reaction of the XOR with RCON performed on the word the word uses the XOR on leftmost byte of the word and is shown in figure 4.7.

It has been found that the round constant is distinct for distinct rounds and can be defined as Rcon [j] = (RC [j], 0, 0, 0) with RC [1]=1, RC[j]= 2 ● RC [j-1] and multiplication is defined over the field GF(2^8) [68].

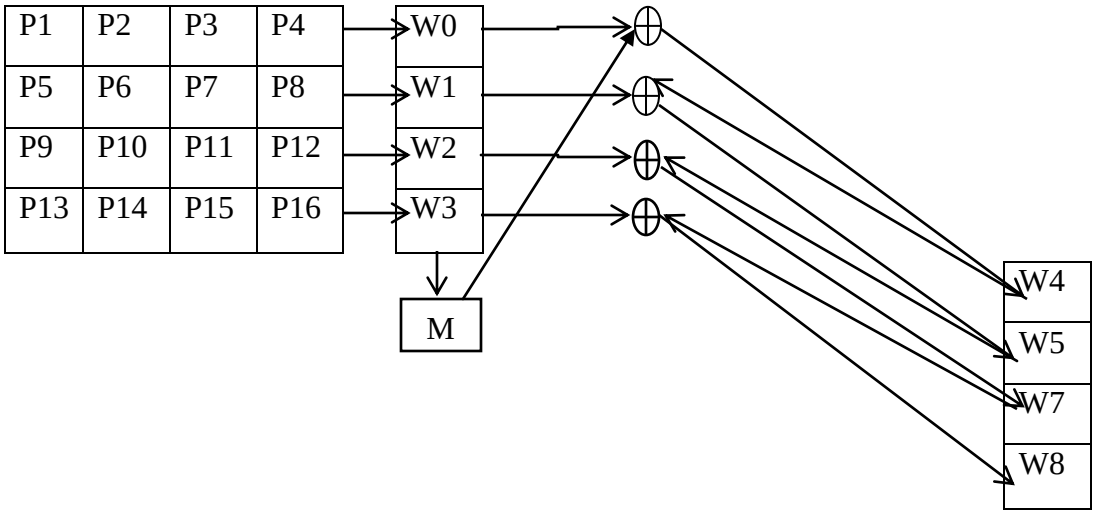

Figure 4.7 AES key Expansion

The values of RC [j] in hexadecimal are shown as:

J	1	2	3	4	5	6	7	8	9	10
RC [j]	01	02	04	08	10	20	40	80	1B	36

Let us take an example in order to make it clearer:

The Round Key used for the 8 rounds is

EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F

AES was designed to key expansion algorithm for the resistant against the known cryptanalytic attack.

4.8 Decryption process

In decryption process exact reversal of what is done in encryption is carried out. All the steps to recover original data wiz: inverse mix columns, inverse shift rows and inverse sub byte are performed.

a) Inverse Mix columns

In this same methodology as considered in modified Mix-columns is used but exactly in reverse way. The last row of cipher key matrix is considered in this process. Then, all mathematical process is carried out on the data matrix in opposite way.

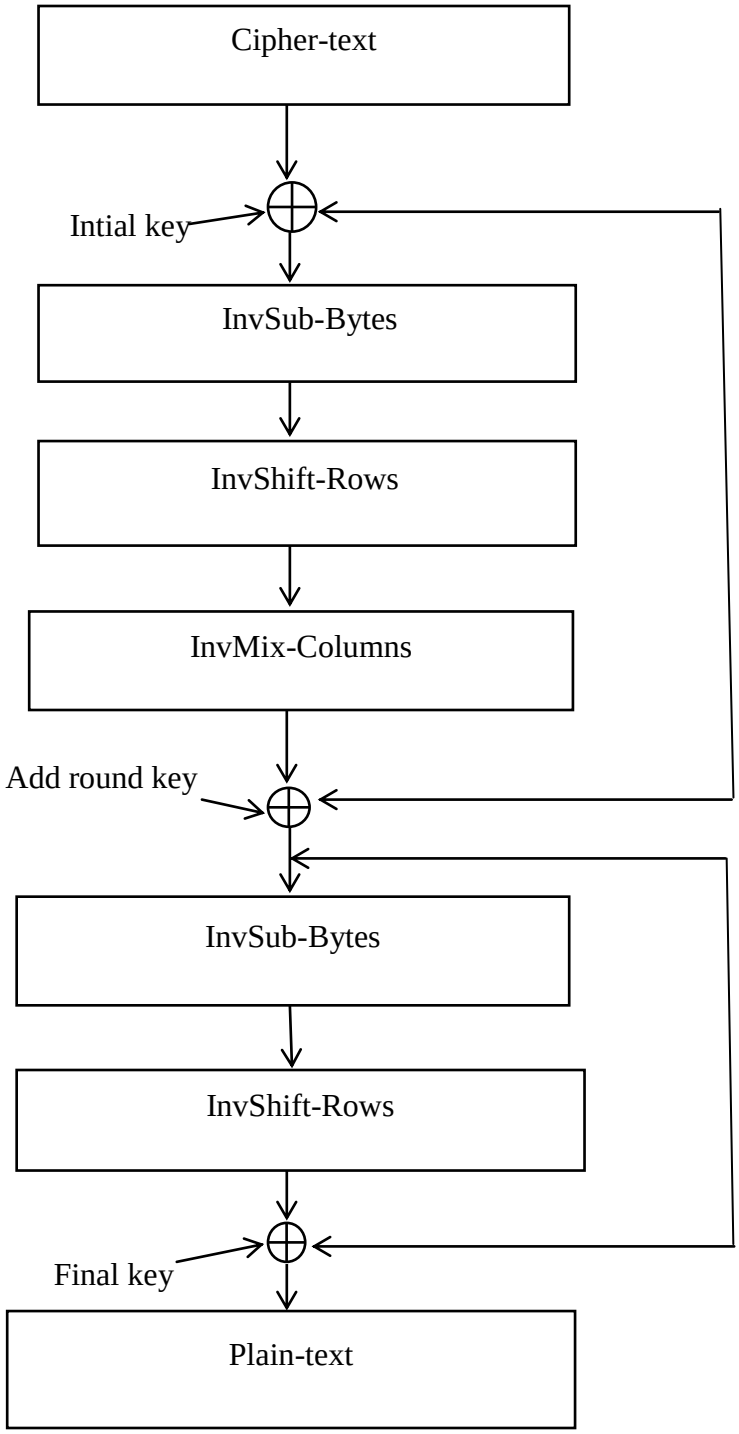

Figure 4.8: AES Decryption Process

a) Inverse shift rows

The bits of third row of cipher matrix are patterned in the same way as done in process of shift rows. All steps are carried out in the way explained in figure 4.8

b) Inverse sub byte

In this process, second row of cipher matrix is retrieved back. The methodology carried out in process Modified sub byte is used here as well but order of substitution is reversed. It is carried out in inverse way such as (g4g5), (g3g6), (g2g7) and (g1g8). Inverse S-Box is employed for substitution of the data in the cipher matrix.

4.8.1 Inverse S-Box Table

Inverse S-Box is shown in table 4.2.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	52	09	6a	d5	30	36	a5	38	Bf	40	a3	9e	81	f3	d7	Fb
1	7c	e3	39	82	9b	2f	Ff	87	34	8e	43	44	c4	de	e9	Cb
2	54	7b	94	32	a6	c2	23	3d	Ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	60	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	Cc	5d	65	b6	92
5	6c	70	48	50	5d	Ed	b9	Da	5e	15	46	57	a7	8d	9d	84
6	90	d8	Ab	00	8c	Bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	Ca	3f	0f	02	c1	Af	Bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	Dc	Ea	97	f2	Cf	Ce	f0	b4	e6	73
9	96	Ac	74	22	e7	Ad	35	85	e2	f9	37	t8	1c	75	df	6e
A	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	Aa	18	be	1b
B	Fc	56	3e	4b	c6	d2	79	20	9a	Db	c0	Fe	78	cd	6a	f4
C	1f	Dd	Aa	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
D	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	Ef
E	a0	e0	3b	4d	Ae	2a	f5	b0	68	Eb	Bb	3c	83	53	99	61
F	17	2b	04	7e	Ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Table 4.2: Inverse S- Box Implementation

4.9 Modified Approach

The generation process of S-Box is mentioned. We have to choose random key of size 8 bytes or 64 bits and at the receiver end it is known by the acceptor for decrypt the message.

Develop a 4 by 4 matrix with these 8 bytes. Test that matrix formed is singular or not. Singularity means that it determinant is zero. We have to check its singularity with respect to an irreducible polynomial which is also key dependent as it is in S-Box construction. If developed matrix is singular then use XOR operation and do XOR with each byte of the key with 01H. Now, again check the singularity of the matrix.

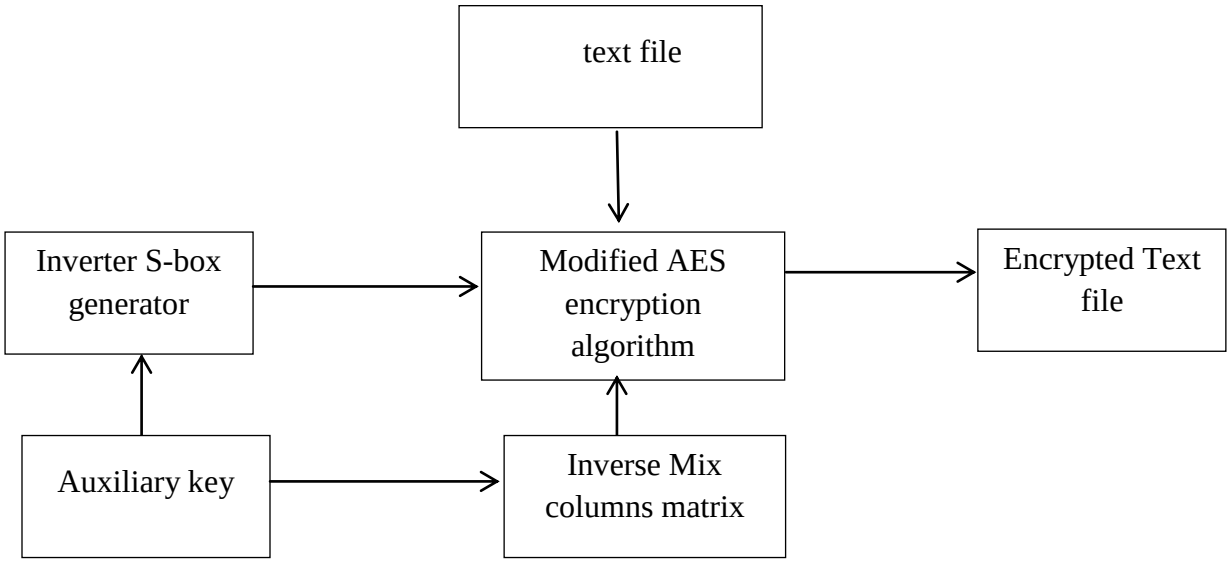

Figure 4.9 Modified AES encryption

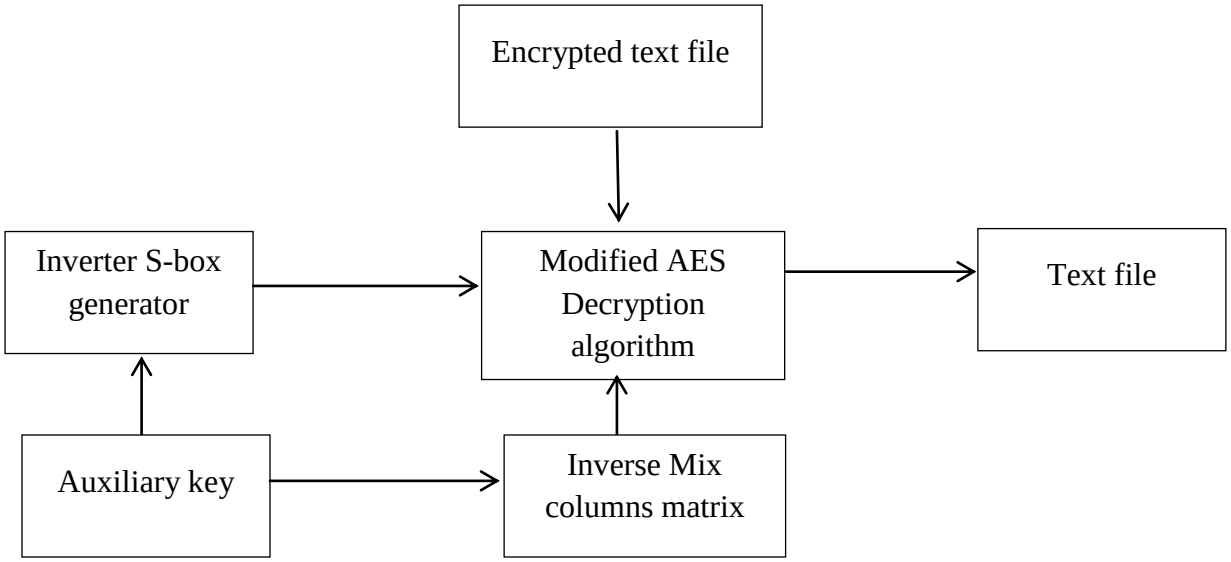

Figure 4.10 Modified AES decryption

Repeating the above step until the nonsingular matrix has been obtained. Use this matrix for the operation in mix column matrix as done in the original AES encryption algorithm. Figure, show the block diagram of modified encryption and decryption algorithms for encrypts or for decrypts the text. Figure of modified AES encryption and decryption process shown in figure 4.9 and 4.10 respectively.

Chapter 5: Results and Discussion

This chapter shows the simulation results for encryption and decryption time which have been obtained using MATLAB 2013. Further, comparison of proposed algorithm with AES has been done.

5.1 Calculation of encryption time

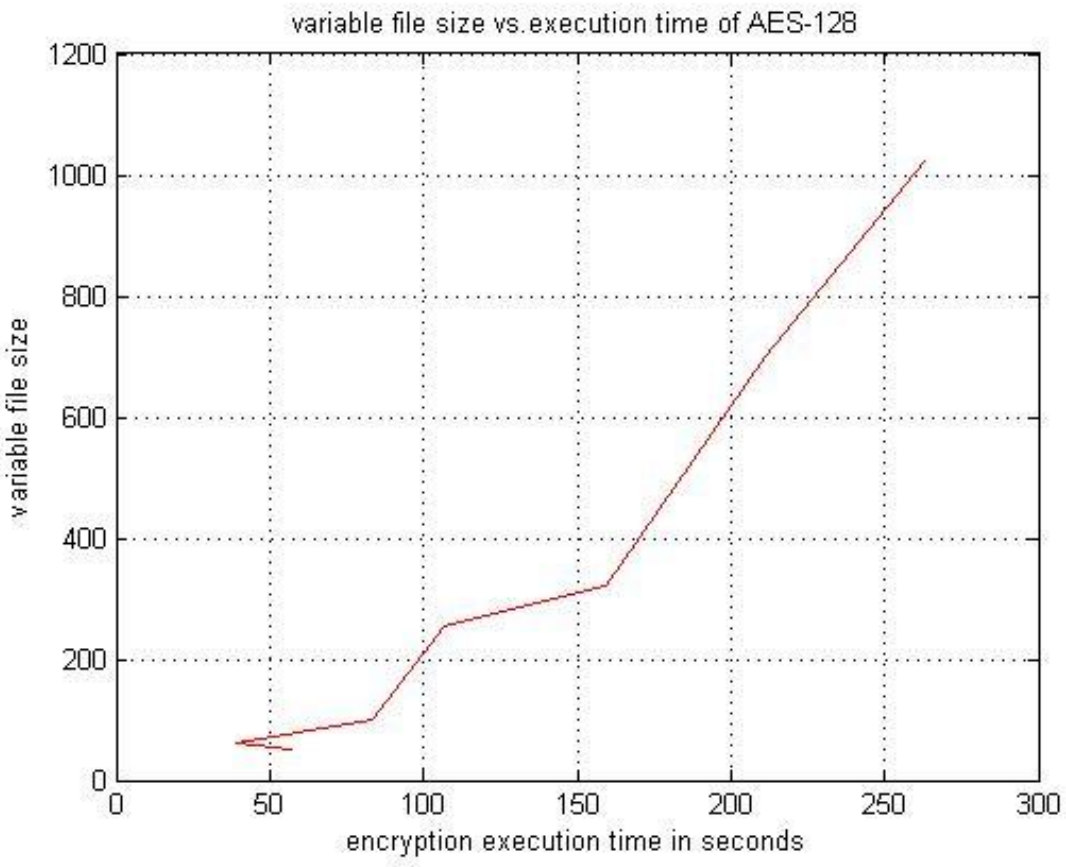

Figure 5.1 Encryption time of AES-128

The figure 5.1 depicts the time taken for encryption with respect to the file size of AES128. It draws a relationship between encryption time and file size keeping bit size constant. In this 500KB file takes 190 seconds to encrypt.

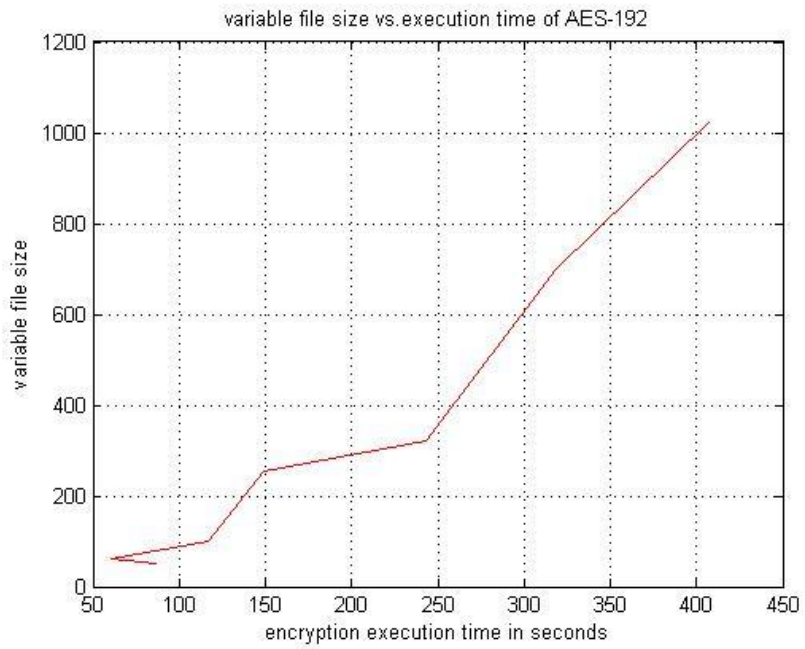

Figure 5.2 Encryption time of AES-192

The figure 5.2 depicts the time taken for encryption with respect to the file size of AES192. Here for AES-192 encryption time taken by file size of 600 KB is 300 seconds.

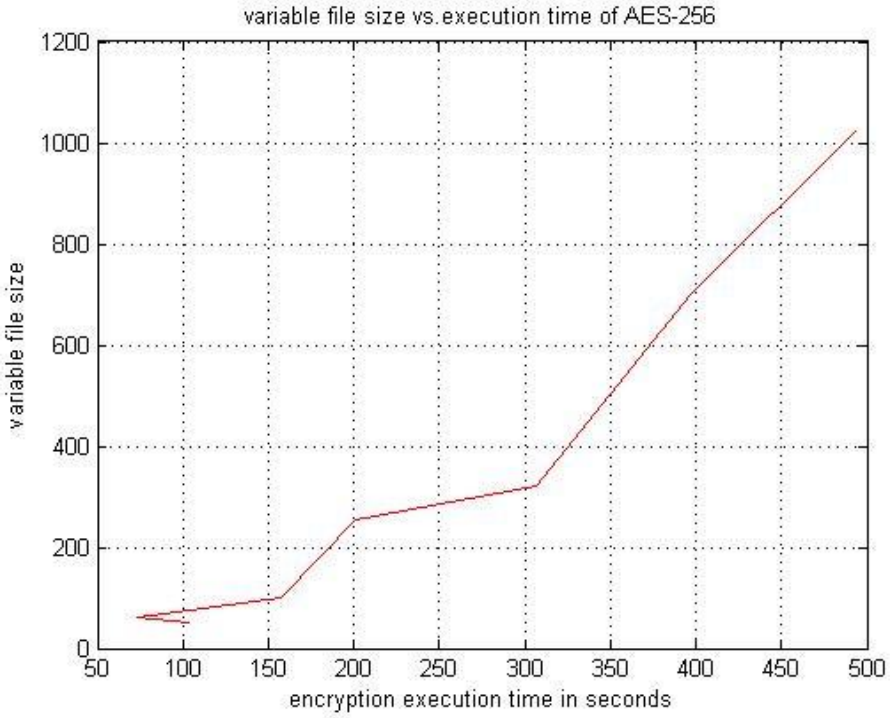

Figure 5.3 Encryption time of AES-256

The figure 5.3 depicts the time taken for encryption with respect to the file size of AES256. Here, it shows that as the bit length increases encryption time taken also increases. In this plot for 600 KB file size encryption time taken is 370 seconds.

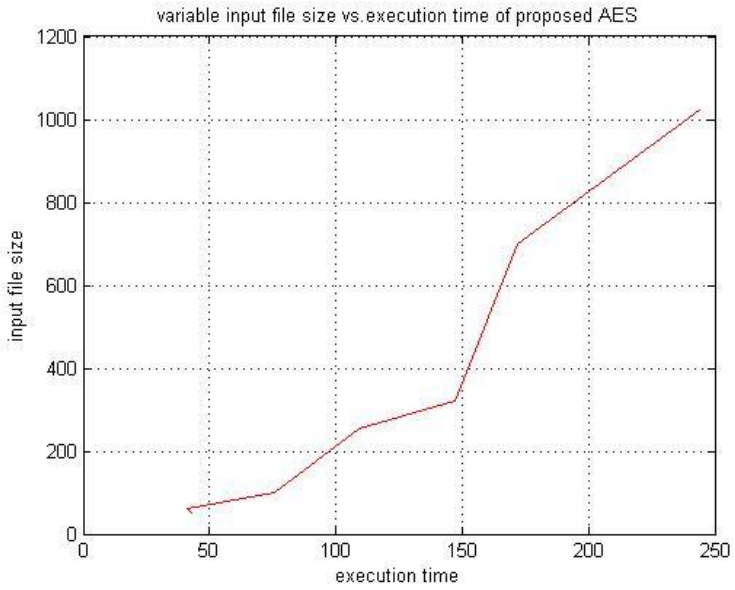

Figure 5.4 Encryption time of AES-proposed

5.1.1 Comparison with various encryption AES schemes

The proposed scheme is compared with AES-128, 192 and 256 variations. Table 5.1 shows the encryption time comparison among the proposed scheme and AES variations.

Table 5.1 Encryption time comparison (sec)

File size (kb)	AES-128	AES-192	AES-256	Proposed
50	57	86	103	43
60	39	61	73	41
100	83	117	157	76
256	107	149	201	109
320	159	243	307	147
700	211	319	397	172
1024	263	407	493	244

From figures 5.1, 5.2, 5.3 and 5.4, it has been observed that the proposed scheme requires less encryption time as compare to the others schemes. For a file size of 100 kb, AES-128

takes 83 seconds, AES-192 takes 117 and AES-256 takes 157 seconds to encrypt the data. The proposed scheme takes 76 seconds, which is less in compassion to AES algorithm. In comparison to AES-128, 8.4% time has been saved using our scheme. As file size increases from 100 kb to 1024 kb, only 7.9% time has been saved. It is because as the file size increases number of files are increases and it takes more time to encrypt more numbers of file. Lastly, the advantage to use our scheme is that we can encrypt the message with lesser time than the other AES scheme.

5.1.2 Calculation of Encryption Throughput

Encryption Throughput (Kb/sec) = ∑ Input file size/ ∑ Encryption Execution time

∑ Input file size = 50+60+100+256+320+700+1024

∑ Input file size = 2510 Kb

Encryption Throughput for AES-128

∑ Encryption Execution Time [AES-128] = 57+39+83+107+159+211+263

∑ Encryption Execution Time [AES-128] = 919

Encryption Throughput [AES-128] = 1260/1649

Encryption Throughput [AES-128] = 2.73 Kb/sec

Encryption Throughput for AES-192

∑ Encryption Execution Time [AES-192] = 86+61+117+149+243+319+407

∑ Encryption Execution Time [AES-192] = 1382

Encryption Throughput [AES-192] = 2510/1382

Encryption Throughput [AES-192] = 1.82 Kb/sec

Encryption Throughput for AES-256

∑ Encryption Execution Time [AES-256] = 103+73+157+201+307+397+493

∑ Encryption Execution Time [AES-256] = 1731

Encryption Throughput [AES-256] = 2510/1731

Encryption Throughput [AES-256] = 1.45 Kb/sec

Encryption Throughput for Proposed Algorithm

∑ Encryption Execution Time [Proposed] = 43+41+76+109+147+172+244

∑ Encryption Execution Time [Proposed] = 832

Encryption Throughput [Proposed] = 2510/832

Encryption Throughput [Proposed] = 3.01 Kb/sec

From the above calculated values of throughput, it is clear that the proposed algorithm provides optimized results in comparison to the AES and result is shown in figure 5.5.

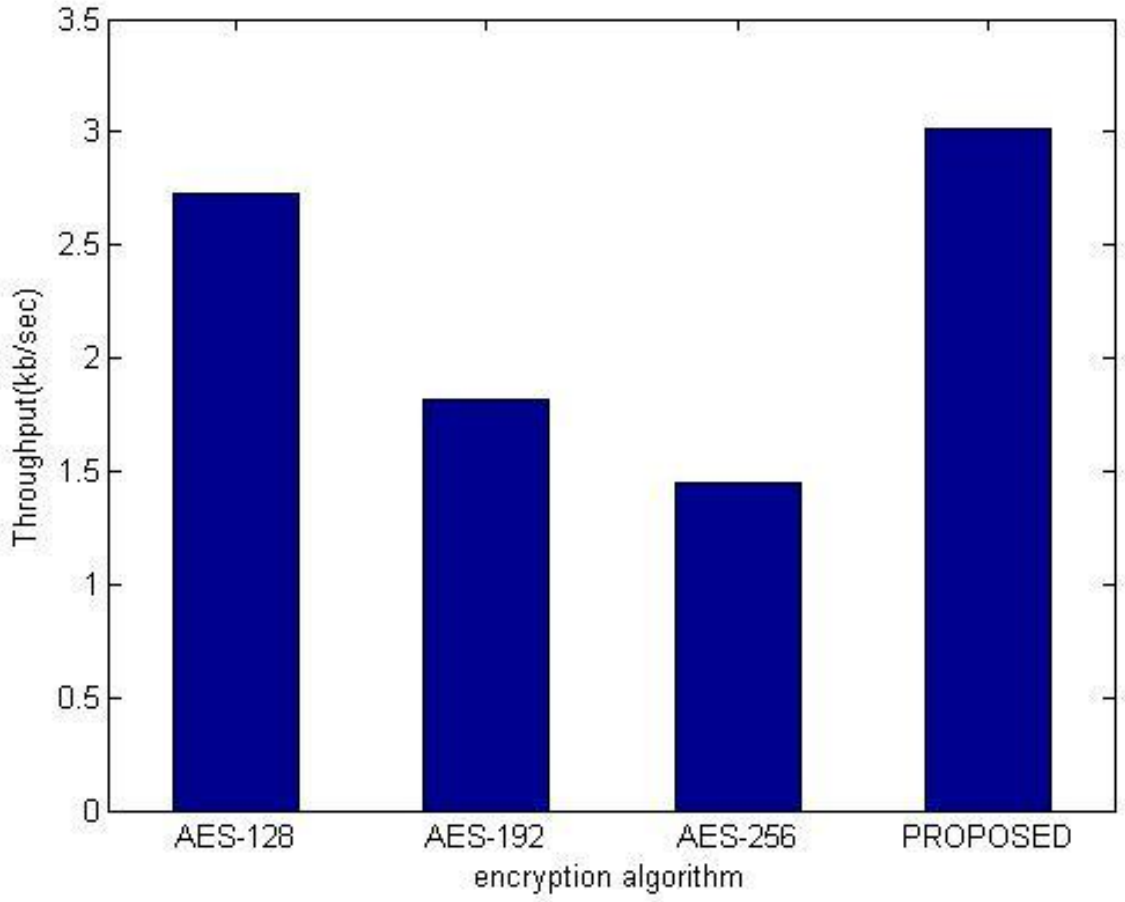

Figure 5.5 Throughput of various encryption algorithms

5.2 Calculation of decryption time

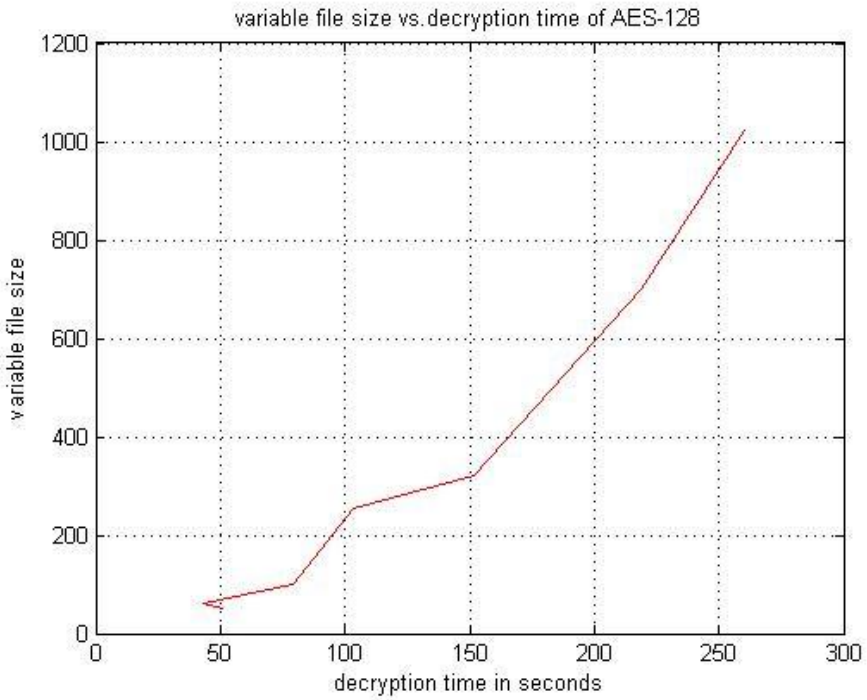

Figure 5.6 Decryption time for AES-128

The figure 5.6 depicts the time taken for decryption with respect to the file size of AES128. This is plotted using values obtained by the proposed algorithm mentioned in table 5.2. For 600KB input file size time taken for decryption is 200 seconds.

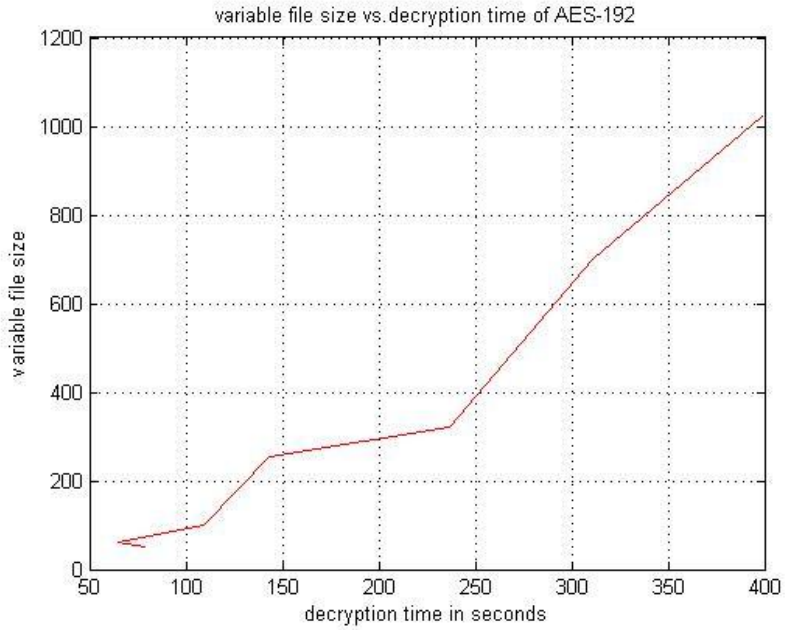

Figure 5.7 Decryption time for AES-192

The figure 5.7 shows using key length of 192 bit in AES; if file size increases, the decryption time also increases. Time taken to decrypt input file size of 100KB is 109 seconds whereas file size of 1024KB, the decryption time is 399 seconds. It has been observed that if a file size increases10 times, decryption time increases four times which does not affects the cryptographic model so much.

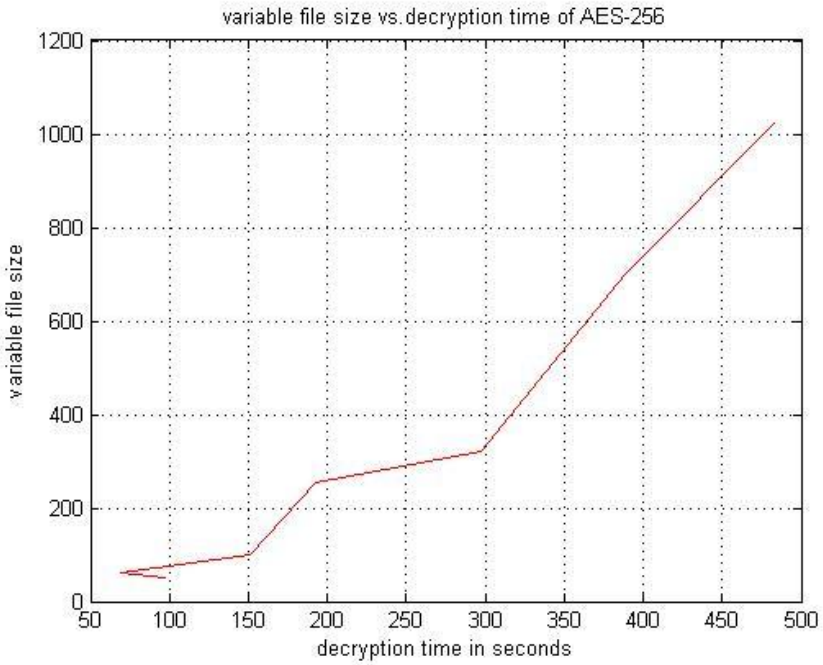

Figure 5.8 Decryption time for AES-256

The figure 5.8 depicts the time taken for decryption with respect to the file size of AES256. Time taken to decrypt input file size of 600KB in AES-256 is 370 seconds. The figure 5.8 depicts the time taken for decryption with respect to the file size of AES proposed work.

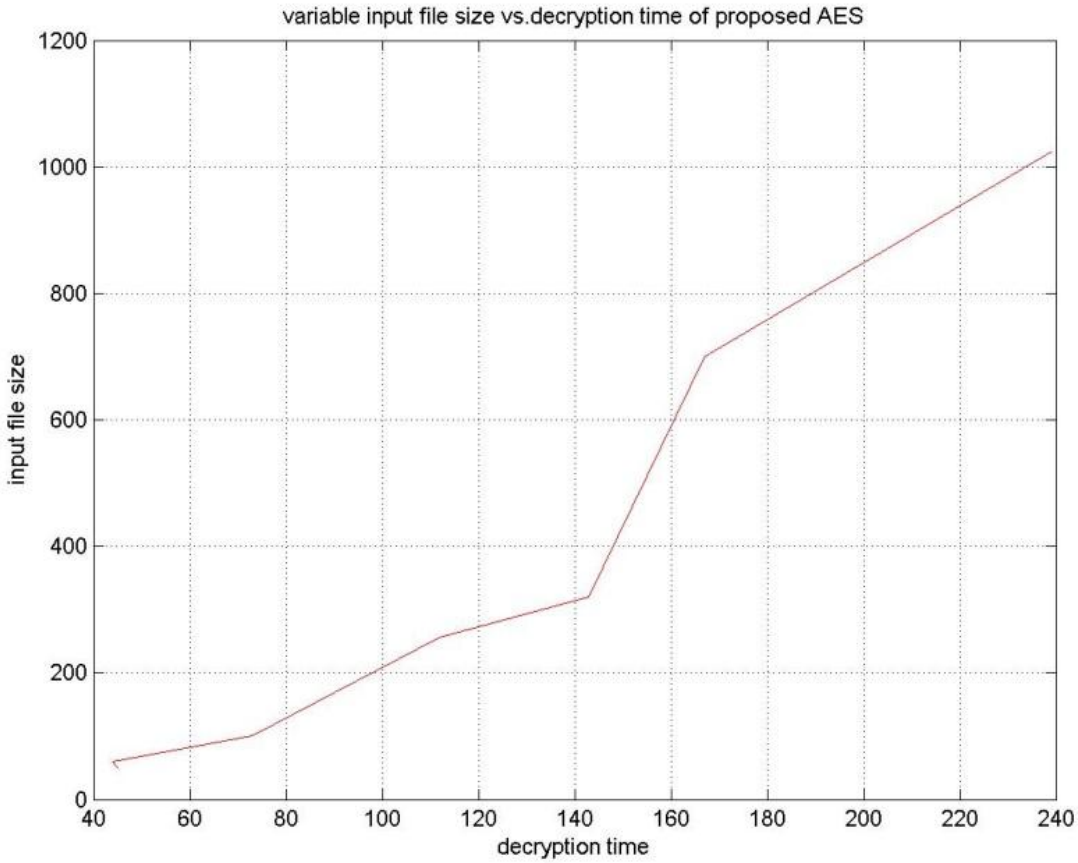

Figure 5.9 Decryption time for AES-proposed

5.2.1 Comparison with various decryption AES scheme

The proposed scheme is compared with AES-128, 192, 256. Table 5.2 shows the decryption time among the various schemes of AES and proposed scheme.

Table 5.2 Decryption time comparison

File size	AES-128	AES-192	AES-256	PROPOSED
50 kb	51	79	97	45
60 kb	43	65	69	44
100 kb	79	109	151	73
256 kb	103	143	193	112
320 kb	152	237	297	143
700 kb	219	311	389	167
1024 kb	260	399	483	242

From figures 5.6, 5.7, 5.8 and 5.9, it has been observed that the proposed scheme requires less decryption time as compare to the others schemes. For a file size of 100 kb, AES-128 takes 79 seconds, AES-192 takes 109 and AES-256 takes 151 seconds to decrypt the data. The proposed scheme takes 73 seconds, which is less in compassion to AES algorithm. In comparison to AES-128, 7.6% time has been saved using our scheme. As file size increases from 100 kb to 1024 kb, only 6.9% time has been saved. It is because as the file size increases number of files are increases and it takes more time to decrypt more numbers of file. Lastly, the advantage to use our scheme is that it can decrypt the message with lesser time than the other AES scheme.

5.2.2 Calculation of Decryption Throughput

Decryption Throughput (Kb/sec) = ∑ Input file size/ ∑ Decryption Execution time

∑ Input file size = 50+60+100+256+320+700+1024

∑ Input file size = 2510 Kb

Decryption Throughput for AES-128

∑ Decryption Execution Time [AES-128] = 51+43+79+103+152+219+260

∑ Decryption Execution Time [AES-128] = 907

Decryption Throughput [AES-128] = 2510/907

Decryption Throughput [AES-128] = 2.76 Kb/sec

Decryption Throughput for AES-192

∑ Decryption Execution Time [AES-192] = 79+65+109+143+237+311+399

∑ Decryption Execution Time [AES-192] = 1343

Decryption Throughput [AES-192] = 2510/1382

Decryption Throughput [AES-192] = 1.87 Kb/sec

Decryption Throughput for AES-256

∑ Decryption Execution Time [AES-256] = 97+69+151+193+297+389+483

∑ Decryption Execution Time [AES-256] = 1679

Decryption Throughput [AES-256] = 2510/1679

Decryption Throughput [AES-256] = 1.49 Kb/sec

Decryption Throughput for Proposed Algorithm

∑ Decryption Execution Time [Proposed] = 45+44+73+112+143+167+239

∑ Decryption Execution Time [Proposed] = 823

Decryption Throughput [Proposed] = 2510/823

Decryption Throughput [Proposed] = 3.05 Kb/sec

From the above calculated values of throughput, it is clear that the proposed algorithm provides optimized results in comparison to the other decryption algorithm and results are shown in figure: 5.10

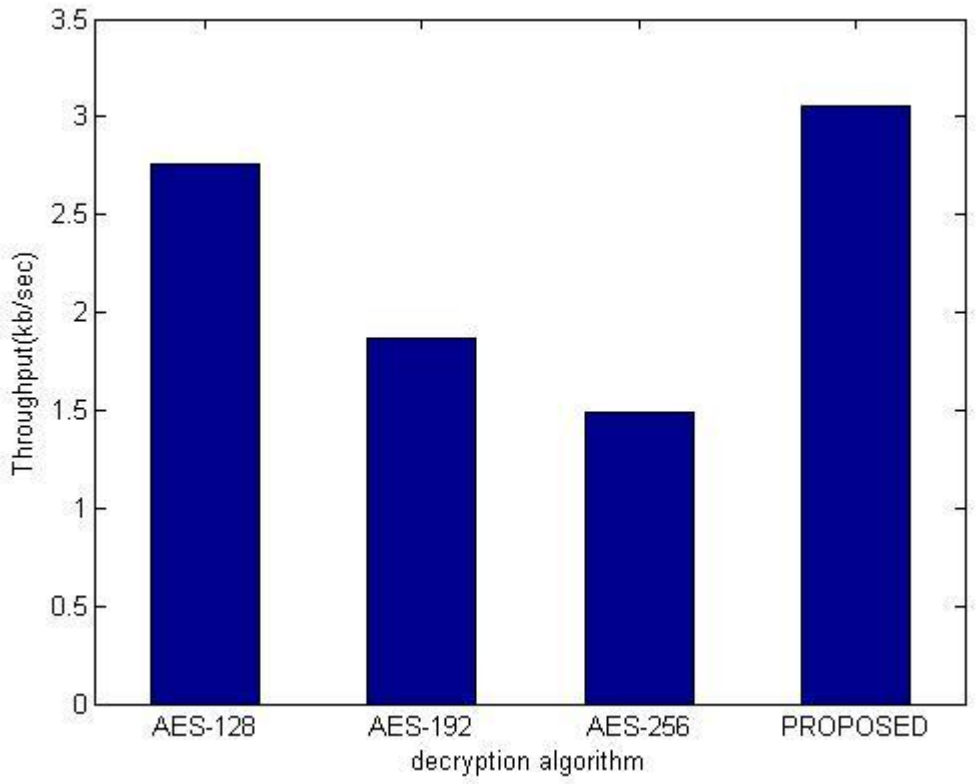

Figure 5.10 Throughput of various decryption algorithms

5.3 Variations of plain-text file Size and cipher-text file Size in KB

Table 5.3 shows the variation of different file sizes of plain-text input file and the corresponding cipher-text file. It has been observed that as the size of input text file increases, the output file size varies linearly. It has also been shown from table 5.3 that

cipher-text file size is larger than the plain-text file. With the help of above table 5.3, the plot of cipher-text file size and plain-text has been drawn for different file size and is shown in figure 5.9.

Table 5.3 variation of plain-text and cipher-text file size

S. No.	Plain text size	Cipher text size
1	50	77
2	60	103
3	100	155
4	256	479
5	320	528
6	700	1337
7	1024	1983

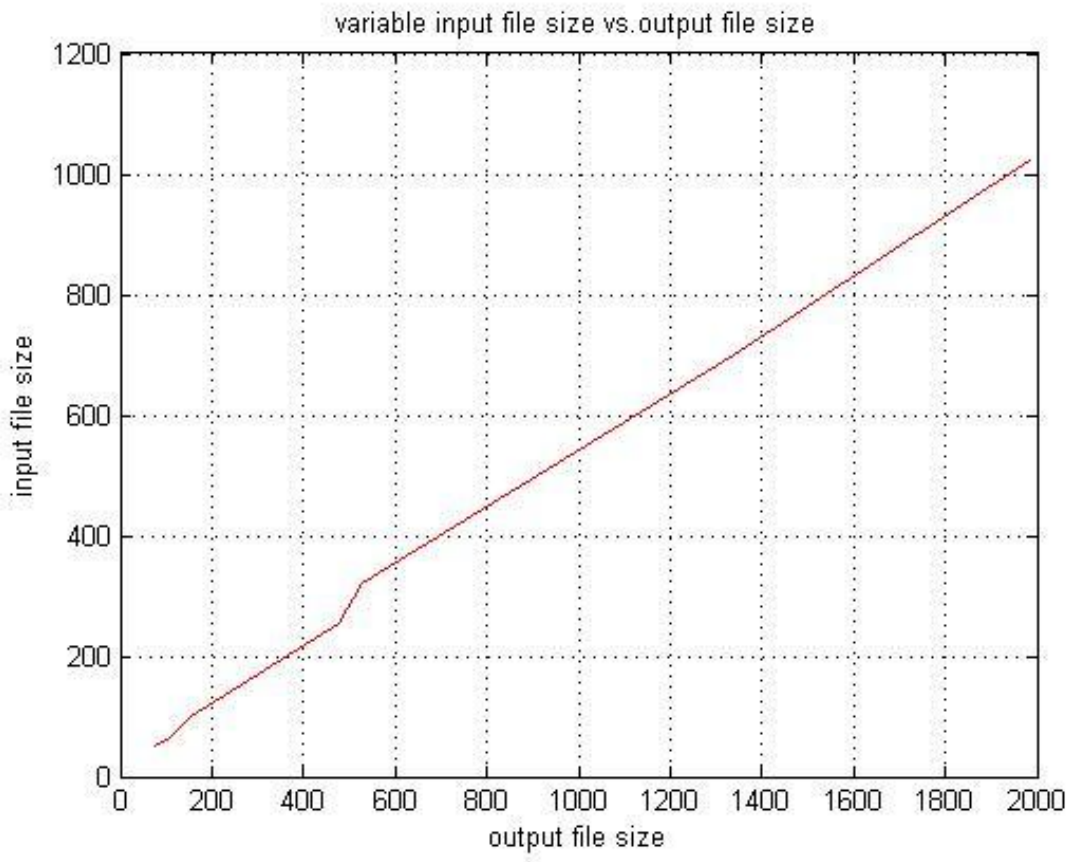

Figure 5.11 File size of cipher and plain text

The figure 5.11 shows the comparison between the file size of plain-text and cipher-text. This plot checks the validity of AES algorithm. It shows that there is an increase in output file size in comparison to the input file size. For input file size of 600KB output file size is 1100KB which indicates that overhead bits required additional space to store the decrypted data.

Chapter 6: Conclusion and Future Scope of Research

The objectives of the thesis have been successfully achieved. Comparative study of various encryption algorithms has also been done. From the Literature Survey; various observations and gaps were reported. Objectives have also been drawn from the observations and gaps. The optimized key management has been successfully achieved using AES which takes less encryption and decryption time for different file sizes. Hence, the time available for the hackers to break the cryptographic model definitely decreases, it increases data security. Simulation results have been achieved using MATLAB 2013. The results clearly highlight that the proposed scheme takes less time as compared with AES algorithm. Finally comparison of our approach with existing AES (128, 192 and 256 key length) has also been done in terms of encryption and decryption time. The work can be further extended by considering the more iteration in the key generation process. The key length can be increased for a better secured model by keeping an eye on the processing time.

References

[1] Daniyal M. Alghazzawi, Syed Hamid Hasan and Mohamed Salim Trigui, "Advanced Encryption Standard – Cryptanalysis Research", *Journal of Cryptology*, vol. 4, no. 1, pp. 3-12, 1991.

[2] Bruce Schneier, "Applied Cryptography", John Wiley and Sons, 2nd Edition, 1996.

[3] Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 5th Edition, 1996.

[4] Data Encryption Standard (DES), Federal Information Processing Standards Publication, FIPS, vol. 46, no. 3, 1999.

[5] M. O. Neill and M.J.B. Robshaw, "Low-cost digital signature architecture suitable or radio frequency identification tags", *IET Computers and Digital Techniques*, vol. 4, no. 7, pp. 14-26, 2000.

[6] Bruce Schneier "Cryptography Secrets and Lies: Digital Security in a Networked World*", Wiley Computer Publishing Inc.,* pp. 90-91, 2000.

[7] Salasiah Sulaiman, "The New Approach of Rijndael Key Schedule", *IEEE Proceedings Information Security*, vol.13, no. 15, pp. 13-20, 2005.

[8] Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location Based Compromise Tolerant Security Mechanisms for Wireless Sensor Networks", *IEEE Transactions Selected Areas in Communications*, vol. 24, no. 2, pp. 1-14, 2006.

[9] Monjur Alam, "An Area Optimized Reconfigurable Encryptor for AES-Rijndael", *IEEE Transactions on Circuits and Systems*, vol. 53, no. 3, pp. 381-386, 2006.

[10] Yukio Mitsuyama, Zaldy Andales, Akao onoye, and Isao Shirakawai, "Burst Mode: A New Acceleration Mode for 128-bit Block Ciphers", *International Journal of Computer Science and its Applications*, vol. 5, no. 12, pp. 1923-1928, May 2006.

[11] Chih-Hsu Yen and Bing-Fei Wu, "Simple Error Detection Methods for Hardware Implementation of Advanced Encryption Standard", *IEEE Transactions on Computers*, vol. 55, no. 6, pp. 213-218, 2006.

[12] Omer K. Jasim Mohammad, Safia Abbas, El-Sayed M. ElHorbaty, "Advanced Encryption Standard Development Based Quantum Key Distribution", *IEEE Transaction on Electronics and Devices*, vol. 53, no. 11, pp. 2816-2823, 2006.

[13] Francesco Buccafurri, Gianluca Lax, "Hardening Digital Signatures against Un-trusted Signature Software", *IEEE Transactions on Cryptography*, vol. 7, no. 2, pp. 2147-2153, 2007.

[14] S. T. Halkidis, N. Tsantalis and A. Chatzigeorgiou, "Architectural Risk Anaylisis of Software Systems Based on Security Patterns", *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 3, pp. 129-142, 2008.

[15] Roohi Banu, Sushma verma, "Fault-Tolerant Encryption for Space Applications", *IEEE Transactions on Aerospace and Electronic Systems*, vol. 45, no. 1, pp. 103-112, Jan 2009.

[16] Xiaojiang Du, "A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks", *IEEE Transactions on Wireless Communications,* vol. 8, no. 3 .pp. 1223-1229 , 2009.

[17] Julita A., Fauziyah S., Azlina O., Mardiana B., Hazura H. and Zahariah A.M., "Online Signature Verification System", *IEEE 5th International Colloquium on Signal Processing and its Applications,* vol. 3, no. 4, pp. 4244-4152 , 2009.

[18] Panagiota Lagou and Gregory Chondrokoukis, "Survey on Non-repudiation: Digital Signature versus Biometrics", *Information Security Journal*, vol. 18, no. 14, pp. 257–266, 2009.

[19] B. Acharya, S. K. Panigrahy, S. K. Patra and G. Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, pp. 663-667, 2009.

[20] Feng Liu and Chuankun Wu ," Step Construction of Visual Cryptography Schemes", *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 27-38, 2010.

[21] Mao-Yin Wang, Chih-Pin Su, Chia-Lung Horng, Cheng-Wen Wu, and Chih-Tsun Huang," Single- and Multi-core Configurable AES Architectures for Flexible Security", *IEEE Transactions on Very Large Scale Integration Systems*, vol. 18, no. 4, pp. 541-552, 2010.

[22] M.Y. Wang and C.W. Wu, "A Mesh Structured Scalable IPsec Processor", *IEEE Transaction on Very Large Scale Integration System*, vol. 18, no. 5, pp. 725-731, 2010.

[23] A. Khalique, K. Singh and S. Sood, " A Password Authenticated Key Agreement Scheme Based on ECC Using Smart Cards", *International Journal of Computer Applications*, Vol. 2, No. 3, pp. 26-30, 2010.

[24] Jing Liu and Bo Yang, "Collusion-Resistant Multicast Key Distribution Based on Homomorphic One-Way Function Trees", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 980-991, 2011.

[25] Y.S. Shiu, S. Y. Chang, H.C. Wu, S. C.H. Huang and H.H. Chen, " Physical Layer Security In Wireless Networks", *IEEE Wireless Communications*, vol. 1, pp. 66-74, 2011.

[26] Lein Harn and Jian Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for secure Communications", *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2372-2379, 2011.

[27] Nadia M.G. AL-Saidi and Mohamad Rushdan Md Said, "Improved digital signature protocol using iterated function systems", *International Journal of Computer Mathematics*, vol. 88, no. 17, pp. 3613–3625, 2011.

[28] Jjude H. moore and Gustavus J. Simmons, "Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys", *IEEE Transactions on Software Engineering*, vol. 13, no. 2, pp. 845-852, 2012.

[29] Amid Jamshidi Jam, Farshid Hossein Nejad, Saman Sabah,, "Analysis of Avalanche Effect on Advance Encryption Standard by using Dynamic S-Box Depends on Rounds Keys", *IEEE Transactions on Very Large Scale Integration Systems*, vol. 20, no. 6, pp. 125-131, 2012.

[30] Abdul Hamid M. Ragab, Nabil A. Ismail, "Enhancements and Implementation of RC6T Block Cipher for Data Security" *IEEE Transaction on Computers Science and Applications*, vol. 7, no. 14, pp. 565-570, 2012.

[31] Zhiguo Wan, Jun'e Liu, and Robert H. Deng," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 743-754, 2012.

[32] Shiva Murthy G, Robert John D'Souza and Golla Varaprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks" , *IEEE Sensors Journal*, vol. 12, no. 10, pp. 2941-2949, 2012.

[33] Ajay Kakkar, M. L. Singh and P. K. Bansal, "Mathematical analysis and simulation of multiple keys and S-Boxes in a multi-node network for secure transmission", *International Journal of Computer Mathematics,* vol. 89, no. 16, pp. 2123-2142, 2012.

[34] Kun Ma, Han Liang and Kaijie Wu, "Homomorphic Property-Based Concurrent Error Detection of RSA: A Countermeasure to Fault Attack", *IEEE Transactions on Computers,* vol. 61, no. 7, pp. 1042-1049, 2012.

[35] B. Liu and B.M. Mass, "Parallel AES Encryption "Engines For Many-Core Processor Arrays", *IEEE Transactions on Computers,* vol. 62, no.3, pp. 536-547, 2013.

[36] T.E. Humphreys, "Detection Strategy For Cryptographic GNSS Anti-spoofing", *IEEE Transactions on Aerospace and Electronic Systems,* vol. 49, no.2, pp. 1073-1090, 2013.

[37] Koji Nuida and Goichiro Hanaoka ," On the Security of Pseudorandomized Information-Theoretically Secure Schemes", *IEEE Transactions on Information Theory*, vol. 59, no. 1, pp. 635-653, 2013.

[38] Peng Xu, Hai Jin ," Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack", *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2266-2278 , 2013.

[39] OBV Ramanaiah: "A Study on Rijndael Algorithm for Providing Confidentiality to Mobile Devices", *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 1162-1169, 2013.

[40] Zahir Zainuddin, "E-Learning Concept Design of Rijndael Encryption Process", *IEEE International Conference on Teaching, Assessment and Learning for Engineering,* vol. 3, no. 8, pp. 875-881, 2013.

[41] Erfaneh Noroozi, Salwani Mohd Daud and Ali Sabouhi, "Secure Digital Signature Schemes Based on Hash Functions", *International Journal of Innovative Technology and Exploring Engineering*, vol. 2, no. 4, pp. 2278-3075, 2013.

[42] SK Hafizul Islam and G.P. Biswas, "Provably secure and pairing-free certificate-less digital signature scheme using elliptic curve cryptography", *International Journal of Computer Mathematics*, vol. 90, no. 11, pp. 2244-2258, 2013.

[43] William Stallings, "Digital Signature Algorithms", *International Journal of Cryptologia*, vol. 37, no. 4, pp. 311-327, 2013.

[44] S. Rashidi, A. Fallah and F. Towhidkhah, "Similarity Evaluation of Online Signatures Based on Modified Dynamic Time Warping", *Applied Artificial Intelligence: An International Journal*, vol. 27, no. 5, pp. 599-617, 2013.

[45] Othman o-khalifa, Md. Khorshed Alam and Aisha Hassan Abdalla, " An Evaluation on Offline Signature Verification using Artificial Neural Network Approach", *International Conference on Computing, Electrical And Electronic Engineering*, vol. 3, no. 8, pp. 213-217, 2013.

[46] Ashok K. Bhateja, Santanu Chaudhury and P. K. Saxena, "A Robust Online Signature based Cryptosystem", *14th International Conference on Frontiers in Handwriting Recognition*, vol. 13, no. 7, pp. 123-129, 2014.

[47] Xinyi Huang, Yang Xiang, Jianying Zhou, and Li Xu, "Robust Multi-Factor Authentication for Fragile Communications", *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 6, pp. 568-581, 2014.

[48] Chun-I Fan, "Arbitrary-State Attribute-Based Encryption with Dynamic Membership", *IEEE Transactions on Computers*, vol. 63, no.8, pp. 1951-1961, 2014.

[49] Xiaofeng Chen, Jianfeng Ma, Qiang Tang, and Wenjing Lou, "New Algorithms for Secure Outsourcing of Modular Exponentiations", *IEEE Transaction on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2386-2396, 2014.

[50] Joseph K. Liu and Man Ho Au ," Linkable Ring Signature with Unconditional Anonymity", *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 1, pp. 157-165 , 2014.

[51] Xinqiang Luo, Yue Qi, Yadong Wan, Qin Wang, "A Fast AES Encryption Method Based on Single LUT for Industrial Wireless Network", *International Conference on Identification, Information and Knowledge in the Internet of Things*, vol. 16, no. 9, pp. 2056-5063, 2014.

[52] Joseph Soryal, Irippuge Milinda perer, Ihab Darwish,Nelly Fazio, Rosario Gennaro, and Tarek Saadawi, "Combating Insider Attacks in IEEE 802.11 Wireless Networks with Broadcast Encryption*", IEEE 28th International Conference on Advanced Information Networking and Applications*, vol. 6, no. 2, pp. 409-415, 2014.

[53] Bassem Bakhache, Joseph M. Ghazal, and Safwan El Assad, "Improvement of the Security of ZigBee by a New Chaotic Algorithm", *IEEE Systems Journal*, vol. 8, no. 4, pp. 563-569, 2014.

[54] Hassan Noura, Steven Martin, Khaldoun Al Agha: "EDCA: Efficient Diffusion Cipher and Authentication Scheme for Wireless Sensor Networks", *IEEE Transactions on Computer Networks and Science*, vol. 14, no. 8, pp. 1220-1235, 2014.

[55] Walid Y. Zibideh "An Optimized Encryption Framework based on the Modified-DES Algorithm: A Trade-Off between Security and Throughput in Wireless Channels", *IEEE Transaction Signal Process*, vol. 48, no. 5, pp. 1338-1353, 2014.

[56] Jinguang Han, "Identity-Based Secure Distributed Data Storage Schemes", *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 6, pp. 568-581, 2014.

[57] Joan Arnedo, "A secure communication setup for peer to peer communications", *IET Computers and Digital Techniques*, vol. 6, no. 9, pp. 18-22, 2014.

[58] Kirtiraj B hatele, "Design of new hybrid security protocol architecture for online transaction", *International Journal of Computer Mathematics*, vol. l. 92, no. 7, pp. 1313-1328, 2014.

[59] V.A.Suryawanshi, "Area-High Speed Design Trade-Offs for Advanced Encryption Standard Cipher Engine", *International Conference on Nascent Technologies in the Engineering Field*, vol. 41, no. 29, pp. 203- 216, 2015.

[60] Gianluca Lax, Francesco Buccafurri and Gianluca Caminiti, "Digital Document Signing: Vulnerabilities and Solutions", *Information Security Journal*, vol. 3, no. 6, pp. 1-14, 2015.

[61] N.Mehrav and E.Arikan, "The Shannon cipher system with a guessing wiretapper", *IEEE Transaction Signal Process*, vol. 45, no. 6, pp. 1860-1866, 1999.

[62] J. Daemen and V. Rijmen, "AES Proposal: Rijndael", AES Algorithm Submission, September 3, 1999.