Cryptography Algorithms and approaches used for data security

Gaurav Sharma
Research Scholar
Thapar University, Patiala

Ajay Kakkar
Asstt. Prof.
Thapar University, Patiala

Abstract:
In separate used systems, the computers are exposed to the other users. To keep the data secured from different users various encryption algorithms are entered. As computer systems become more pervasive and complex, security is increasingly important. Cryptographic algorithms and protocols constitute the central component of systems that protect network transmissions and store data. Encryption is the translation of data to a secret code. Apart from its uses in Military and Government to facilitate secret communication, Encryption is used in protecting many kinds of civilian systems such as Internet e-commerce, Mobile networks, automatic teller machine transactions, copy protection (especially protection against reverse Engineering and Software piracy), and many more. The Encrypted data can only be deciphered if one has the password or the Key. The Encryption algorithm is a set of well defined steps to transform data from a readable format to an encoded format using the Key. This set of well defined steps is also called cipher.

Key words: encryption, keys, authenticate, user.

1. Introduction
Security attacks against network are increasing significantly with time. Our communication media should also be secure and confidential. Cryptanalysis is the study used to describe the methods of code-breaking or cracking the code without using the security information, usually used by hackers. For this purpose, these three suggestions arrive in every one's mind: (i) one can transmit the message secretly, so that it can be saved from hackers, (ii) the sender ensures that the message arrives to the desired destination, and (iii) the receiver ensures that the received message is in its original form and coming from the authenticate person. In order to achieve the same one can use two techniques, (i) one can use invisible ink for writing the message or can send the message through the confidential person, and (ii) use of scientific approach called "Cryptography". Cryptography is the technique used to avoid unauthorized access of data. Data can be encrypted using a cryptographic algorithm by various keys. It will be transmitted in an encrypted state, and later decrypted by the intended party. If a third party intercepts the encrypted data, it will be difficult to decipher. The security of modern cryptosystems is not based on the secrecy of the algorithm, but on the secrecy of a relatively small amount of information, called a secret key. The fundamental and classical task of cryptography is to provide confidentiality by encryption methods. It is used in applications present in technologically advanced societies; it includes the security of ATM cards, computer passwords, and electronic commerce. For secured communication between two parties following points are considered:

Plaintext: the original message or data that is in readable form is known as plain-text.
Ciphertext: the encoded message with the help of keys is known as cipher-text.
Encryption: the process to convert the original message into coded form with the help of key, i.e., plain-text into cipher-text is known as encryption.
Decryption: the reverse process of encryption, i.e., to convert cipher-text into plain-text with the help of key is known as decryption.

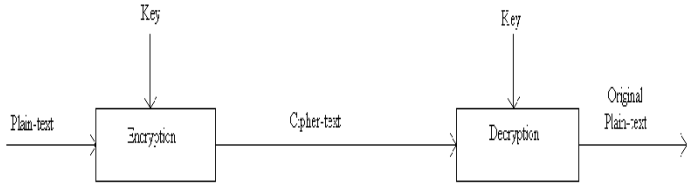


Figure 1: Symmetric cryptography [1]

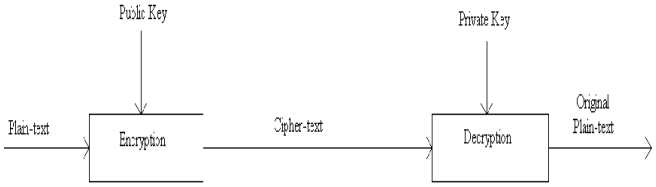


Figure 2: Asymmetric cryptography [1]

1.2 Motivation
An encryption algorithm provides Confidentiality, Authentication, Integrity and Non-repudiation. Confidentiality ensures that the information is accessible to only authorized set of people. Authentication is the act of establishing that the algorithm is genuine. Integrity in general means completeness but in encryption it is adhering to some set of principles. It is based on consistency with some mathematical proof. Non-repudiation in cryptology means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively.

In separate used systems, the computers are exposed to the other users. To keep the data secured from different users various encryption algorithms are entered. As computer systems become more pervasive and complex, security is increasingly important. Cryptographic algorithms and protocols constitute the central component of systems that protect network transmissions and store data. Encryption is the translation of data to a secret code. Apart from its uses in Military and Government to facilitate secret communication, Encryption is used in protecting many kinds of civilian systems such as Internet e-commerce, Mobile networks, automatic teller machine transactions, copy protection

(especially protection against reverse Engineering and Software piracy), and many more. The Encrypted data can only be deciphered if one has the password or the Key. The Encryption algorithm is a set of well defined steps to transform data from a readable format to an encoded format using the Key. This set of well defined steps is also called cipher. An encryption algorithm provides Confidentiality, Authentication, Integrity and Non-repudiation. Confidentiality ensures that the information is accessible to only authorized set of people. Authentication is the act of establishing that the algorithm is genuine. Integrity in general means completeness but in encryption it is adhering to some set of principles. It is based on consistency with some mathematical proof. Non- repudiation in cryptology means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively.

In today's digital world, encryption is emerging as a disintegrable part of all communication networks and information processing systems, for protecting both stored and in transit data. Encryption is the transformation of plain data (known as plaintext) into unintelligible data (known as ciphertext) through an algorithm referred to as cipher. There are numerous encryption algorithms that are now commonly used in computation, but the U.S. government has adopted the Advanced Encryption Standard (AES) to be used by Federal departments and agencies for protecting sensitive information. The National Institute of Standards and Technology (NIST) has published the specifications of this encryption standard in the Federal Information Processing Standards (FIPS) Publication 197.

The security of such systems greatly depends on the methods used to manage, establish, and distribution of keys the keys used by the cryptographic techniques. Even if a cryptographic algorithm is ideal in both theory and implementation, the strength of the algorithm will be rendered useless if the relevant keys are poorly managed. Cryptography is the art and science behind the principles, means, and methods for keeping messages secure. Cryptanalysis is a study of how to compromise cryptographic mechanism. There are two classes of key-based encryption algorithms: symmetric and asymmetric algorithms. Symmetric algorithms use the same key for encryption and decryption, whereas asymmetric algorithms use different keys for encryption and decryption. Ideally it is infeasible to compute the decryption key from the encryption key.

1.3 Applications

Cryptography is used to achieve the following goals:

1.3.1 Confidentiality:
It is the protection against unauthorized disclosure of information. Confidentiality may be applied to whole messages, parts of messages, and even existence of messages [9]. Confidentiality is the protection of transmitted data from passive attacks.

1.3.2 Authentication:
The authentication service is concerned with assuring that a communication is authentic. It is the corroboration of the claimed source of a message. Authentication is of two types: (i) Peer entity, and (ii) Data origin

1.3.3 Data integrity:
The integrity can apply to a stream of messages, a single message, or selected fields within a message. It assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service.

1.3.4 Access control:
It is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

1.3.5 No repudiation:
No repudiation prevents either sender or receiver from denying a transmitted message. When a message is sent, the receiver can prove that the alleged sender in fact sent the message.

2. Cryptography

Cryptography is defined as the conversion of plain text into cipher text with help of key is known as cryptography. There are two main processes in the cryptography, named as encryption and decryption. In the encryption process the key has been used to convert the plain text into cipher text[11]. The key may be any word or value and is known to only sender and receiver. The key should be kept secure from the hacker; as the key is the main parameter if gets hacked then the encryption algorithm must generate the new key immediately.

Cryptography systems are characterized along three independent dimensions:
The type of operation used for transforming plaintext to cipher text.
The number of keys used.
The way in which the plaintext is processed.

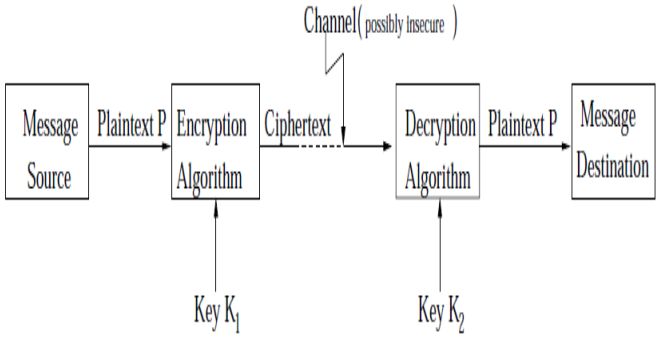


Figure 3: Cryptosystem [2]

2.1 Cryptography Definitions

Algorithm Set of mathematical rules used in encryption and decryption. Cryptography Science of secret writing that enables you to store and transmit data in a form that is available only to the intended individuals. Cryptosystem Hardware or software implementation of cryptography that transforms a message to ciphertext and back to plaintext. Cryptanalysis Practice of obtaining plaintext from ciphertext without a key or breaking the encryption. Cryptology The study of both cryptography and

cryptanalysis. Ciphertext Data in encrypted or unreadable format. Encipher Act of transforming data into an unreadable format. Decipher Act of transforming data into a readable format. Key Secret sequence of bits and instructions that governs the act of encryption and decryption. Key clustering Instance when two different keys generate the same ciphertext from the same plaintext[6,7]. Key space Possible values used to construct keys. Plaintext Data in readable format, also referred to as clear text. Work factor Estimated time, effort, and resources necessary to break a cryptosystem.

2.2 Key Management

Cryptography can be used as a security mechanism to provide confidentiality, integrity, and authentication, but not if the keys are compromised in any way. The keys have to be distributed to the right entities and updated continuously. The keys need to be protected as they are being transmitted and while they are being stored on each workstation and server. The keys need to be generated, destroyed, and recovered properly. Key management can be handled through manual or automatic processes. The frequency of use of a cryptographic key can have a direct correlation to how often the key should be changed. The more a key is used, the more likely it is to be captured and compromised[8,10]. Keeping keys secret is a challenging task. Keys should not be in clear-text outside the cryptography device

Rules for keys generation and their handling:

1. The key length should be of variable size for the highly secure communication.
2. Keys should be randomly selected by using the full spectrum of available key-space.
3. Multiple use of keys leads to short lifetime.
4. Keys should be properly destroyed when their lifetime is over.
5. For the secure communication, the keys are to be kept secret.

3. Cryptography Techniques

There are two techniques used for data encryption and decryption, which are:

Symmetric Cryptography:

Symmetric encryption is also referred as 'conventional encryption' or 'single key' encryption. The symmetric encryption is referred as if both sender and receiver both use same key or secret key is known as symmetric encryption.

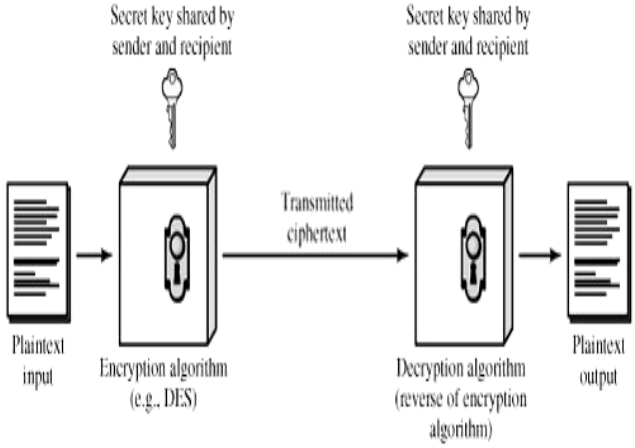


Figure 4: Simplified Model of Conventional Encryption [3].

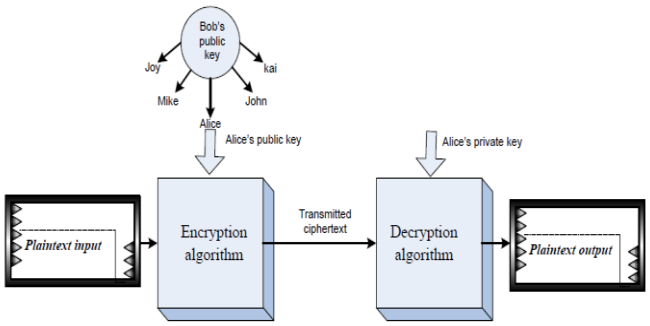
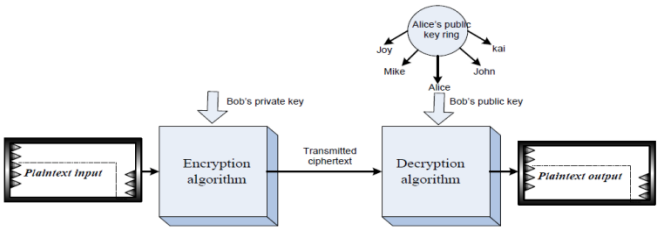


Figure 5 (a): Asymmetrical Cryptography [12]



(b)

Figure 5 (b): Asymmetrical Cryptography [12]

Summary of comparison

Public-key cryptography facilitates efficient signatures (particularly nonrepudiation) and key management, and Symmetric-key cryptography is efficient for encryption and some data integrity applications.

4. Digital Signatures

Public key cryptography gives a major benefit by providing a method for employment of digital signatures. Digital signatures and hand-written signatures both rely on the fact that it is very hard to find two people with the same signature. The authentication and data integrity are the two features of digital signatures by providing a seal over a document or a handwritten signature[13]. Anyone with access to the public key of the signer may verify the signature. For example, in the field of E-commerce, an instruction to your bank to transfer money can be authenticated with a digital signature. Digital signatures cannot be copied to another document.

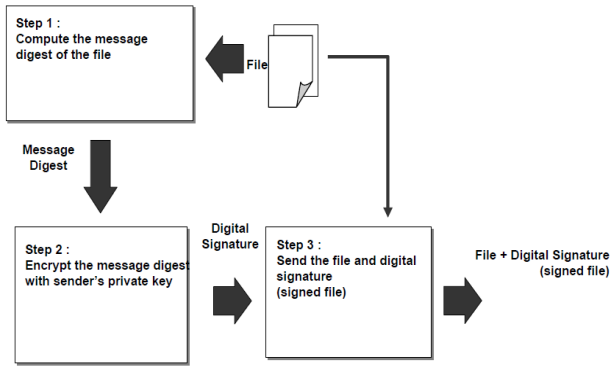


Figure 6: Steps for digital signature generation [4]

The steps for the digital signature generation are as follows:

1) The message digest of the plain-text is computed, i.e., what type of data is - text, video, image, etc. and what is the length of the data is, etc.
2) This message digest will be encrypted using key techniques and a digital signature is also attached before sending to the receiver.
3) The encrypted plain-text (including plain-text and digital signature) is sent to the receiver.

5. Ciphers & their types

Substitution Cipher
It is the one in which the letter of plaintext are replaced by other letter or by numbers or symbols such process are known as substitution techniques[16]. There is various substitution techniques are as follows:
Caser Cipher: It has been discovered by JULIUS CASER. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Plain text: My Name is Gaurav
Cipher text: - Ob Qdoh lv Jdxudy

One can be able create their own algorithm by selecting the key. e.g. same data has been encrypted by using R5 (shifting of data by 5 bits towards right)

Plain text: My Name is Gaurav
Cipher text: - Rd Serj nx Lezwea

Transposition Cipher
In the transposition techniques are very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred as transposition ciphers. The simplest such cipher is the rail fence techniques in which plaintext is written in diagonal and then read off as a sequence of rows. In a transposition cipher, permutation is used, meaning that letters are scrambled. The key determines the positions that the characters are moved to, as illustrated in Figure 7. This is a simplistic example of a transposition cipher and only shows one way of performing transposition. Most ciphers used today use long sequences of complicated substitutions and permutations together on messages. The key value is inputted into the algorithm and the result is the sequence of operations (substitutions and permutations) that are performed on the plaintext. Simple substitution and transposition ciphers are vulnerable to attacks that perform frequency analysis. These patterns help attackers figure out the transformation between plaintext to ciphertext, which enables them to figure out the key that was used to perform the transformation.

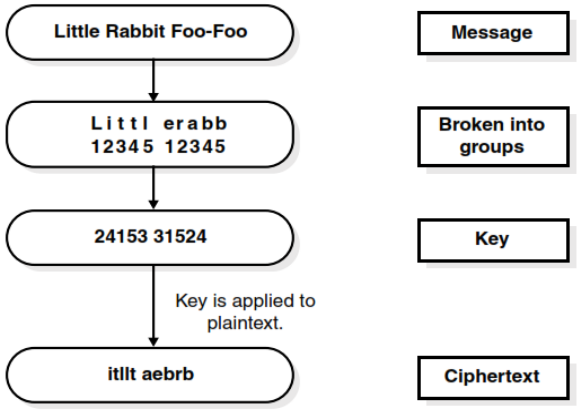


Figure 7. Transposition cipher [5]

It is important for cryptosystems to not reveal these patterns. More complex algorithms usually use more than one alphabet for substitution and permutation, which reduces the vulnerability to frequency analysis. The more complicated the algorithm, the more the resulting text (ciphertext) differs from the plaintext; thus, the matching of these types of patterns becomes more difficult.

Plain text: - I am the student of m-tech.
I m h s u e t f t c
A t e t d n o m e h
Cipher text: - imhsuetftcatetdnomeh.

6. DES (Data Encryption Standard)

Data Encryption Standard (DES) is a cryptographic standard that was proposed as the algorithm for secure and secret items in 1970 and was adopted as an American federal standard by National Bureau of Standards (NBS) in 1973. It is one of the most widely accepted, publicly available cryptographic systems today. It was developed by IBM in the 1970s but was later adopted by the US government as a national standard DES is a block cipher, which means that during the encryption process, the plain-text is broken into fixed length blocksand each block is encrypted at the same time[17]. Basically it takes a 64 bit input plain text and a key of 64-bits (only 56 bits are used for conversion purpose and rest bits are used for parity checking) and produces a 64 bit cipher text by encryption and which can be decrypted again to get the message using the same key. The simplified DES is shown in Fig. 8.

6.1 Working Principle of DES:

DES uses a 56-bit key. In fact, the 56-bit key is divided into eight 7-bit blocks and an 8th odd parity bit is added to each block (i.e., a "0" or "1" is added to the block so that there is an odd number of 1 bits in each 8-bit block). [6]By using the 8 parity bits for rudimentary error detection, a DES key is actually 64 bits in length for computational purposes (although it only has 56 bits worth of randomness, or entropy).

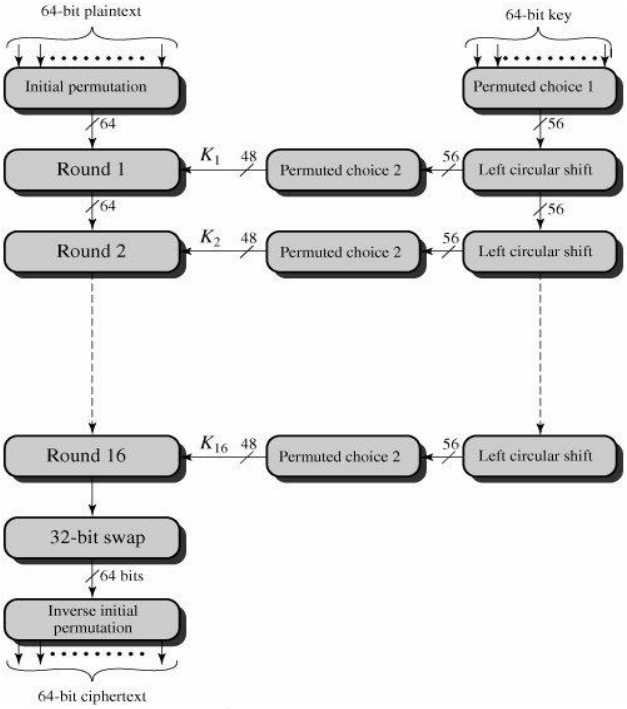


Figure 8: Simplified DES Encryption Algorithm [1]

DES then acts on 64-bit blocks of the plaintext, invoking 16 rounds of permutations, swaps, and substitutes, as shown in Figure 3.2. The standard includes tables describing all of the selection, permutation, and expansion operations mentioned below; these aspects of the algorithm are not secrets. The basic DES steps are:

1) The 64-bit block to be encrypted undergoes an initial permutation (IP), where each bit is moved to a new bit position; e.g., the 1st, 2nd, and 3rd bits are moved to the 58th, 50th, and 42nd position, respectively.

2) The 64-bit permuted input is divided into two 32-bit blocks, called left and right, respectively. The initial values of the left and right blocks are denoted L0 and R0.

3) There are then 16 rounds of operation on the L and R blocks. During each iteration (where n ranges from 1 to 16), the following formulae apply:

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} XOR\ f(R_{n-1}, K_n)$$

At any given step in the process, the new L block value is merely taken from the prior R block value. The new R block is calculated by taking the bit-by-bit exclusive-OR (XOR) of the prior L block with the results of applying the DES cipher function, f, to the prior R block and Kn. (Kn is a 48-bit value derived from the 64-bit DES key. Each round uses a different 48 bits according to the standard's Key Schedule algorithm).

The cipher function, f, combines the 32-bit R block value and the 48-bit sub key in the following way. First, the 32 bits in the R block are expanded to 48 bits by an expansion function (E); the extra 16 bits are found by repeating the bits in 16 predefined positions. The 48-bit expanded R-block is then XORed with the 48-bit subkey. The result is a 48-bit value that is then divided into eight 6-bit blocks. These are fed as input into 8 selection (S) boxes, denoted S1,..., S8. Each 6-bit input yields a 4-bit output using a table lookup based on the 64 possible inputs; this results in a 32-bit output from the S-box. The 32 bits are then rearranged by a permutation function (P), producing the results from the cipher function.

(4) The results from the final DES round — i.e., L16 and R16 — are recombined into a 64-bit value and fed into an inverse initial permutation (IP-1). At this step, the bits are rearranged into their original positions, so that the 58th, 50th, and 42nd bits, for example, are moved back into the 1st, 2nd, and 3rd positions, respectively. The output from IP-1 is the 64-bit cipher text block.

7. International Data Encryption Algorithm (IDEA)

It is a block cipher designed by James Massey and Xuejia Lai and was first described in 1991.It is a block cipher and operates on 64-bit blocks of data. The key is 128 bits long. The 64-bit data block is divided into 16 smaller blocks and each has eight rounds of mathematical functions performed on it.

It offers different modes similar to the modes described in the DES section, but it is much harder to break than DES. IDEA is used in the PGP encryption software. It was thought to replace DES, but it is patented, meaning that licensing fees would have to be paid to use it.

8. Advanced Encryption Standard (AES)

The AES algorithm is a symmetric cipher[14]. In symmetric ciphers, a single secret key is used for both the encryption and decryption, whereas in asymmetric ciphers, there are two sets of keys known as private and public keys.

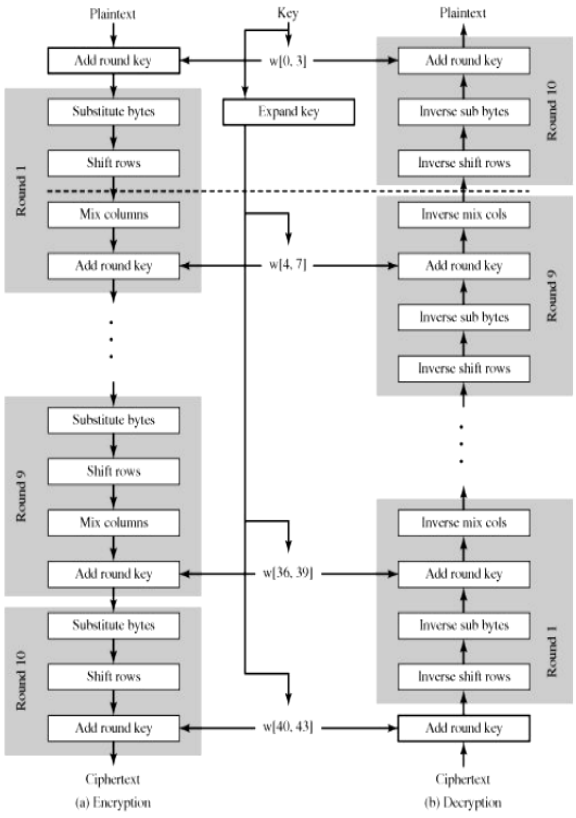


Figure 9: Structure of the AES algorithm [8]

The plaintext is encrypted using the public key and can only be decrypted using the private key. In addition, the AES algorithm[16] is a block cipher as it operates on fixed-length groups of bits (blocks), whereas in stream ciphers, the plaintext bits are encrypted one at a time, and the set of transformations applied to successive bits may vary during the encryption process. The AES algorithm operates on blocks of 128 bits, by using cipher keys with lengths of 128, 192 or 256 bits for the encryption process. Although the original Rijndael encryption algorithm was capable of processing different blocks sizes as well as using several other cipher key lengths, but the NIST did not adopt these additional features in the AES [2-5,15]

Conclusion and Future Scope

The study of various encryption algorithms and the concept of keys have been successfully observed. From the observation it has been observed that by increasing the key length better secured system can be achieved. Longer key lengths consume more power and dissipate more heat. Basically it is a trade off between security and overheads. In order to achieve more secured system continuous efforts are required. An efficient encryption algorithm should consist of two factors – fast response and reduced complexity. A proposed direction for the future work could be to analyze the performance/security trade-off in greater depth. For instance, an algorithm with more complex rounds and a larger number of rounds is generally considered more secure. The impact of these and other such factors on the overall performance of an algorithm needs to be measured. The work can be extended if more number of keys are used for the encryption process and then implemented on DSP kits in order to determine the value various factors such as power consumption and heat dissipation.

References:

[1] Cryptography and Network Security Principles and Practices, Fourth Edition, By William Stallings.
[2] Classification of IDEA and RSA ciphers, by M. Brahmji Rao,phd thesis,IIT Kanpur
[3] Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi, Peformance Analysis Of Data Encryption Algorithms, O P Verma, 2011 IEEE.
[5] CISSP All-in-One Certification Exam Guide200075_ch08_HarrisX 11/30/01 10:22 AM Page 495
[6] National Bureau of Standards – Data Encryption Standard, FIPS Publication 46, 1977.
[7] www.schneier.com/paper-twofish-fpga.pdf
[8] NIST Advanced Encryption Standard (AES), Development Effort web site http://csrs.nist.gov/encryption/aes/aes-home.htm

[9] C. Boyd. "Modern Data Encryption," Electronics & Communication Engineering Journal,
October 1993, Vol. 5, pp 271-278
[10] G.Gong and A. Hasan, "An Efficient Algorithm for Exponentiation in DH Key Exchange and DSA in Cubic Extension Fields", Faculty of Mathematics, University
[11]Xin Zhou ; Xiaofei Tang, Research and implementation of RSA algorithm for encryption and decryption, Strategic Technology (IFOST), 2011 6th International Forum.
[12] Cong Chen, Xiangyu Li, Liji Wu, Xiangmin Zhang, Design and implementation of a Differential Power Analysis System for cryptographic devices, 10th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT), pp.1967 – 1969, 2010.
[13] R. L. Rivest, "The RC5 Encryption Algorithm, in Practical Cryptography for Data Internetworks" IEEE Computer Society Press, 1996.
[14] National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, CNSS Policy No.1, Fact Sheet No. 1, June 2003.
[15] Federal Information Processing Standards Publication (FIPS 197), Advanced Encryption Standard (AES), Nov. 26, 2001.
[16] M. Mozaffari-Kermani, A. Reyhani-Masoleh, A low-cost S-box for the Advanced Encryption Standard using normal basis, IEEE International Conference on Electro/Information Technology, pp. 52 – 55, 2009.
[17] D. Coppersmith "The Data Encryption Standard (DES) and Its Strength against Attacks", IBM Journal of Research and Development, No.5, 1994.