A Literature Survey on the Cryptographic Encryption Algorithms for Secured Data Communication

Sreeparna Chakrabarti
Research Scholar,
Visvesvaraya Technological University,
Belagavi, India.

Dr. G.N.K. Suresh Babu
Professor, Department of Computer Applications,
Acharya Institute of Technology,
Bangalore, India

Abstract :- Security has become a buzzword over the current years. As per Wikipedia, 55.1% of global population has internet access (June 2018). Hence, it is obvious that huge volume of data is exchanged among the users over the internet. As a result, everybody is worried about data security while transmission of any confidential data. In this proposed paper, several cryptographic algorithms are discussed based on concepts of encryption and decryption. Cryptography algorithms provide the mechanisms necessary to implement accountability, accuracy and confidentiality in secured communication. This is further preceded with the widespread adoption of secure protocols such as secure Internet Protocol and virtual private networks. Efficient cryptographic processing, therefore, will become increasingly vital to good system improvement results. Cryptographic algorithms provide many key building block for network security related services. Cyber attacks (intrusion) were up 44% globally during Q1 2018, and the speed of attacks continues to increase exponentially. 75% of organizations have experienced a breach, but only 25–35% believes they are equipped to deal with these intrusions effectively.

Keywords : *Cryptography, Encryption, Decryption, IoT, Intrusion, Attacks*

*****

I. Introduction

Cryptography has had an interesting history and has undergone many changes through the centuries. It seems that keeping secrets has been important throughout the ages of civilization for one reason or another. Keeping secrets gives individuals or groups the ability to hide true intentions, gain a competitive edge, and reduce vulnerability. The changes that cryptograph has undergone throughout history closely follow the advances in technology. Cryptography methods began with a person carving messages into wood or stone, which were then passed to the intended individual who had the necessary means to decipher the messages. This is a long way from how cryptography is being used today. Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text. Cryptography is a technique of hiding the plain information from the web. By using cryptography we can assist this shaky information by secrete writing on our computer network. Cryptography renders the message unintelligible to outsider by various transformations. Information that are disseminated within an office, across offices, between branches, of an organization and other external bodies and establishments at times get into the hands of the unauthorized persons who may tamper with the contents of the information. And if no security measures are taken, there is no doubt that such data and other sensitive information will be exposed to threats such as impersonation, insecrecy, corruption, repudiation, break-in or denial of services that may cause serious danger on the individual or organization. A secure system should maintain the integrity, availability, and privacy of data. Data integrity usually means protection from unauthorized modification, resistance to penetration and protection from undetected modification. Therefore, algorithms which help prevent interception, modification, penetration, disclosure and enhance data/information security are now of primary importance. This is to ensuring that the intruders do not have access to the plaintext without a secret key. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric schemes, one key is used for encryption and another is used for decryption. The increased confidence in the integrity of systems that use encryption is based on the notion that cipher text should be very difficult to decipher without knowledge of the key. Fig.1 explains the process about how the plain text converting into encrypted data and encrypted data converted into plain text using decryption algorithm.

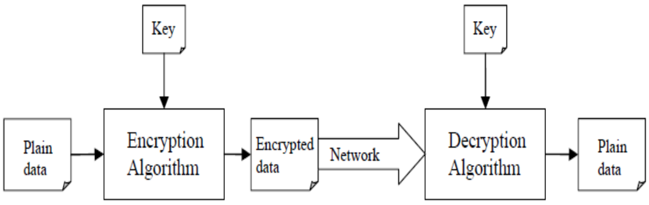

Fig.1 – Basic process of Cryptography

II. OVERVIEW OF CRYPTOGRAPHY

Modern cryptography can be divided into two main subfields of study: Symmetric-key and Asymmetric-key cryptography. Symmetric-key can be divided into block ciphers and stream ciphers. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and their applications.

Asymmetric-key cryptography is also known as public-key cryptography whereby two different but mathematically related keys are used. A public key and a private key. A public-key system is so constructed that calculation of one key from the other is computationally infeasible, even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. The public key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption. The most famous applications of public-key cryptography are Elliptic-curve cryptography, PGP and the public-key infrastructure (PKI). Elliptic Curve Cryptography (ECC) provides the highest strength-per-key-bit of any cryptography algorithm known to take. Compared with other public-key approaches, ECC not only has the higher security but also has lows computation overhead, shorter key size and narrower bandwidth. Therefore, the experts believe that ECC will become the next generation widely used public-key cryptography.Pretty Good Privacy (PGP) is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting and decrypting e-mails to increase the security of e-mail communication.A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. Fig.2 represents overview of cryptography.

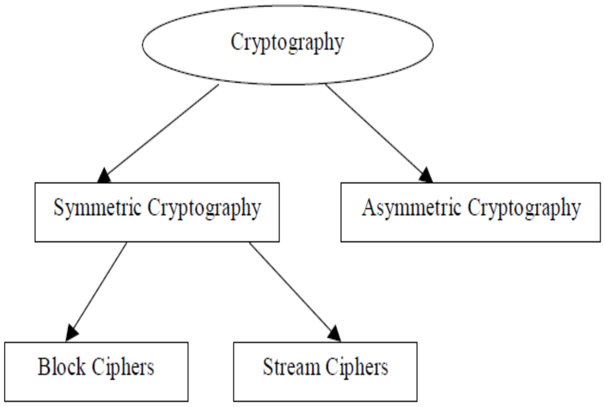

Fig.2 Overview of Cryptography

1.1 Security Service Methods

- **Authentication:** This service involves the authentic communication .It also ensures the genuineness of user. This service not only monitors the initial stage but also take care of throughout the session.
- **Access Control:** This service starts once authentication process is over. This service mainly takes care of controlling /limiting in network.
- **Data Confidentiality:** this service protects the data from passive attacks. This service monitors contents of data and the packets where they are going to and coming from.
- **Data Integrity:** The main purpose of this service is to detect when data has been altered in transit.
- **Non-repudiation:** This service prevents the sender and receiver form denying sending a message.

1.2 Vulnerabilities

- Wiretapping
- Impersonation(IP-Spoofing)
- Message confidentiality violations
- Message integrity violations
- Code integrity violations
- Denial of service (DOS)

1.3 Attacks

Vulnerabilities are also called threats because the risk of their being exploited exists. A threat becomes an attack once the dreaded has occurred. There is countless number of attacks. Some of them are:

- **Masquerade:** Pretending to be someone, they are not. It is an attack on authentication and data integrity.
- **Bypassing:** Controls circumventing access control.
- **Authorization violation:** Circumventing both authorizing and access control.
- **Trojan horse:** A program that has covert activity beyond what it appears to be doing. This attack makes all security services get compromised.
- **Trapdoor**: A program that has a secret entry point. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography, which is the focus of this chapter. But it is important to note that while cryptography is *necessary* for secure communications, it is not by itself *sufficient*. The reader is advised, then, that the topics covered in this chapter only describe the first of many steps necessary for better security in any number of situations.

III. CRYTOGRAPHY APPLICATIONS

Cryptography can be applied anywhere in TCP/IP stack. It is widely used for data confidentiality. All the security services would not be possible to offer anything without cryptography, no doubt. Cryptography is also used in complicated protocols that help to achieve different security services. Some of the mechanisms are:

- **Encryption:** used heavily to accomplish all security services

- **Access control mechanism**: commonly access control list (ACL) or used capability list (UCL)
- **Data integrity mechanism:** this mechanism aims at detecting the passive attacks in transit.
- **Authentication exchanges**: this mechanism to realize authentic communication. In client server model, this includes various handshaking protocols and also includes the digital signature.
- **Traffic padding**: a technique that aids in data confidentiality

3.1 Cryptography based protocols

- **SSL** It creates secure tunnel to create a secure channel for exchange of arbitrary data
- **SSH** Similar to SSL, It uses an encrypted tunnel for exchange of data that can be used as a transport layer for other non-secure protocols
- **Kerberos** Complex protocol used in open distributed system to provide mutual authentication for both the client and server.
- **SET** Designed to protect credit card transaction over internet
- **PGP** Used for encrypting the content of an email inside a regular SMTP email with the use of asymmetric for convenient key exchange.

Fig.3 represents a overview of cryptography protocols

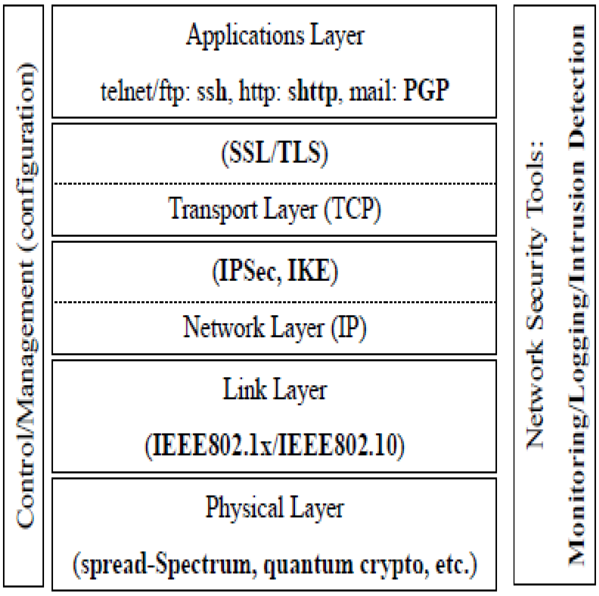
Control/Management (configuration)
Applications Layer
telnet/ftp: ssh, http: shttp, mail: PGP
(SSL/TLS)
Transport Layer (TCP)
(IPSec, IKE)
Network Layer (IP)
Link Layer
(IEEE802.1x/IEEE802.10)
Physical Layer
(spread-Spectrum, quantum crypto, etc.)
Network Security Tools:
Monitoring/Logging/Intrusion Detection

Fig.3 Cryprography Protocols

IV. SURVERY OF ENCRYPTION ALGORITHMS

1. *Data Encryption Standard (DES):* This SKC scheme is the most frequent in present scenario. DES was planned by IBM around 50 years ago and followed by the National Bureau of Standards (NBS) for profitable and uncategorized government projects. DES comes under the category of block-cipher. It uses a 56-bit key which works on 64-bit blocks. There is a complex bunch of protocols designed specifically to defer speedy hardware and sluggish software implementations. The speed of software implementation has less significance in current world because the speed of processors is multiple times more today than a decade ago. IBM also projected a 112-bit key for DES, but that was unfortunately discarded by the government. DES is distinct in "American National Standard X3.92" and three "Federal Information Processing Standards (FIPS)". Two vital types that increase the power of DES are:

   - *Triple-DES (3DES):* This variant of DES employs up to three 56-bit keys and makes three encryption/decryption passes over the block; 3DES is also described in FIPS 46-3 and is the recommended replacement to DES.
   - *DESX:* In this variant 64 additional key bits are mixed to the plaintext before encryption, which increases the keylength to 120 bits.

2. *Advanced Encryption Standard (AES):* 1997 saw the starting of a public, 4-1/2 year method to build up a novel and safe cryptosystem wished-for U.S. government applications by NIST. The resultant "Advanced Encryption Standard", turned out to be the authorized descendant to DES in December 2001. AES makes use of an SKC based block cipher called Rijndael. The algorithm utilizes a changeable *block* length and key length. The newest version permits any blend of keys of lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits. NIST originally chose Rijndael in 2000 and official acceptance as the AES standard occurred in December 2001.

   a) *CAST-128/256:* CAST-128, as defined in Request for Comments (RFC) 2144, is a substitution-permutation crypto algorithm similar to DES, using a 128-bit key operating on a 64-bit block. CAST-256 is an extension of CAST-128, using a 128-bit block size and a key length from (128, 160, 192, 224, or 256 bit). CAST-256 is among one of the first round algorithms in the AES progression.

   b) *International Data Encryption Algorithm (IDEA):* Private-key cryptosystem penned down by Xuejia Lai and James Massey and patented by Ascom. It is a 64-bit SKC block cipher that makes use of a 128-bit key.

   c) *Rivest Ciphers* (aka *Ron's Code):* The algorithm received its name from Ron Rivest, a sequence of SKC algorithms:

   RC1: Only documented but never applied.

RC2: A 64-bit block cipher which works via keys designed to substitute DES. The sizes of the keys are not fixed. RC2's conventions are restricted to private use, though multiple companies have accredited RC2 for use in their goods.

RC3: Noticed to be decodable while growth.

RC4: A stream cipher that makes use of keys whose sizes are not fixed. It is profusely used in marketable cryptography stuffs, though rule says that in exportable products keys of length 40 bits or less can be used.

RC5: A block-cipher that has a range of block sizes, key sizes, and number of encryption passes over the data.

RC6: An improved version of RC5, RC6 came under AES Round 2 algorithms.

d) *Blowfish:* This "symmetric 64-bit block cipher" was invented by Bruce Schneier. At a later stage, it was made more efficient for 32-bit processors via huge data caches. It is noticeably swifter than DES on a Pentium/PowerPC system. Key lengths can range from 32 to 448 bits in length. Blowfish is accessible without any cost and is applied on over 80 products.

e) *Twofish:* A 128-bit block cipher making use of 128-, 192-, or 256-bit keys. This cipher is extremely safe and flexible, good-fit for huge microprocessors, 8-bit smart card microprocessors, and devoted hardware. This algorithm is among the Round 2 algorithms in the AES genre.

f) *Camellia:* This is a private-key, block-cipher algorithm developed together by "Nippon Telegraph and Telephone (NTT) Corp." and "Mitsubishi Electric Corporation (MEC)". It is considered under AES due to the following similarities: block size is 128-bit, support for the following length of keys-128, 192 and 256-bits, and appropriateness for software and hardware implementations on ordinary 32-bit processors and 8-bit processors (as in smart cards, cryptographic hardware, and embedded systems).

g) *MISTY1:* This block cipher is made at Mitsubishi Electric Corp., making use of 128-bit key with block size of 64-bits. Designed for hardware and software applications, this cipher is resistant to differential and linear cryptanalysis.

h) *Secure and Fast Encryption Routine (SAFER):* Hidden-key algorithm made for application in software. Versions are there for 40-, 64-, and 128-bit keys.

i) *KASUMI:* This block cipher uses a 128-bit key."Third-Generation Partnership Project (3gpp)" holds it as a part. KASUMI has privacy and reliability for message content and signaling data for up-and-coming mobile connections systems.

j) *SEED:* This block cipher uses 128-bit blocks and 128-bit keys and made by the "Korea Information Security Agency (KISA)". It is standardized algorithm nationwide in South Korea.

k) *Skipjack:* This SKC scheme, planned for Capstone, is a block cipher using an 80-bit key and 32 iteration cycles per 64-bit block. The working mechanisms of the algorithm were never disclosed.

3. *RSA:* This is the foremost, most widespread and popular PKC implementation, named after its developers *Ronald Rivest*, *Adi Shamir*, and *Leonard Adleman*. At present, RSA is implemented in numerous software applications and is used for key swap, *digital* signatures, or encryption of tiny blocks of records. RSA makes use of encryption block and a key, both of varying size. The pair of keys is resulting from a very large number, *n*. The number is actually the result of multiplication of a couple of prime numbers selected as per a bunch of unique rules. The prime numbers in discussion are likely >=100 digits in length each, resulting in an *n* with approximately double the number of digits present in the prime factors. The unrestricted key data includes "*n* and a derivative of one of the factors of *n"*. An intruder is unable to find out the prime factors of *n* and, hence, the secret key is extracted from only this information and that is the reason why RSA algorithm is highly safe. In a few places, the information on PKC mistakenly says that RSA's security is because of the trouble in factoring enormous prime numbers. The talent of computers to factor big numbers, and hence attack protocols like RSA, is improving fast. At present cryptosystems can find out the prime factors of numbers that have greater than 200 digits. Hence, if a huge number is made up from a couple of same sized prime factors, there never exists a factorization algorithm which will resolve the trouble in a sensible quantity of time. For instance, a test which was conducted to factor a 200-digit big number took 1.5 years for completion of the process. An advantage security measure provided by RSA is that users can effortlessly make the key size bigger to stay in front of the computer processing arch. Though, the patent for RSA expired in September 2000, its influence on many other algorithm is widely noticed.

a) *Diffie-Hellman:* Following the publishing of RSA algorithm, Diffie and Hellman invented the D-H algorithm to be used for private-key switch over. It cannot be used for verification of digital signatures.

b) *Digital Signature Algorithm (DSA):* This algorithm, mentioned in “NIST's Digital Signature Standard (DSS)”, gives digital signature competence meant for the confirmation of messages.

c) *ElGamal:* Planned by Taher Elgamal, it is a PKC system alike to Diffie-Hellman and applied in key switch over.

d) *Elliptic Curve Cryptography (ECC):* This is a PKC algorithm working upon elliptic curves. ECC offers levels of safety with minute keys similar to RSA and other PKC methods. It was intended for devices with partial compute supremacy and/or memory, such as smartcards and PDAs.

Comparison charts among the existing algorithms:

Encryption Algorithms	Structure	Flexibility	Modification	Known Attacks
DES	Feistal	No	No Modification	Brute Force Attack
Blowfish	Feistal	Yes	64-448 key in length in multiples of 32	Dictionary Attack
AES	Substitution & Permutation	Yes	256 key in length in multiples of 64	Side channel Attack
RSA	Factorization	Yes	MultiPrime RSA, Multipower RSA	Factoring the public key

Table 1 : Comparison of Encryption algorithms based on Structure, Flexibility, Modification and Known attacks.

Encryption Algorithms	Key Length (Bits)	Rounds	Block Size (Bits)	Level of Security	Encryption Speed
DES	64 (56 usable)	16	64	Adequate Security	Very Slow
Blowfish	Variable key length i.e. 32 – 448	16	64	Highly Secure	Very Fast
AES	128,192, 256	10,12,14	18	Excellent Security	Faster
RSA	Key length depends on number of bits in the module	1	Variable block size	Good level of security	Average

Table 2 : Comparison of Encryption Algorithms based on Key length, Rounds, Block Size, Level of Security and Encryption Speed.

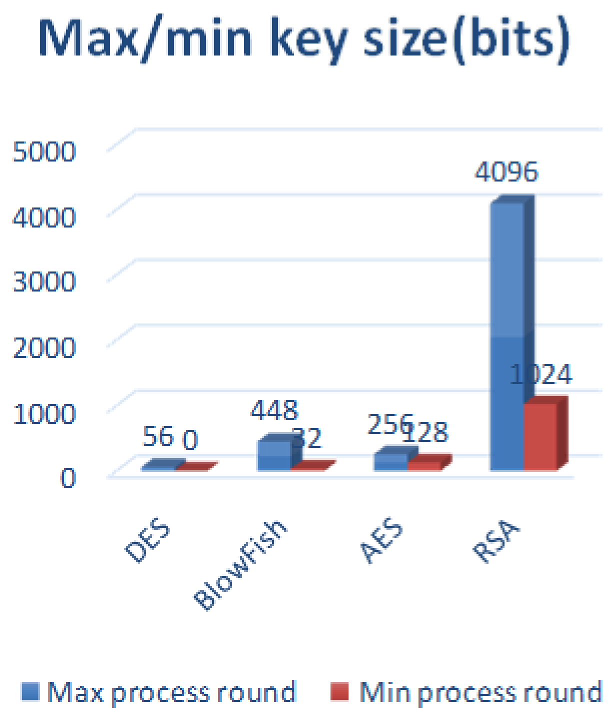

Fig.3 Comparison of Algorithms based on Min Process and Max Process round Vs Max/ Min Key size

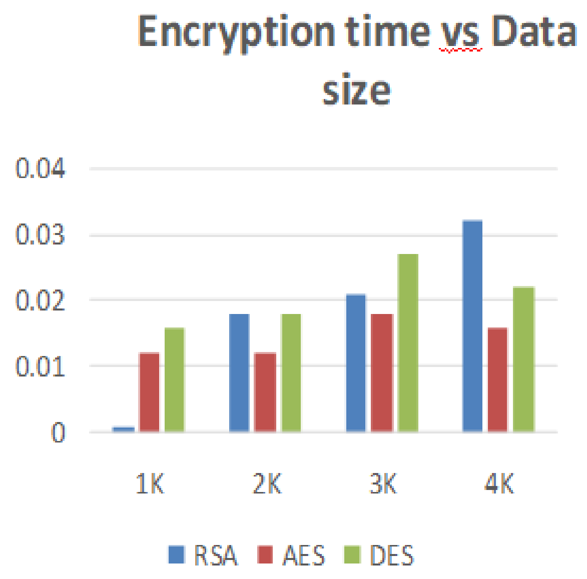

Fig.4 Comparison of Encryption algorithms with Encryption time Vs Data size

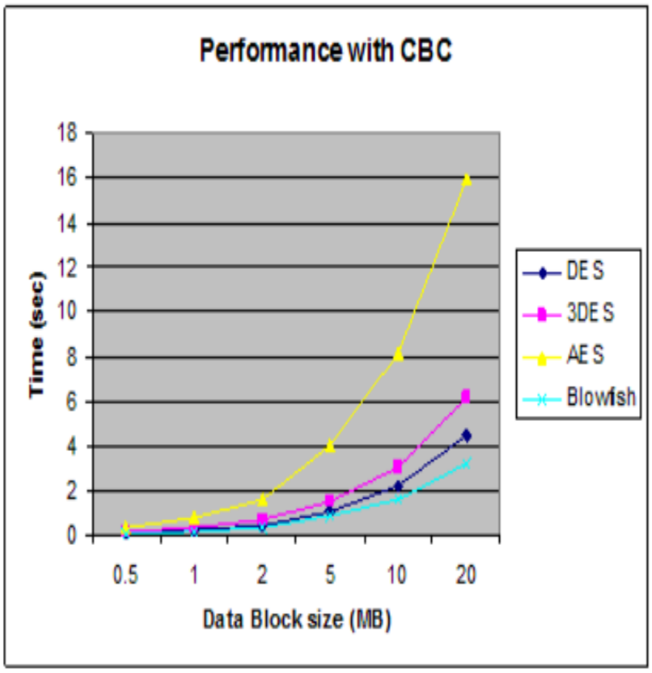

Fig.5 Comparison of Encryption algorithms with CBC

V. ALGORITHM EVALUATION PARAMETERS

Success of the execution test is required to evaluate the efficiency and security. Every encryption algorithm has some strength and weaknesses. In order to find and employ a secure encryption scheme to the applications, the performance parameters [24], [32]-[35] must be evaluated first. The discussion involves a few assessment parameters:

1) Encryption time: The time required to convert the plaintext into the cipher text. Time needed for encrypting is dependent on the size of message block as well as that of the key, and expressed in milliseconds. It has straight effect on the performance of the encryption algorithm. All cryptographic algorithms need smallest amount of time to encrypt, so that the encryption plan is reactive and rapid.

2) Decryption time: Time needed to pull through the plaintext from cipher text is known as decryption time. Cryptographic algorithms are desired to be fast and responsive, and so, it is obvious that the encryption and decryption time should be less (both measured in milliseconds).

3) Memory used: Memory utilized varies based on the execution of various algorithms. The memory needed for that depends on the size of key, initialization vectors, and operation types. Memory size should ideally be petite since it does not affect the cost of the system much.

4) Throughput: For finding the throughput of encryption algorithm, total block size (MegaByte) encrypted is divided by total encryption time. Larger the throughput value, lesser is the power consumption of algorithm.

5) Avalanche effect: It helps to figure out the changes in the plaintext, if any, after that the ciphertext will change drastically. Stating in a different way, it measures the difference between the plaintext and ciphertext to note the changes. Avalanche effect can be calculated using the hamming expanse. If degree of diffusion desired is high, then the avalanche effect should also be high. It can measure the effectiveness of cryptographic algorithms and valued by dividing the humming distance on the file size:

$$Avalanche = \frac{(Total\ number\ of\ bits - number\ of\ flip\ bits)}{Total\ number\ of\ bits} x100$$

6) Entropy: The effectiveness of the algorithm is approximately found out by applying random matrix method. Entropy helps to quantify the arbitrariness and ambiguity in the data. The connection between the ciphertext and key becomes more complicated with the more arbitrariness. Encryption algorithms need soaring arbitrariness in encrypting the plaintext. Ultimately dependency between the ciphertext and key is nil, which is referred to as the confusion. It is desirable to achieve a high degree of confusion since that makes it tough for an attacker to guess the complete set of information. Shannon's entropy can be calculated using the equation:

$$H(X) = -\sum_{i=0}^{n-1} p(x_i) \log_b p(x_i)$$

7) The number of bits required for encoding optimally: This evaluation parameter states the bandwidth needed to transmit data. A character encrypted with less number of bits, will consume less memory, bandwidth and will be less costly.

VI. CONCULSION AND FUTURE WORK

In this paper we described about the encryption and decryption techniques and discussed several encryption algorithms. Further we discussed algorithm evaluation parameters also. In today's world, security is required to communicate important and confidential information over the network. Security is vital in wide range of applications. Cryptographic algorithms provide the data security against malicious attacks. The most important aspect is the secure communications on the Internet or web is the foundation of network security and web security. Cryptography practices and studies of how to hide information from potential enemies, hackers or the public. The sender sends an encrypted a message along with a small piece of secret information (key) to the receiver. The encrypted message is decrypted by the receiver with a key that is same or different from the key used by the sender and recovers the original message. People without the right keys would not be able to read the message even if they steal the decrypted version. New techniques are used to generated the secret key ciphers and public key ciphers like secret key ciphers has techniques for defeating differential and linear cryptanalysis and public key ciphers are generated from simple instances of *NP*-hard problems as their bases. Cryptanalytic techniques have improved to the development of differential cryptanalysis came linear cryptanalysis. The complicated problems are reduced to simpler cases using *NP*-hard problems. The advancements in both cryptography and cryptanalysis lead to "provable security." The issue is to prove under what conditions a cipher is unbreakable. Similar issues arise with cryptographic protocols which can lead to excellent test base for many assurance techniques.

REFERENCES

[1] S. Ahmad, K. M. R. Alam, H. Rahman, and S. Tamura, “A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets,” in Proceedings of the IEEE International Conference on Networking Systems and Security, 2015.

[2] S.A.M. Diaa, M.A.K. Hatem, and M.H. Mohiy (2010). “Evaluating The Performance of Symmetric Encryption Algorithms” *International Journal of Network Security*, 2010, 10(3), pp.213-219

[3] Priti V. Bhagat, Kaustubh S. Satpute and Vikas R. Palekar “Reverse Encryption Algorithm: A Technique for Encryption &Decryption” International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 1 January 2013,pp 90-95.

[4] Z. Hercigonja, D. Gimnazija, and C. Varazdin, “Comparative analysis of cryptographic algorithms and advanced cryptographic algorithms,” International Journal of Digital Technology & Economy, vol. 1, no. 2, pp. 1–8, 2016.

[5] Gagandeepshahi, Charanjitsingh “Cryptography and its two Implementation Approaches” International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 3, May 2013,PP 668-672.

[6] Kuldeep Singh, Rajesh Verma, Ritika Chehal “Modified Prime Number Factorization Algorithm (MPFA) For RSA Public Key Encryption”International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012, pp 204-206

[7] Rostyslav Barabanov, Stewart Kowalski and Louise Yngström, “Information Security Metrics”, DSV Report series No 11-007, Mar 25, 2011

[8] Pallavi Vaidya and S. K. Shinde, “Application for Network Security Situation Awareness”, in International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012), IJCA, ISSN: 0975 – 8887, 2012.

[9] SunJun Liu, Le Yu and Jin Yang, “Research on Network Security Situation Awareness Technology based on AIS”, in International Journal of Knowledge and Language Processing, ISSN: 2191-2734, Volume 2, Number 2, April 2011.

[10] Disina, A. H., Pindar, Z. A., & Jamel, S., “Enhanced caeser cipher to exclude repetition and withstand frequency cryptanalysis,” Journal of Network and Information Security, 2015.