A Study Survey on the Deep Cryptographic data and its Algorithms Application

Kamali C[1] and Sreeram K[2]

[1]*Student, Department of Computer science and Engg, R V college of Engineering, Karnataka, India*
[2] *Student, Department of Computer science and Engg, Ramaiah Institute of Technology, Karnataka, India*

ABSTRACT

Data is a facts and statistics collected together and stored digitally for reference or analysis. In contemporary era, appraisal of networking and wireless networks. To improve the security in network we need to use cryptography. It provides secrecy and integrity to our data. The main aim of this is to provide Confidentiality, Authenticity, Integrity and Non-Repudiation. There are plenty of cryptographic techniques which is used to achieve this goal and to secure the data. In this paper we propose various tools and techniques of cryptography and its uses with various encryption and decryption algorithm.

Keyword -*: Cryptography, Encryption, Decryption, Symmetric, Message Authentication and Asymmetric.*

1. INTRODUCTION

In the present world, there are many situation to secure the data, ranging from secure commerce and payments to private communication we are using cryptography. Cryptography is an ancient art cryptography is used when communicating over untrusted medium. The five functions of cryptography are: confidentiality, authentication, integrity, non-repudiation, key exchange. The elements of cryptography are plaintext, cipher text, encryption, decryption, sender and receiver. Sender is the system which sends the message to the receiver. Receiver is the system which accepts the data. Plaintext is the unencrypted data. Cipher text is the encrypted text sent to the receiver. Encryption is the technique used to encrypt the data (plaintext) at the sender side. Decryption is the technique used to decrypt the cipher text which is received at the receiver side.

Cryptanalysis is the process of studying cryptographic systems and thought of as exploring the cryptographic systems. Cryptanalysis is the science of cracking codes and decoding secrets. It is used in information applications-like, an encrypted signal to be accepted as authentic. Opponent who have been able to discover the key will now want to use it to their advantage, therefore they will want to send wrong information to others, there are several attacks they are: cipher text only attacks, Known plaintext attacks, chosen plaintext attacks, chosen cipher text attacks, man in the middle attacks, side channel attacks, brute force attacks, birthday attacks.

Cryptology is converting information into the human unreadable form. Encryption is done using encryption algorithm and decryption is done using secret key. The secret will be known only to the receiver who needs that message.
The different types of encryption algorithms are: symmetric and asymmetric. Symmetric is where it uses a single key for encryption as well as decryption. Whereas asymmetric uses separate key for encryption and decryption. There are different types of techniques used for encryption and decryption it may be DES, triple DES, AES, blowfish, RSA, elliptic curve algorithms. Cryptography can also be used in various applications which uses hardware and software together.

2. LITERATURE SURVEY

Sarita Kumari.et.al [1], in this paper they have illustrated on basics of cryptography, security for the networks. And the goals of cryptography. To hide data in most critical situation two techniques is used cryptography and steganography. Network security is the security which is provided to the data in the network which is carried from sender to receiver. In this paper it tells about the goals of cryptography they are: confidentiality, authentication, data integrity, Non-repudiation, and access control. Data encryption is a technique which is used to convert the plaintext into some human unreadable form using some secret key. There are two types of secret key stream ciphers or block cipher. Block cipher is the technique which uses a key and an algorithm simultaneously where as in stream cipher a key and an algorithm is used one after the other. But the major drawback of this technique is if the key is lost by both sender and receiver it will not be able to recover the original text that was sent. Data decryption is a technique which is used to unencrypt the data that is sent by the sender.in this process the cipher text will be converted to the plaintext.

There are two types of cryptography they are: symmetric key cryptography and asymmetric key cryptography.

- Symmetric key cryptography is also called as private key cryptography. Only one key will be used to encrypt as well as decrypt. The key should be there with both sender and receiver.
- Asymmetric key cryptography is also called as public key cryptography. Two keys are used one for encryption and another for decryption. One more approach is illustrated that is compression which is used to compress the files or data into smaller size for utilization of memory.

A. Joseph Amalraj.et.al [2], in this paper they illustrated the techniques of cryptography. The main aim of using the cryptography technique is to secure the data from the third party that is hackers. When the sensational data is transferred from sender to the receiver it should not be seen by the hackers. There are n number of encryption algorithms that are being evolved. To secure the data from the hackers. They are improving the complexity of decrypting the data so that it is tough for the hackers to get the information that has been sent. And cryptography is classified into two types that is secret key cryptography and public key cryptography and certificate less public key cryptography is a new technique that was introduced by Al-Riyami and Paterson in the year 2003. In this technique the trusted third party will generate the key to encrypt and decrypt.In secret key cryptography there are different techniques they are: DES,triple DES,AES, RC5,blowfish.In public key cryptography the techniques are: RSA, elliptic curve etc.
DES algorithm as described by A. Joseph Amalraj, Dr. J. John Raybin Jose2 DES is a block cipher technique that uses same key for encryption and decryption simultaneously and it is fixed length algorithm.3DES it is a triple DES algorithm it is an improved version of DES the only difference is it uses 192 bits key size. AES algorithm is same as block cipher algorithm and a secret key cryptography. When compared to all others it is flexible.
Blowfish is a public domain algorithm. It encrypts 64 bit block cipher with variable key length's it is called with name because of the Rivets, Shamir, Adelman three inventors. It is public key cryptography where it uses 2 keys for encryption and decryption.

Suthar Monali.et.al [3], in this paper they have given the complete use of cryptography in authenticating RFID devices using elliptical curve cryptography. RFID is radio frequency identification it is wireless device for communication used to uniquely identify an object. It has a tag, reader etc.
There are several security attacks on RFID are: Denial of service (DOS), eavesdropping, user privacy, replay attack, spoofing attack and cloning attack.
When we need to implement the cryptography in RFID the complexity of algorithm must not be high because the hardware used are only high and cost effective so when we are using the technology addition to that it should be less complicated. For authentication purpose it uses simple bitwise operation, AES, HMAC schema can be used. In this paper they have discussed the three ECC based RFID algorithms they are:

- A secure ECC based RFID authentication protocol with ID verifier
- Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography
- Elliptic Curve Cryptography Based Mutual Authentication Protocol for Low Computational Capacity RFID Systems -Performance Analysis by Simulations

At last they have proved that all the three are more efficient and has highest computational time.

3. COMPARATIVE STUDIES AND COMPARSION OF ALGORITHMS

DES algorithm was created by IBM in the year 1975, it's a 56 bit key. So there are 2^56 possibilities of keys, encryption and decryption takes the same algorithm [4]. The security is weak this algorithm is very efficient for software and hardware requirements the main application is when network and endpoint communicate seamlessly.

3DES algorithm was created by IBM in the year 1978, it's a 112/168 bit key. It is a symmetric block type. The weakness of hacking is due to brute force linear cryptanalysis. The security is inadequate, 48 rounds run through this algorithm. AES algorithm was created by Joan Daemen and Vincent Rijmen in year 1998, it's a 256 bit key.it is a symmetric block cipher. It is implemented in secure file transfer protocols like fttps, https, sftp.

AES remains the preffered encryption algorithm for governments, banks and high security systems [5]. Blowfish algorithm was created by Bruce Schneier in year 1993, it's a 32/448 bit key. It is suitable for the application in which the key does not change frequently. Applications like packet switching, one way hash function.

RSA algorithm was created by adi Shamir and leonard adleman in year 1982.it is a public key cipher. It is safe because it uses complex mathematics. It is very tough to hack by the hackers because it is hard to crack it involves factorization of prime numbers which are difficult to factorize [6]. Elliptic curve algorithm is a public key cipher. It uses smaller keys for the same level of security.it has smaller cipher text and signatures. Very fast key generation. Binary curves are faster in hardware.

4. CONCLUSIONS

There are many techniques to secure the data to the network but we use cryptography because of its variety of its advantages and algorithms for encryption and decryption. And it is very secure, faster a flexible. It can be used with the hardware too. It has also complicated algorithm for sensitive data and most crucial data used for variety of applications. And also in future steganography will also be used in wider range to encrypt the images that we send through network it may be through wired or wireless connection. Example like social media etc. hiding the secret data from the intruder is a most challenging task for network security. The hardware devices are also used in order to secure the data.

5. REFERENCES

[1]. Sarita Kumari, "A research Paper on Cryptography Encryption and Compression Techniques", International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 6 Issue 4 April 2017, Page No. 20915-20919

[2]. A. Joseph Amalraj, Dr. J. John Raybin Jose, "A SURVEY PAPER ON CRYPTOGRAPHY TECHNIQUES", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.8, August- 2016, pg. 55-59

[3]. Suthar Monali, Prof Alka J Patel, "A Survey of Authentication of RFID Devices Using Elliptic Curve Cryptography", 2018 IJSRSET | Volume 4 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN: 2394-4099 National Conference on Advanced Research Trends in Information and Computing Technologies (NCARTICT-2018), Department of IT, L. D. College of Engineering, Ahmedabad, Gujarat, India In association with International Journal of Scientific Research in Science, Engineering and Technology

[4]. Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008

[5]. D. Boneh and M. Franklin, "Identity-based encryption form the weil pairing", in Advance in Cryptology (CRYPTO'01), LNCS 2139, Springer Verlag, 37, 213-229, 2011

[6]. Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Nov 1978.