CRYPTOGRAPHY AND NETWORK SECURITY

Mohammed Aslif. P[1], Shihas Backer[2], Ajmal Farhan. V. K[3], Thamjeed Roshan[4]
mohammedaslif3@gmail.com

B.tech III Year, Department of Computer Science and Engineering,
Kerala Technological University

Abstract-Cryptography is the ancient science of encoding messages so that only the sender and receiver can understand them. Cryptography can perform more mathematical operations in a second than a human being could do in a lifetime. Cryptography is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired'', an increasing number of people need to understand the basics of security in a networked world explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them. We go on to consider risk management, network threats, firewalls, and more special-purpose secure networking devices. Network security is the practice of preventing and protecting against unauthorized intrusion into corporate network

Keywords: Security, Threats, Cryptography, Encryption, Decryption

1. INTRODUCTION

A basic understanding of computer networks is requisite in order to understand the principles of network security. The Internet is a valuable resource, and connection to it is essential for business, industry, and education. Cryptography means "Hidden Secrets" is concerned with encryption . cryptography, the investigation of systems for secure correspondence. It is helpful for examining those conventions, that are identified with different viewpoints in data security, for example, verification, classification of information, non-denial and information uprightness.

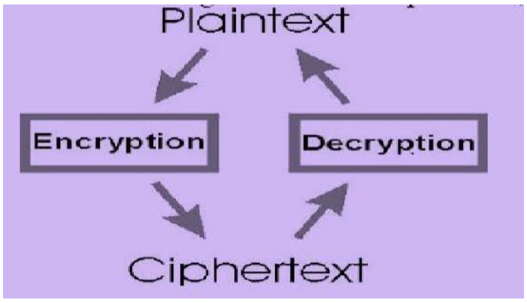


Fig 1. Cryptography

What Is Network Security?

Network security consists of the policies and practices adopted to prevent and monitor unauthorised access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator

Network security typically consists of three different controls: physical, technical and administrative. Here is a brief description of the different types of network security and how each control works.

Physical Network Security-Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on. Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.

Technical Network Security-Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network. Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

Administrative Network Security-Administrative security controls consist of security policies and processes that control user behaviour, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

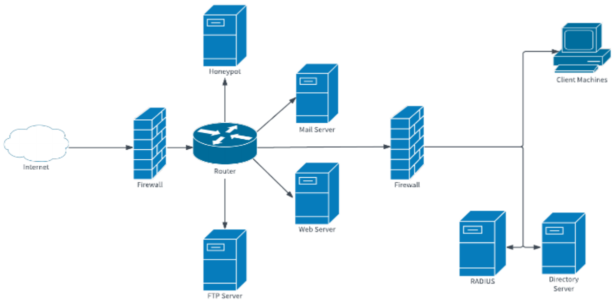


Fig 2. Network Security Diagram

Encryption:-In Cryptography, Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. **Encryption** does not itself prevent interference but denies the intelligible content to a would-be interceptor.

Decryption:-It is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of unencrypting the data manually or unencrypting the data using the proper codes or keys.

2.HISTORY OF CRYPTOGRAPHY

*Cryptography from 1800 to World War II
Edgar Allan Poe used systematic methods to solve cis in the 1840s. In particular he placed a notice of his abilities in the Philadelphia paper Alexander's Weekly (Express) Messenger, inviting submissions of ciphers, of which he proceeded to solve almost all. His success created a public stir for some months.[24] He later wrote an essay on methods of cryptography which proved useful as an introduction for novice British cryptanalysts attempting to break German codes and ciphers during World War I, and a famous story, The Gold-Bug, in which cryptanalysis was a prominent element.

In World War I the Admiralty's Room 40 broke German naval codes and played an important role in several naval engagements during the war, notably in detecting major German sorties into the North Sea that led to the battles of Dogger Bank and Jutland as the British fleet was sent out to intercept them. However its most important contribution was probably in decrypting the Zimmermann Telegram, a cable from the German Foreign Office sent via Washington to its ambassador Heinrich von Eckardt in Mexico which played a major part in bringing the United States into the war.

In 1917, Gilbert Vernam proposed a teleprinter cipher in which a previously prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the cyphertext. This led to the development of electromechanical devices as cipher machines, and to the only unbreakable cipher, the one time pad.

*World War II cryptography
By World War II, mechanical and electromechanical cipher machines were in wide use, although—where such machines were impractical—code books and manual systems continued in use. Great advances were made in both cipher design and cryptanalysis, all in secrecy. Information about this period has begun to be declassified as the official British 50-year secrecy period has come to an end, as US archives have slowly opened, and as assorted memoirs and articles have appeared.

3.MODERN CRYPTOGRAPHY

Encryption in modern times is achieved by using algorithms that have a key to encrypt and decrypt information. These keys convert the messages and data into "digital gibberish" through encryption and then return them to the original form through decryption. In general, the longer the key is, the more difficult it is to crack the code. This holds true because deciphering an encrypted message by brute force would require the attacker to try every possible key.

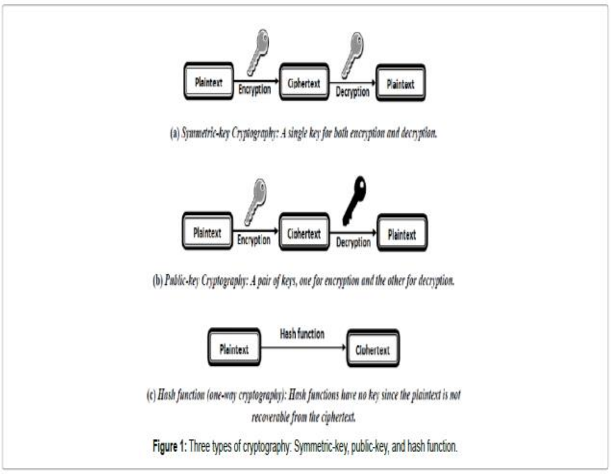
Claude E. Shannon is considered by many to be the father of mathematical cryptography. Shannon worked for several years at Bell Labs, and during his time there, he produced an article entitled "A mathematical theory of cryptography".

Public key:- asymmetric key encryption uses a pair of mathematically related keys, each of which decrypts the encryption performed using the other. Some, but not all, of these algorithms have the additional property that one of the paired keys cannot be deduced from the other by any known method other than trial and error. An algorithm of this kind is known as a public key or asymmetric key system. Using such an algorithm, only one key pair is needed per user. By designating one key of the pair as private (always secret), and the other as public (often widely available), no secure channel is needed for key exchange. So long as the private key stays secret, the public key can be widely known for a very long time without compromising security, making it safe to reuse the same key pair indefinitely.

Hashing:-Hashing is a common technique used in cryptography to encode information quickly using typical algorithms. Generally, an algorithm is applied to a string of text, and the resulting string becomes the "hash value". This creates a "digital fingerprint" of the message, as the specific hash value is used to identify a specific message. The output from the algorithm is also referred to as a "message digest" or a "check sum". Hashing is good for determining if information has been changed in transmission. If the hash value is different upon reception than upon sending, there is evidence the message has been altered. Once the algorithm has been applied to the data to be hashed, the hash function produces a fixed-length output. Essentially, anything passed through the hash function should resolve to the same length output as anything else passed through the same hash function

Modern cryptanalysis:-While modern ciphers like AES and the higher quality asymmetric ciphers are widely considered unbreakable, poor designs and implementations are still sometimes adopted and there have been important cryptanalytic breaks of deployed crypto systems in recent years. Notable examples of broken crypto designs include the first Wi-Fi encryption scheme WEP, the Content Scrambling System used for encrypting and controlling DVD use, the A5/1 and A5/2 ciphers used in GSM cell phones, and the

CRYPTO1 cipher used in the widely deployed MIFARE Classic smart cards from NXP Semiconductors, a spun off division of Philips Electronics.



(a) Symmetric-key Cryptography: A single key for both encryption and decryption.

(b) Public-key Cryptography: A pair of keys, one for encryption and the other for decryption.

(c) Hash function (one-way cryptography): Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Figure 1: Three types of cryptography: Symmetric-key, public-key, and hash function.

Fig 3. Telecommunications System Management Cryptography

4.EXISTING SYSTEM

In the traditional architecture there existed only the server and the client. In most cases the server was only a data base server that can only offer data.Therefore majority of the business logic i.e., validations etc. had to be placed on the clients system. This makes maintenance expensive. Such clients are called as ‘fat clients ’.This also means that every client has to be trained as to how to use the application and even the security in the communication is also the factor to be considered.

Since the actual processing of the data takes place on the remote client the data has to be transported over the network, which requires a secured format of the transfer method. How to conduct transactions is to be controlled by the client and advanced techniques implementing the cryptographic standards in the executing the data transfer transactions. Present day transactions are considered to be “un-trusted” in terms of security, i.e. they are relatively easy to be hacked. And also we have to consider the transfer the large amount of data through the network will give errors while transferring. Nevertheless, sensitive data transfer is to be carried out even if there is lack of an alternative. Network security in the existing system is the motivation factor for a new system with higher-level security standards for the information exchange.

5.PROPOSED SYSTEM

The proposed system should have the following features. The transactions should take place in a secured format between various clients in the network. It provides flexibility to the user to transfer the data through the network very easily by compressing the large amount of file. It should also identify the user and provide the communication according to the prescribed level of security with transfer of the file requested and run the required process at the server if necessary. In this system the data will be send through the network as a audio file. The user who received the file will do the operations like de embedding, decryption, and decompress in their level of hierarchy etc.

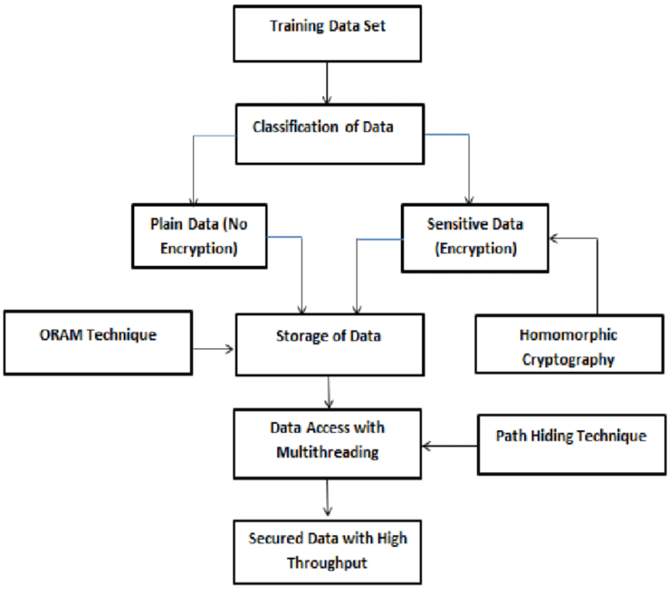

Training Data Set
Classification of Data
Plain Data (No Encryption)
Sensitive Data (Encryption)
ORAM Technique
Storage of Data
Homomorphic Cryptography
Data Access with Multithreading
Path Hiding Technique
Secured Data with High Throughput

Fig 4. Architecture Of Proposed System

6.BENEFITS OF CRYPTOGRAPHY:-

Cryptography is an essential information security tool. It provides the four most basic services of information security:−

Confidentiality − Encryption technique can guard the information and communication from unauthorized revelation and access of information.

Authentication − The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.

Data Integrity − The cryptographic hash functions are playing vital role in assuring the users about the data integrity.

Non-repudiation − The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

7.DRAWBACKS OF CRYPTOGRAPHY

>A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at a crucial time of decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.

>High availability, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the

threats such as denial of service or complete breakdown of information system.

>Another fundamental need of information security of selective access control also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.

>Cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols, and procedures. These need to be fixed through proper design and setting up of a defensive infrastructure.

>Cryptography comes at cost. The cost is in terms of time and money −

>Addition of cryptographic techniques in the information processing leads to delay.

>The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.

>The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

8.FUTURE OF CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) has already been invented but its advantages and disadvantages are not yet fully understood. ECC allows to perform encryption and decryption in a drastically lesser time, thus allowing a higher amount of data to be passed with equal security. However, as other methods of encryption, ECC must also be tested and proven secure before it is accepted for governmental, commercial, and private use.

Quantum computation is the new phenomenon. While modern computers store data using a binary format called a "bit" in which a "1" or a "0" can be stored; a quantum computer stores data using a quantum superposition of multiple states. These multiple valued states are stored in "quantum bits" or "qubits". This allows the computation of numbers to be several orders of magnitude faster than traditional transistor processors.

To comprehend the power of quantum computer, consider RSA-640, a number with 193 digits, which can be factored by eighty 2.2GHz computers over the span of 5 months, one quantum computer would factor in less than 17 seconds. Numbers that would typically take billions of years to compute could only take a matter of hours or even minutes with a fully developed quantum computer.

9.CRYPTOGRAPHY ALGORITHMS

There are a number of algorithms for performing encryption and decryption. The most successful algorithms use a key. A key is simply a parameter to the algorithm that allows the encryption and decryption process to occur. The modern field of key-based cryptographic algorithms can be divided into two classes, such as symmetric-key cryptography and asymmetric cryptography or publickey cryptography. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. This was the only kind of encryption publicly known until June 1976 . The public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Another cryptographic algorithm is cryptographic hash function that uses a mathematical transformation to irreversibly “encrypt” information.

Public-key cryptography:-Symmetric-key cryptosystems use the same key for encrypting and decrypting message in network security. A significant disadvantage of symmetric encryption is the key management necessary to use them securely. In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key cryptography in which two different but mathematically related keys are used; a public key and a private key [7]. A public-key system is so constructed that calculation of one key (the ‘private key’) is computationally infeasible from the other (the ‘public key’). Instead, both keys are generated secretly, as an interrelated pair. The historian David Kahn described public-key cryptography as “the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance”. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key

Types of ciphers in cryptography:- Encryption is the process of transforming plaintext data into something that appears to be random and meaningless, known as cipher text. Decryption is the process of converting cipher text back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of cipher text, the key that was used to encrypt the data must be used. There several types of operations used for encryption and decryption . Substitution and transposition ciphers are two categories of ciphers used in classical cryptography. All encryption algorithms are based on these two principles. In substitution, each element in the plain text is mapped into another element, and in transposition, the plaintext are rearranged. Most systems referred to as product systems, involved multiple stages of substitution and transposition. Substitution and transposition differ in how chunks of the message are handled by the encryption process.

Keyword mono-alphabetic encryption:-A mono-alphabetic substitution is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding cipher text symbol to generate cipher text. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed. An affine cipher E(x) = (ax+b) MOD 26 is an example of a mono-alphabetic substitution. In a keyword mono alphabetic cipher, substitution characters are a random permutation of the 26 letters of the alphabet.

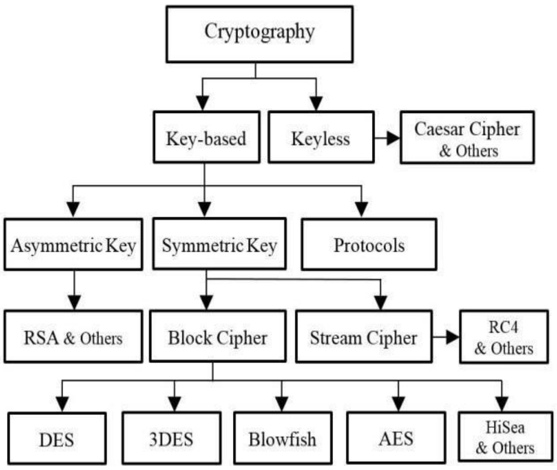


Fig 5. Overview Of Cryptography Algorithms

10.CONCLUSION

Cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against any kind of intruding. DES Encryption with two keys instead of one key already will increase the efficiency of cryptography.

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data Now, in order to achieve these goals various cryptographic algorithms are developed by various people. For a very minimal amount of data those algorithms wouldn’t be cost effective since those are not designed for small amount of data. The aim of this work was to design and implement a new algorithm to address this issue so that we don’t have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but of-course not sacrificing the security issues. A single is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm. But as public key cryptography is more secured then secret key cryptography our next task would be to develop and design a public key cryptographic algorithm in a simple manner as it is done in this paper.

REFERENCES

[1] Liddell, Henry George; Scott, Robert; Jones, Henry Stuart; McKenzie, Roderick (1984). A Greek-English Lexicon. Oxford University Press.
[2] Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen (ed.). Handbook of Theoretical Computer Science. 1. Elsevier.
[3] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10.
[4] Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. (1997). Handbook of Applied Cryptography. ISBN 978-0-8493-8523-0.
[5] Biggs, Norman (2008). Codes: An introduction to Information Communication and Cryptography. Springer. p. 171.
[6] "Overview per country". Crypto Law Survey. February 2013. Retrieved 26 March 2015.
[7] "UK Data Encryption Disclosure Law Takes Effect". PC World. 1 October 2007. Retrieved 26 March 2015.
[8] Ranger, Steve (24 March 2015). "The undercover war on your internet secrets: How online surveillance cracked our trust in the web". TechRepublic. Archived from the original on 12 June 2016. Retrieved 12 June 2016.
[9] Doctorow, Cory (2 May 2007). "Digg users revolt over AACS key". Boing Boing. Retrieved 26 March 2015.
[10] Whalen, Terence (1994). "The Code for Gold: Edgar Allan Poe and Cryptography". Representations. University of California Press (46): 35–57. doi:10.2307/2928778. JSTOR 2928778