INTRODUCTION TO CRYPTOGRAPHY AND NETWORK SECURITY

Dr. Prakash D\(^1\), Riyas M\(^2\), Mitha PS\(^3\)

Assistant Professor\(^1\), PG Student\(^2\&^3\)

Department Of Computer Science\(^1\), \(^2\&^3\)

Ajk College Of Arts And Science\(^1\), \(^2\&^3\)

Coimbatore, Tamil Nadu

Abstract: In today’s information age, communication play a very important role which help in growth of new technologies. So security is an essential parameter to be considered. A mechanism is therefore needed to secure the information that is sent. The process of transforming the original information into an unreadable format is known as encryption. The process of again converting the unreadable format in to the original information is known as decryption. The study of both encryption and decryption is known as cryptography. This paper focuses on analyzing different types of cryptography, concept of encryption and decryption, a brief introduction to cryptography techniques. If we are taking about security of information then following services come in mind i.e. Confidentiality (privacy of information), Authentication, Integrity (has not been altered). This paper provides a detailed description of all these cryptography techniques and a public key cryptography algorithm RSA.

Keywords: Introduction, Terminology, Purpose of Cryptography, Encryption Approach, Cryptography Technique, Algorithm, Problem Statement

I. INTRODUCTION

CRYPTOGRAPHY: If message we sent through internet should be secure or protected But there is a chance of corruption which is done by intruders. To provide the security and protect valuable information we use cryptography. A plain or normal text, which is send over the network, is firstly get transformed into cipher text so that only the sender and the recipient can use the information. In technical terms, the process of encoding plain text messages into cipher text messages is known as encryption. Transformation process of cipher text again into plain text is known as decryption. Decryption is just opposite to encryption. In computer to computer communications, the computer at sender’s end usually transforms a plain text messages into cipher text messages by performing encryption. Then this message is sent to the receiver over the network. The receiver’s computer takes the encrypted message and performs the decryption process to obtain plain text. The process of encryption and decryption is known as cryptography. In general cryptography is the art and science of achieving security by encoding message to
make them non readable. It can be used to hide the meaning of information in any form. It can also be applied to software, graphics or voice.

**Figure 1. Cryptography Process**

Cryptography is the art of secret coding. The basic service provided by cryptography is the ability to send the information between participants in a way that prevents others reading it. The main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity.

1) Plain text - original message
2) Cipher text - coded message
3) Encrypt - convert plain text into coded text

**II. TERMINOLOGY**

4) Decrypt - convert coded text into plain text
5) Cryptography - study of encryption principles and methods.

**III. PURPOSE OF CRYPTOGRAPHY**

In data and telecommunications, cryptography is necessary when communicating over any non-trusted medium, which includes just about any network, particularly the Internet. Within the context of any application-to-application communication, there are some specific security requirements, including:
1) Authentication: The process of proving one’s identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address based, both of which are notoriously weak.)
2) Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
3) Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
4) Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

IV. ENCRYPTION APPROACH

In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines.

![Encryption Method](image.png)

**Figure 2. Encryption Method**

In the proposed technique we have a common key between sender and receiver, which is known as private key. Basically private key concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where cipher text decrypted by same private key into plain text. The encryption key is trivially related to the decryption key.
V. Cryptographic Technique
There are two basic techniques for encrypting information: symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption). Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. Asymmetric encryption, in which there are two related keys—a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

A. Symmetric Key Cryptography
Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. Symmetric are much faster than asymmetric cryptography.

B. Asymmetric Key Cryptography
Asymmetric-key cryptography refers to encryption methods in which both the sender and receiver share the different key. One key is used for encryption and another for decryption. This provides more stability than symmetric systems.
VI. ALGORITHMS:
The algorithms for private (symmetric) key are DES (Data Encryption Standard), AES etc. and for public(asymmetric)key are RSA (Rivest, Shamir, Adleman), Diffie-Hellman etc.

A. RSA Algorithm

RSA stands for Rivest Shamir and Adleman name of three inventors. RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.

B. Key Generation:

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:
1) Choose two distinct prime numbers p and q.
2) For security purposes, the integers p and q should be chosen at random.
3) Compute n = pq.
4) n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
5) Compute φ(n) = φ(p)φ(q) = (p - 1)(q - 1) = n - (p + q - 1), where φ is Euler's totient function. This value is kept private.
6) Choose an integer e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1; i.e., e and φ(n) are coprime.
7) e is released as the public key exponent.
8) Determine d as d = e−1 (mod φ(n)); i.e., d is the modular multiplicative inverse of e (modulo φ(n)).
9) d is kept as the private key exponent.

Encryption
Cipher text c corresponding to calculated as:
c = m^e (mod n)

Decryption
Plain text can be calculated as:
m = c^d (mod n)
C. Disadvantages

In RSA encryption that is a deterministic encryption algorithm (i.e., has no random component) an attacker can successfully launch a chosen plaintext attack against the cryptosystem. RSA has the property that the product of two cipher texts is equal to the encryption of the product of the respective plaintexts. That is \( m_1m_2 \equiv (m_1m_2)e \pmod{n} \). Because of this multiplicative property a chosen-cipher text attack is possible.

VII. PROBLEM STATEMENT

Customer’s stores data at cloud service providers is vulnerable to various threats. In our work, we consider four types of threat models. First is the single point of failure, which will affect the data availability that could occur if a server at the cloud service provider failed or crashed, which makes it harder for the customer to retrieve his stored data from the server. Availability of data is also an important issue which could be affected, if the cloud service provider (CSP) runs out of service. Our second threat is data integrity. Integrity is a degree confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. Such worries are no more beneficial issues; therefore, a cloud service customer can not entirely rely upon a cloud service provider to ensure the storage of his vital data. Security is a necessary service for wired network as well as wireless network communication to improve what was offered in cloud. Simply storing the information on clouds solves the problem is not about data availability, but about security. The strong point of this method is that the secret key has to be combined by reconstructing. Most of the businesses that have held back from adopting the cloud have done so in the fear of having their data leaked. This feat stems from the fact that the cloud is a multi-user environment, wherein all the resources are shared. It is also a third-party service, which means that data is potentially at risk of being viewed or mishandled by the provider. It is only human nature to doubt the capabilities of a third-party, which seems like an even bigger risk when it comes to businesses and sensitive business data. There are also a number of external threats that can lead to data leakage, including malicious hacks of cloud providers or compromises of cloud user accounts. The best strategy is to depend on file encryption and stronger passwords, instead of the cloud service provider themselves.

VIII. CONCLUSION

The main goal is to securely store and access data in cloud that is not controlled by the owner of the data. We exploit the technique of elliptic curve cryptography encryption to protect data files in the cloud. Two part of the cloud server improved the performance during storage and accessing of data. The ECC Encryption algorithm used for encryption is another advantage to improve the performance during encryption and decryption process. We assume that this way of storing and accessing data is much secure and have high performance. Our efforts are going on to solve the problem of group sharing of data in the shared data section as in this scheme only member of group can access the data stored over shared data section. One to many, many to one, many to many communications is not possible.
REFERENCES


