Analysis of Cryptography and its Types

M. Abinaya
Assistant Professor
Department of Computer Science
Sri Saradha College for Women, Perambalur, India

Abstract:
In the globalization era, cryptography becomes more popular and powerful. Cryptography is one of the main constituents of computer security. To meet a user’s needs cryptographic algorithm needs to be selected on the basis of attributes like security and performance. Cryptography is one such way to make sure that confidentiality, authentication, integrity, availability and identification of user data can be maintained as well as security and privacy of data can be provided to the user. Encryption is the process of converting normal data or plaintext to something incomprehensible or cipher-text by applying mathematical transformations or formulae. These mathematical transformations or formulae used for encryption processes are called algorithms. This research paper provides an overview of cryptography which offers public and private key encryption, finally this paper also present types and techniques of cryptography.

Keywords: Cryptography, Algorithm, Encryption.

I. INTRODUCTION

Data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. You use encryption to make sure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption. The following figure shows this process.

![Cryptography Process](http://ijesc.org/)

Figure 1. Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

II. OBJECTIVES OF CRYPTOGRAPHY:

There are four main objectives of cryptography:-

a). **Confidentiality:** It guarantees that the sensitive information can only be accessed by those users/entities authorized to unveil it.

b). **Data integrity:** It is a service which addresses the unauthorized alteration of data. This property refers to data that has not been changed, destroyed, or lost in a malicious or accidental manner.

c). **Authentication:** It is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other.

d). **Non-repudiation:** It is a service which prevents an entity from denying previous commitments or actions

III. TYPES OF CRYPTOGRAPHY

- **Symmetric-key cryptography:** Same secret key is used for both encryption and decryption.
- **Asymmetric-key cryptography:** Two different keys are used i.e. one for encryption and other for decryption.

III. SYMMETRIC KEY CRYPTOGRAPHY

Symmetric key cryptography is also known as single-key, secret-key, and private key or one-key encryption. In this technique sender and receiver share the same key for encryption and decryption process. This technique was one of the simplest and earliest. It used the concept of a common key. The key was supposed to be some secret info shared by the sender and the receiver. Symmetric key algorithm is divided into two parts: first one is **BLOCK CIPHER** which is used for blocks of data. In this technique data is divided into blocks and then these blocks are used for encryption and decryption. Example of block cipher is AES, triple DES which is popular techniques of symmetric algorithms. And second one is **STREAM CIPHER** which operates on a single bit at a time. Transmitting the secret key on insecure network is also a curse of destroy the secrecy. There are many advantages of symmetric key cryptography like Symmetric key encryption is much faster. Single-key encryption does not require a lot of computer resources when compared to public key encryption. A different secret key is used for communication with every different party. If a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

ADVANTAGES

1. The one of the main advantage of Symmetric Algorithms is that they are undoubtedly quite simple and easy to implement.
2. However, the same properties make them quite vulnerable to attacks.

DISADVANTAGES
1. Once the key is found, the attacker can easily decode and destroy any of the information at will.
2. Scalability is also an issue, as the number of keys required as compared to the number of participants in the message exchange equals about the square of the number of participants.
3. Also, symmetric algorithms cannot be used for Digital Signatures.

IV. ASYMMETRIC KEY CRYPTOGRAPHY

Asymmetric key cryptography is also known as the public key cryptography. There are two types of key first one is public key which is used for encryption and second is private key which is used for decryption. Only a particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. The major drawbacks of asymmetric ciphers are their speed and security strength; they are much slower than the symmetric algorithms and more vulnerable to intruder attacks but they make key exchange easier. Asymmetric popular ciphers RSA (Rivest, Shamir, Adleman), Elliptic curve, Diffiehellman key exchange algorithm, Digital signature. Advantages of asymmetric key algorithm are it solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret. Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender. The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.

V. SECRET-KEY CRYPTOGRAPHY

Secret-key cryptography, also known as symmetric-key cryptography, employs identical private keys for users, while they also hold unique public keys. “Symmetric key” refers to the identical private keys shared by users. Users employ public keys for the encryption of data, while the private keys serve a necessary purpose in the decryption of data. People wishing to engage in a secure exchange of information will swap public keys and use some method to ensure the existence of identical private keys. In theory, private keys would be brought into the transaction through either the duplication of an existing key or the creation of two identical keys. In modern practice, users utilize key generators to create both keys, but the private keys must still be distributed in a confidential mode.

Strengths:
The private keys used in symmetric-key cryptography are robustly resistant to brute force attacks. While only the one-time pad, which combines plaintext with a random key, holds secure in the face of any attacker regardless of time and computing power, symmetric-key algorithms are generally more difficult to crack than their public key counterparts. Additionally, secret-key algorithms require less computing power to be created than equivalent private keys in public-key cryptography.

Weaknesses:
The biggest obstacle in successfully deploying a symmetric-key algorithm is the necessity for a proper exchange of private keys. This transaction must be completed in a secure manner. In the past, this would often have to be done through some type of face to-face meeting, which proves quite impractical in many circumstances when taking distance and time into account. If one assumes that security is a risk to begin with due to the desire for a secret exchange of data in the first place, the exchange of keys becomes further complicated. Another problem concerns the compromise of a private key.

In symmetric key cryptography, every participant has an identical private key. As the number of participants in a transaction increases, both the risk of compromise and the consequences of such a compromise increase dramatically. Each additional user adds another potential point of weakness that an attacker could take advantage of. If such an attacker succeeds in gaining control of just one of the private keys in this world, every user, whether there are hundreds of users or only a few, is completely compromised.

VI. PUBLIC-KEY ENCRYPTION

Kuchlin introduces the foundations of public-key encryption and presents RSA as an early method of transmitting secret messages over insecure channels. The author recognizes that unauthorized users can attempt to intercept messages, and devises this public-key method for ensuring that such users will not be able to interpret the contents of the message. The author’s public-key method consists of separate encryption and decryption keys, with users only being able to decrypt an encrypted message if they have the appropriate decryption key. Users will exchange public keys; this transaction does not need to be done in a secure manner because the release of public keys does not threaten the security of any private information. After this swap, someone who wishes to send private information to another user will encrypt the data with the intended recipient’s public key and then pass along the encrypted message. The recipient, who will keep his or her private key secure under any circumstance, can use the private key to decrypt the encoded message. Kuchlin introduces separate algorithms for generating encryption and decryption keys as well as an algorithm for combinations of encryption and decryption key.

Strengths:
The asymmetric nature of public-key cryptography allows it a sizable advantage over symmetric-key algorithms. The unique private and public keys provided to each user allow them to conduct secure exchanges of information without first needing to devise some way to secretly swap keys. This glaring weakness of secret-key cryptography becomes a crucial strength of public-key encryption.
Asymmetric cryptography has been the foundation for secure time consuming problem. The disadvantage of this algorithm is too chances of combinations and with two keys requires $2^{112}$ Encrypt-Decrypt-Encrypt. In 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence order of Encrypt-Decrypt-Encrypt. There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation which named as IP and FP.

DES
- DES is a block cipher that uses shared secret key for encryption and decryption.
- DES algorithm as described by Davis takes a fixed length of string in plaintext bits and transforms it through a series of operations into cipher text bit sting of the same length and its each block is 64 bits.
- There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation which named as IP and FP.

3DES
- 3DES is an enhancement of DES and it is 64 bit block size with 192 bits key size. In this standard the encryption of method is similar to the one in the original DES and increases the encryption level and the average safe time.
- In 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence order of Encrypt-Decrypt-Encrypt.
- TDES algorithm with three keys require 2168 chances of combinations and with two keys requires 2112 combinations; and the disadvantage of this algorithm is too time consuming problem.

AES
- In AES is the almost identical of block cipher Rijndael cipher developed by two Belgian cryptographers, Joan and Vincent Rijmen.
- The algorithm explains about by AES is a secret-key algorithm which means of the same key is used for both Encrypting and decrypting the data.
- AES on the other hand which encrypts all 128 bits in one iteration. This is one reason why it has a comparably small number of rounds. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices

Blowfish
- Blowfish is one of the most common public domain encryption algorithm provided by Bruce Schneier one of the world’s leading cryptologists, and the president of Counterpane Systems and a consulting firm specializing in cryptography and computer security
- Blowfish encrypts 64-bits block cipher with variety length key and its contains two parts.

Data Encryption: It involves the iteration of a simple function of 16 times. Each round contains a key dependent permutation and data dependent substitution.

Sub key Generation: It involves converts the key up to 448 bits long to 4168 bits.

RSA
- RSA is a public key algorithm invented by Rivest, Shamir, Adleman. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages.
- Messages encrypted with the public key can only be decrypted using the private key. These keys for the RSA algorithm are generated in many ways.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Created by</th>
<th>Key Size (in bits)</th>
<th>Block Size (in bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>IBM in year 1975</td>
<td>56</td>
<td>64</td>
</tr>
<tr>
<td>3DES</td>
<td>IBM in year 1978</td>
<td>121 (or) 188</td>
<td>64</td>
</tr>
<tr>
<td>AES</td>
<td>Joan Daemen and Vincent Rijmen in year 1998</td>
<td>256</td>
<td>128</td>
</tr>
<tr>
<td>Blowfish</td>
<td>Bruce Schneier in year 1993</td>
<td>32 (or) 448</td>
<td>64</td>
</tr>
</tbody>
</table>

VII. CONCLUSION
This paper gives a detailed study of Cryptography Techniques like AES, DES, 3DES, Blowfish, RSA. Among those algorithms and concepts the security for the data has become highly important. In this paper it has been surveyed about the existing works on the encryption techniques. This paper presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. Secret-key cryptography lags behind asymmetric cryptography. Combinations of the two can be implemented for improved security but secret-key cryptography by itself proves insecure against man in the middle attacks. Asymmetric cryptography has been the foundation for secure
data exchange over networks and while it still has its shortcomings, new ideas still come forth as the field continues to evolve.

VIII. REFERENCE


