Basics of Cryptography

Animesh jain,
Saquib Saqulain
[1]Scholar CCSIT TMU, MORADABAD
[2]Scholar CCSIT TMU, MORADABAD
[1]animeshzain@gmail.com
[2]Saquibsaqulain12@gmail.com

ABSTRACT:-

We are living in 21st century, the era of digital world. For our every work we are dependent on digital system either it be for storing data or for communication around the other part of the world. This digital system has made our work so easy that we even don't need to meet a person to purchase something or to do a business locally or internationally.
Therefore we need to secure our information so that our privacy be maintained. There is cyber crime taking place at a regular interval everywhere on the web. The motive of these attacks may be to blackmail or to damage the organization.
The major issues at this time are to maintain confidentiality, integrity, authentication and non-repudiation. This paper deals with the confidentiality of electronic data which is transmitted over the internet. Cryptography involves conversion of electronic data/plain text into cipher text (encryption) and then sends it to the receiver where the cipher text again is converted to plain text (decryption). Here we will be using different methods of cryptography like HASHING, SYMMETRIC, ASYMMETRIC and KEY EXCHANGE ALGORITHM in order to provide security to our data.

Keywords:- Cryptography, Hashing, Symmetric cryptography, Asymmetric cryptography, Key exchange algorithm, Cipher

INTRODUCTION

CRYPTOGRAPHY is the science of secret writing with the intention of data secret. CRYPTO means secret or hidden. Cryptography is the technique of converting plain text into cipher text (ENCRYPTION) at the point of sender and again cipher text into plain text (DECRYPTION) at the point of the receiver. Cryptography is applying security to digital data. It consist of mechanism of mathematical algorithms which in turn lead to information security.

OBJECTIVE OF CRYPTOGRAPHY

The main objective of cryptography is to provide security to the following 4 information security services.

1. **Confidentiality:** It is a security to keep away unauthorized person.
2. **Data Integrity:** It identifies any alteration of data. It can't stop data from alteration but detect if the data is manipulated.
3. **Authentication:** It confirms receiver that the message or data has been sent by verified sender.
4. **Non-repudiation:** It provides assurance to the receiver as the creater of the data can't deny the creation.

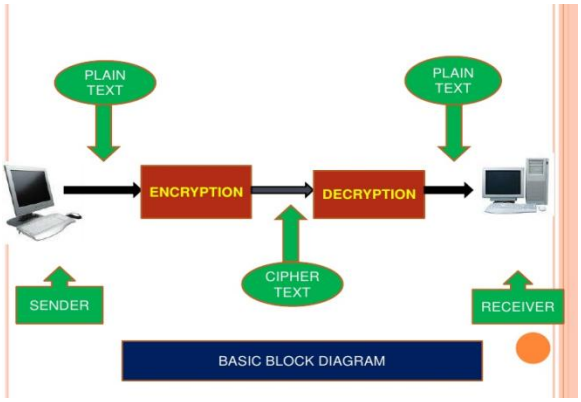
Importance of cryptography

This technique is used to achieve confidentiality. When we send any message or data if anyone tries to steal it, he/she might be able to steal it but can't understand because of encryption.

Modern Cryptography

Its foundation is based on various concepts of mathematics such as number theory, computational-complexity theory, and probability theory.

Secrecy is obtained through a secrete key which is used as the seed for the algorithms.



Understanding ciphers: The basis of cryptography

In cryptography CIPHER is an algorithm for performing encryption or decryption by the use of a series of steps that can be followed as a procedure.

for example: we want to encrypt "hello".

Our plaintext is "hello". We can use one of the simplest forms of encryption known as

"Caesar's Cipher" (also known as shift cipher) to the message.

--with this cipher we simply shift each letter of the text to a fixed number steps forward or backward. Just like below

A=D

B=E

C=F

D=G

And so on. 3 steps forward of the actual place of the alphabets.

Applying this pattern

h=k

e=h

l=o

l=o

o=r

Hence "hello" is encrypted in "khoor".

Types of cryptography

1. Hashing cryptography.

2. Symmetric cryptography.

3. Asymmetric cryptography.

4. Key exchange algorithm.

1. Hash cryptography

A cryptographic **hash function** is a hash function which takes an response (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value', 'message digest', 'digital fingerprint', 'digest' or 'checksum'.

The ideal hash function has three main properties:

1. It is extremely easy to calculate a hash for any given data.
2. It is extremely computationally difficult to calculate an alphanumeric text that has a given hash.
3. It is extremely unlikely that two slightly different messages will have the same hash.

Functions with these properties are used as hash functions for a variety of purposes, not only in cryptography. Practical applications include message integrity checks, digital signature, authentication, and various information security applications.

A hash function takes a string of any length as input and produces a fixed length string

which acts as a kind of "mark" for the data provided. In this way, a person knowing the "hash value" is unable to know the original message, but only the person who knows the original message can prove the "hash value" is created from that message.

1. Finding a (previously unseen) message that matches a given hash values.
2. Finding "collisions", in which two different messages have the same hash value.

An attacker who can find any of the above computations can use them to substitute an authorized message with an unauthorized one.

2. Symmetric cryptography

This type of cryptography is uses a single key to encrypt message/data as well to decrypt that message/data.

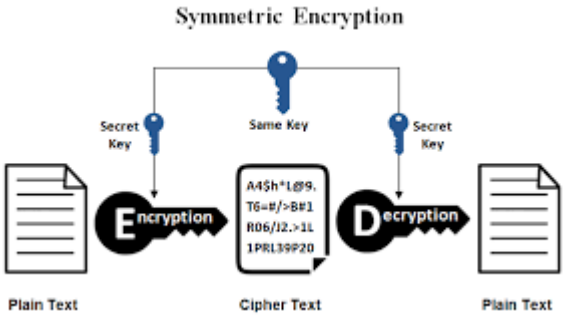
The problem here is exchange of the key. If we applied a key here then how will that key be transferred to the receiver. This method of transferring data is meaningless because if we have a secure way of transferring the key then why not use the same to transfer the message/data.

Symmetric-key type

Symmetric-key encryption can use either Stream Ciphers or Block Ciphers.

- Stream Ciphers encrypt the digits (normally bytes), or letters (in substitution ciphers) of a message one at a time.
- Block ciphers take a number of bits and encrypt them as a single unit, lining the plaintext

so that it is a multiple of the block size.



3. Asymmetric cryptography

This method uses two keys "public key" and "private key" as opposed to single key of symmetric.

The public key is used to encrypt message and the private key is used to decrypt the message.

Every user has both the keys. When we need to send a message we demand his public key to encrypt the message, that particular encrypted message will be only decrypted by that receiver's "private key" only.

Asymmetric cryptography is used in transferring email files, https etc. keeping our information safe.

The generation of such keys depends on cryptographic algorithm based on mathematical problems to produce one way function. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

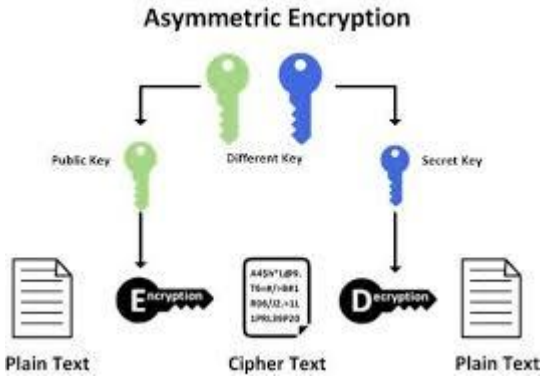
In such a system, any person can encrypt a message using the receiver's public key, but

that encrypted message can only be decrypted with the receiver's private key.

Robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the corresponding public key can combine a message, a putative digital signature on it, and the known public key to verify whether the signature was valid, i.e. made by the owner of the corresponding private key.

Two of the best-known uses of public key cryptography are:

- Public key encryption, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. This is used in an attempt to ensure confidentiality.
- Digital signatures, in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that the sender had access to the private key, and therefore is likely to be the person associated with the public key. This also ensures that the message has not been tampered with, as a signature is mathematically bound to the message it originally was made with, and verification will fail for practically any other message, no matter how similar to the original message.



4. Key exchange algorithm

Key exchange (also key establishment) is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm

If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.

Drawbacks of Cryptography

1. Cryptography is costly. Cost is in terms of time and money.

2. Mathematical computational problems are difficult. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

3. A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legimate user.

Conclusion

In this paper we discussed about how to encrypt and decrypt data to be transferred. The different methodologies like Hashing, Symmetric, Asymmetric and Key exchange algorithms. In the future work, we plan to design sophisticated software based on this technique which will targeted to use in highly secure data transmission.

- It helps in securing our data in order to maintain our privacy.
- It helps us from being cheated as nobody can change the message on the way.
- It provides assurance to the receiver that creator of the message or the action can't deny the creation. Such things help in online shopping etc.

Refrences:-

[1] R. Anderson, and M. Roe. A5, 1994. Available at http://jya.com/crack-a5.htm

[2] Bluetooth CIG, Specification of the Bluetooth system, Version 1.1, February 22, 2001. Available from www.bluetooth.com.

[3] I. Mantin. Predicting and Distinguishing Attacks on RC4 Keystream Generator. Eurocrypt Vol. 3494 of LNCS, pp. 491-506, Springer-Verlag, 2005.

[4] G. Gong, K. C. Gupta, M. Hell, andY. Nawaz, Towards a General RC4-like Keystream Generator, SKLOIS Conference on Information Security and Cryptology (CICS05), December15-17, Beijing, China. Springer-verlag, 2006. (Download: http://comsec.uwaterloo.ca.)

[5] eSTREAM - The ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream/

[6] Y. Nawaz and G. Gong, WG: A family of stream ciphers with designed randomness properties, Information Sciences, Vol. 178, No. 7, April 1, 2008, pp. 1903-1916.

[7] National Bureau of Standards, Data Encryption Standard, FIPS Publication 46, U.S. Department of Commerce, 1977.

[8] National Institute of Standards and Technology, Advanced Encryption Standard, FIPS-197,
http://csrc.nist.gov/archive/aes/index.html,
2000. General References for Cryptography:

[9] D. Stinson, Cryptography, Theory and Practice, CRC Press, Second edition, 2000.

[10] W. Stallings, Cryptography and Network Security: Principles and Practice, Second edition, Prentice Hall, 1999.

[11] . J. Menezes and P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996