International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

General Article

Cryptography

Ritika*

Government College for Women Rohtak, India

Received 01 May 2017, Accepted 10 July 2017, Available online 15 July 2017, **Vol.7, No.4 (Aug 2017)**

Abstract

We are living in a world where majority of business is done online, which raises questions over security of the data. Cryptography secures the data from originating point to end point. Cryptography protects your data by way of encrypting before reaching to end user where you can decrypt the data by using various techniques in this way cryptography protects your data from unknown/suspicious sources for this purpose various techniques can be used like private key encryption, public key encryption or combination of both.

Keywords: *Encrypt, decrypt, cryptography*

Introduction

Cryptography is method of storing and transmitting the data in such a way that only the person for whom it is meant can access and process it coding the data in such a way which cannot be read by others is called encryption and decoding that data back to original form is known as decryption. There are many techniques to encrypt and decrypt which can be used to secure the data online what basically this method does is protecting your data from unwanted access and use.

What types of cryptography is there?

Before discussing the types of cryptography, let us first apprise ourselves with few terms:

Encryption: method of coding the data in a secure unreadable form until it is decoded back to original
Decryption: decoding data back to original form

Key: like a password, used to encrypt and decrypt information

Different types are given below

1) Secure line: a transmission mode where data can be sent securely
2) Public line: a method used to send the data to desired location. Private line is more secure than this.
3) Symmetric cipher: a method in which same key is used for encryption and decryption
4) Public key cryptography: a method in which two different keys are used to encrypt and decrypt these keys are called key pair one is kept secret and is called private key and other one is called public key; complex of the two onetime pad: a method in which both sender and receiver have same no of codes i.e. (a bunch random number) which is sent over transmission line. It is used as symmetric key and destroyed after use it is used for security purpose.
5) Stenography: best understood with the help of an example, when a picture is sent the empty space is used to send the hidden information in this way information can be securely sent without encrypting methods.

Why would I want to use cryptography on a daily basis?

The reason to use cryptography basically comes under three heads:

1) Protection: there many issues related to the use of internet to avoid all these issues, encrypt the data before sending it which can be decrypt by receiver into the original format.
2) Privacy: whenever data is sent from source to destination, we do not want anyone to read, delete or update the information. For this purpose we need to secure the data. This is the reason privacy is important and various cryptography techniques are used for this purpose cryptography hides the data we are reading this is the reason one should not do private business online the encryption should be safe because there is no point in encrypting if someone else decrypt the data.
3) Verification: it means when the information is sent to destination then the destination verifies the

*Corresponding author's ORCID ID: 0000-0003-2385-487X

source of origin of information and confirms that no forgery/malpractice is involved ; as is the case in money transfer from one account to another account where bank maintains all the record.

Cryptographic Key Types

Different type of keys is discussed as under

1) Private signature key: -Asymmetric key pairs used to generate digital signature. It is used to provide genuineness, integrity , non-repudiation
2) Public signature verification key: - Asymmetric key pair used to verify digital signature to authenticate user or confirmation of integrity or combination of both.
3) Symmetric authentication key: - Used to show the integrity of the message.
4) Private authentication key: - An asymmetric key to authenticate identity of user, genuineness of the message.
5) Public authentication key: - Used with public key algorithm to find out the identity of information, entities.
6) Symmetric data encryption key: - Used to protect the information.
7) Symmetric key wrapping key: - Used to encrypt other keys by making use of symmetric key algorithms.
8) Symmetric and asymmetric random number generation keys: - Random numbers are generated with these keys.
9) Symmetric master key: - Used to derive symmetric keys by using symmetric cryptographic methods.
10) Symmetric authorization key: - Provides privileges to an entity using symmetric cryptographic method.
11) Private authorization key: - An asymmetric key pair used to provide privileges to an entity.
12) Public authorization key: - An asymmetric key pair which is used to verify privileges for an entity.

The Basic Principles of Cryptography

1) Encryption: The process in which data is converted to unreadable format to protect it from suspicious/unknown/unwanted persons. The sender encrypts before sending the data to the destination decrypts it to the original form. In addition to above two terms, information is required for cryptography. This information is known as key. There are applications where same key can be used for encryption and decryption and in some applications different keys are desired.
2) Authentication: Authentication means the actual sender has sent the message.
3) Integrity: Integrity means when you transfer money from one account to other, in between, it cannot be altered and integrity is maintained throughout the way. A cryptographic method helps us in such cases.
4) Non Repudiation: It means that the actual sender has sent the message. For example when you request bank to transfer money then bank maintains the record that how much and when the account holder requests the bank.

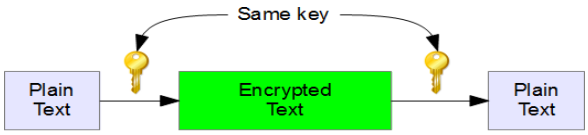
Types of Cryptography

Different types of cryptography techniques are given below

1) Secret key Cryptography
2) Public key cryptography
3) Hash Functions

1) Secret Key Cryptography

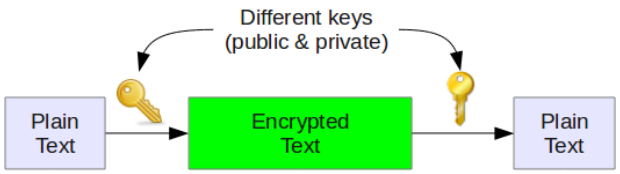
In this technique single key is used. Same key is used by sender and receiver to encrypt and decrypt the message. It is called symmetric encryption because single key is used.



It is no not that secure as compared to other techniques.

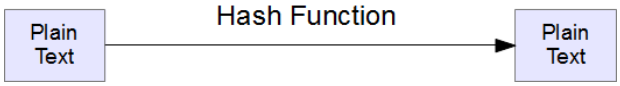
2) Public key Cryptography

Two keys are used to make it more secure. As two keys are used it is called asymmetric encryption.



One key is private and other is public. Private Key is secret and it is not revealed to anyone whereas public key is shared with those with whom you want to share information.

3) Hash Function



No key is involved in this method. It is based on a hash value which is calculated on the basis of plain text. These hash values are used to check the integrity of the message so that it is not altered or affected by virus.

Conclusion

Cryptography is used in our day to day life to make our data secure and protect it from malicious/fraudulent users. As internet and mails are the main media of doing business now days, so to protect your data over internet, we use cryptography, so that data is readable to only those users for which it is meant. For this various encryption and decryption techniques are used together with private and public key encryption methods or sometimes combination of both. To make your data your data more secure, authentic.

Reference

https://www.trilightzone.org/cryptography_in_daily_life.html
http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/life.html
http://all.net/edu/curr/ip/Chap2-4.html
http://en.wikipedia.org/wiki/Cryptographic_key_types
http://wooledge.org/~greg/crypto/crypto.html
https://technet.microsoft.com/en-us/library/cc962030.aspx
http://www.businessdictionary.com/definition/cryptography.html