International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 4 Issue 5, May-2015, pp: (16-19), Impact Factor: 1.296, Available online at: www.erpublications.com

Cryptography

Neetika

Abstract: Now a day's as technology is improving, your whole business is done online, which makes it less secure so to improve security of your data, while you are sending it from source to destination. Here cryptography comes in Picture. It protects your data by encrypting your message before sending it to the destination and at the destination, you decrypt your data using various techniques, so that your data becomes unreadable to suspicious users, which indirectly makes it secure, which is the main purpose of using cryptography. There are various techniques like private key encryption, public key encryption or combination of both.

Keywords: security, encrypt, decrypt, source, destination.

Introduction

Cryptography is a method of storing and transmitting data such that the message is visible to only that user for which it is sent and only that user can process it. Coding your data in the form which is not readable by others is called encryption and decoding that data to the original form is called decryption. For encrypting and decrypting data there are various techniques available. These techniques are followed to provide security to your data. It is basically process to convert your data from readable data to unreadable data. It is a process of protecting your data so that only authorized person can have access to it.

What types of cryptography are there?

There are various types of cryptography, but before discussing that there are few terms you need to know.

1) **Encryption**: -It is method of coding your data so that it becomes unreadable until it is decoded back to the original format.
2) **Decryption: -** Decoding your data back to the original format.
3) **Key: -** it is like password which is used to encrypt and decrypt information.

These are of different types which are given below:

i) **Secure line**: **-** It is a transmission mode where you can send your data secretly.
ii) **Public Line**: **-** This is a method used to send data to correct destination. It is not that secure as compared to secure line.
iii) **Symmetric Cipher**: **-** in this method same key is used to encrypt and decrypt the information.
iv) **Public Key Cryptography**: **-** In this method two keys are used, one key is used to encrypt and other key is used to decrypt. These two keys are called key pair. One key is called private key and it is kept secret. The other key is called public key. This type is bit complex.

One Time Pad: It is encryption method, both sender and receiver both have same no of codes i.e. (a bunch random number), which is sent over transmission line. It is used as a symmetric key. It is destroyed after use because it is used only once. It is used for security purpose.

Steganography: It is explained well with example, when we send a picture there is a lot of space, so that space is used to send hidden information. In that way your secret information is easily sent without using encryption methods.

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

There are many reasons why this cryptographic techniques. They basically come under three categories: -

1) **Protection: -** There are various issues related to internet the way how you access and use it. So to avoid all this fuss if you encrypt your data before sending it, so that no one can read it and the receiver can decrypt it to the original format.
2) **Privacy: -** When you send your data from source to destination, you do not want anyone to read, delete or update your information for that you need to secure your data. That is why privacy is very important and that is why cryptographic techniques are used to secure your data. Best feature of cryptography is that it hides your data what you are reading. That is why you should not do any private business over internet. Another point which is need to consider that if you encrypt your message and if anyone decrypt it then there is no point of using encryption.
3) **Verification: -** It means that when you send the information to the destination, then destination verifies it whether the actual source sent the information and there is no forgery involved in it. For example when you transfer money from one account to another then bank maintains the record that the actual account holder requests for the money transfer.

Cryptographic Key Types

Key management is an important factor in cryptographic system. There are different keys which are used for different purposes.

1) **Private signature key: -** These are asymmetric key pairs used to generate digital signature. It is used to provide authentication, integrity, non-repudiation.
2) **Public signature verification key: -** It is an asymmetric key pair which is used to verify digital signature to authenticate user or determination of integrity or combination of both.
3) **Symmetric authentication key: -** It is basically used to provide the integrity of the message.
4) **Private authentication key: -** it is an asymmetric key to authenticate identity of user, originality of the message.
5) **Public authentication key: -** is used with public key algorithm to determine the identity of information, entities.
6) **Symmetric data encryption key: -** it is used to apply protection to the information.
7) **Symmetric key wrapping key: -** used to encrypt other keys using symmetric key algorithms.
8) **Symmetric and asymmetric random number generation keys: -** these keys are used to generate random numbers.
9) **Symmetric master key: -** used to derive symmetric keys using symmetric cryptographic methods.
10) **Symmetric authorization key: -** used to provide privileges to an entity using symmetric cryptographic method.
11) **Private authorization key: -** It is an asymmetric key pair used to provide privileges to an entity.
12) **Public authorization key: -** it is an asymmetric key pair to verify privileges for an entity.

The Basic Principles of Cryptography

1. Encryption

It is the process of converting the data to unreadable format to protect it from suspicious persons. The sender before sending the data to the destination it is encrypted, and destination decrypts it to the original form. In addition to these two terms further information are required for cryptography. This information is known as key. There are applications where same key is used for encryption and decryption and in some applications different keys are required.

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 in between and integrity is maintained on the way. This is done using cryptographic methods.

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.

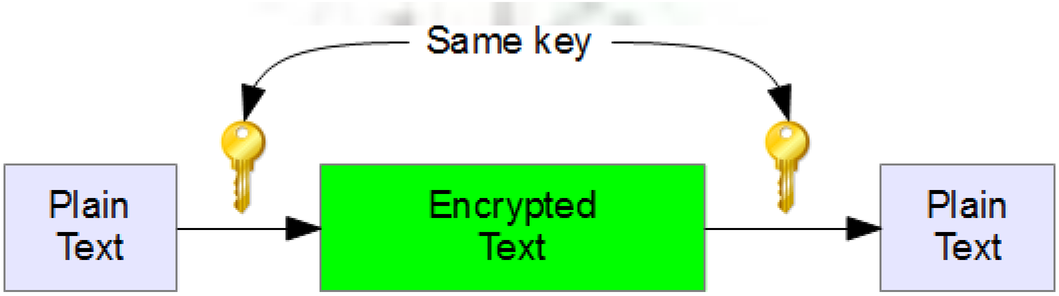
Types of Cryptography

Types of cryptography techniques given below:

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

1. Secret Key Cryptography:

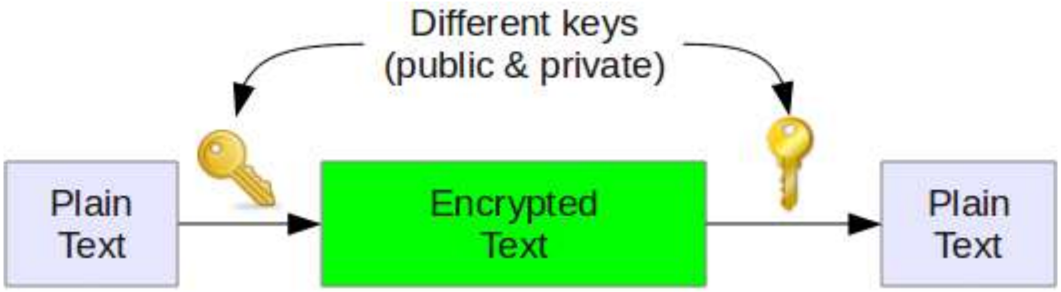
This technique uses single key. The sender uses a key to encrypt the message and receiver uses the same key to decrypt the message. Single key is used so it is called symmetric encryption.



It is no not very secured as compared to other techniques.

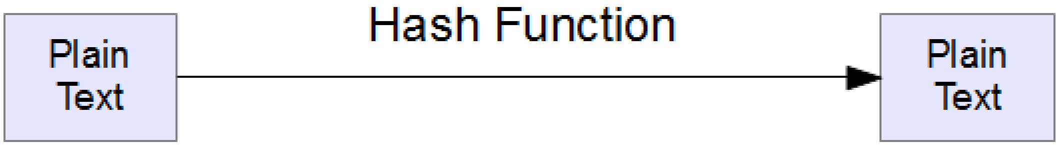
2. Public key Cryptography:

In this method two keys are used to make it more secure. Here two keys are used so it is called asymmetric encryption.



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 communicate.

3. Hash Function:



This method does not involve any key. It contains 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 daily life to make our data secure and protect it from malicious 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.

References

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