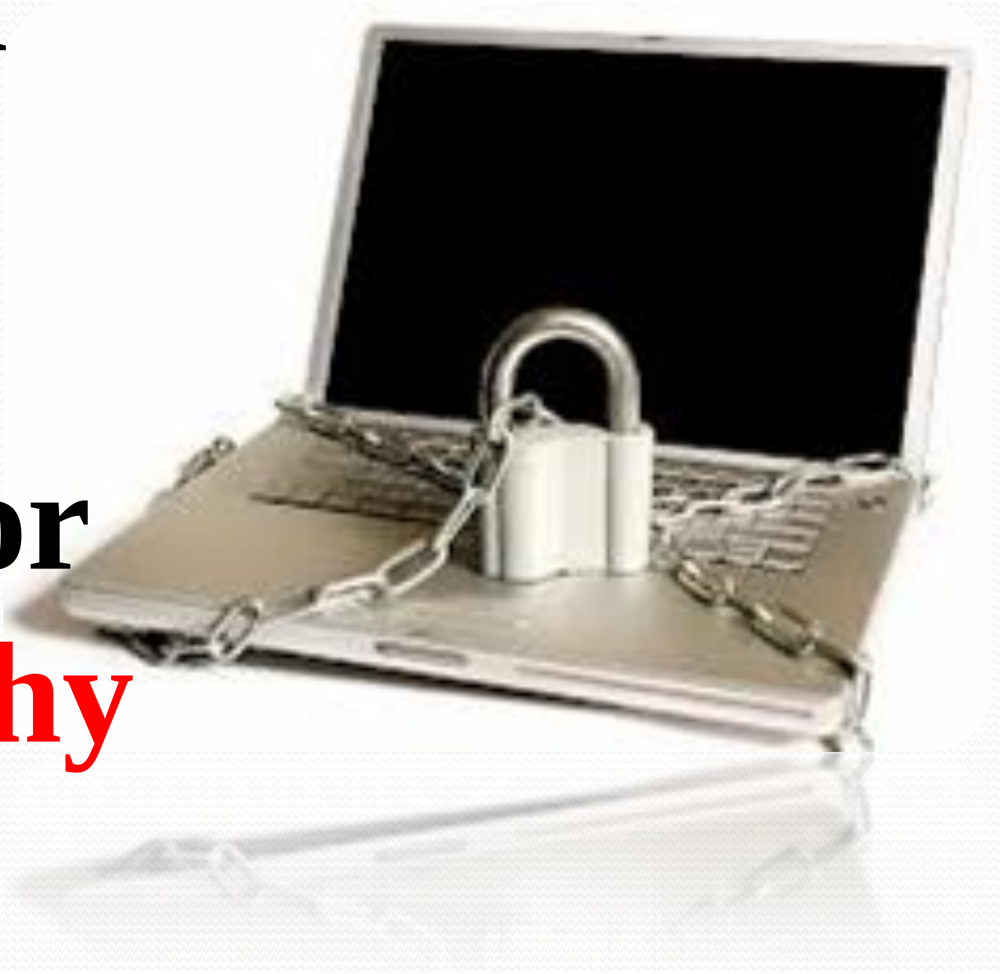
Welcome To:

The 2nd International Conference on Computer Science & Computational Mathematics

(ICCSCM 2013)

Does Data Security Matter? The Case for Cryptography



- Introduction
- Review of Cryptography
- What is Cryptography
- How Cryptography Works?
- Basic Principles of Cryptography
- Types of Cryptography
- Conclusion

INTRODUCTION

Fast growth of digital communication
Electronic data exchange,
we communicate with the world
without protection.
Exchange millions of our private
information

Using computers across the cyberspace.

Our digital footprint is in cyber space.

Whatever we communicate is unprotected

Open to cyber criminals for manipulation.

Therefore, information security is becoming one of the hot topics around the world.

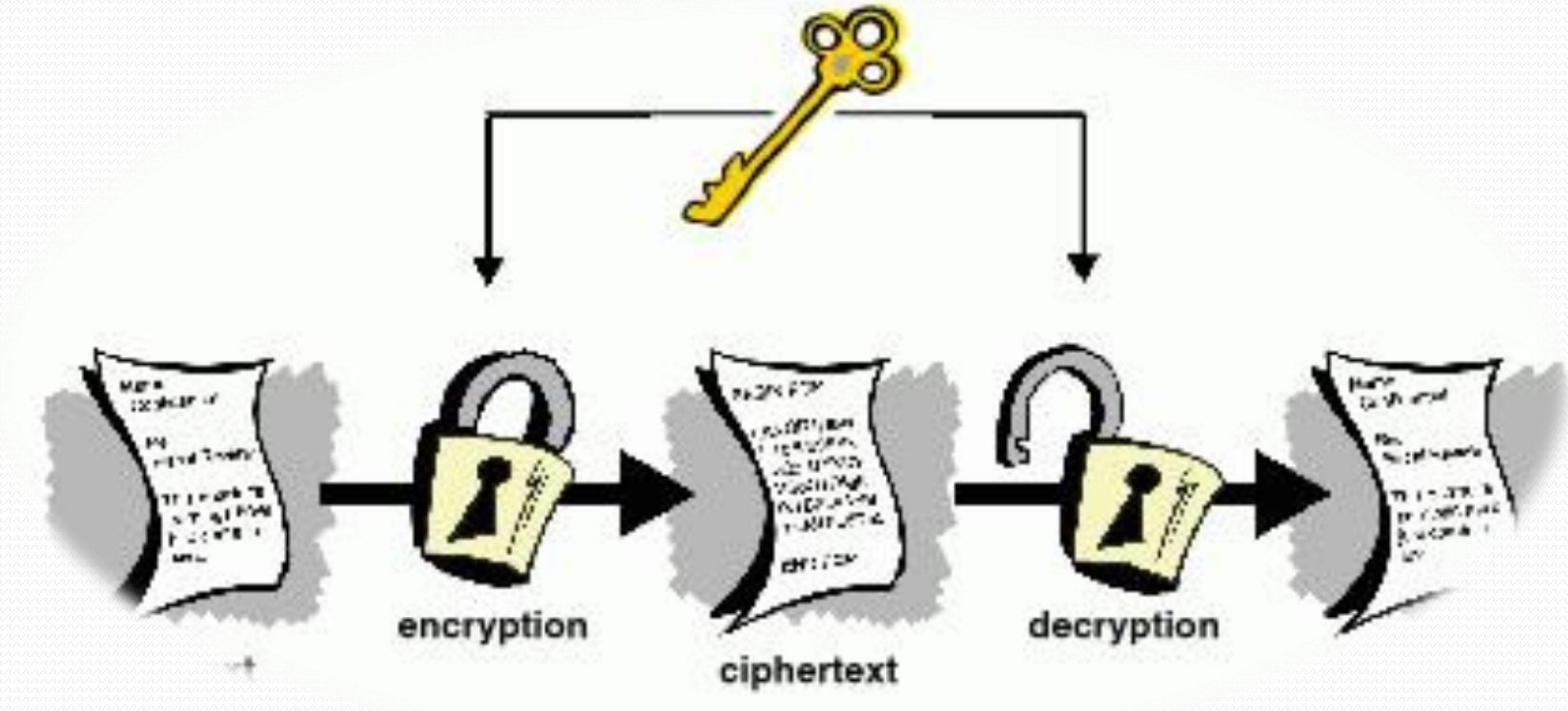
The need for modern cryptography to provide techniques and keys to protect our information is necessary.

The concept of Encryption and Decryption is highly important in communicating highly sensitive information.

We need to convert our information into unreadable form.

Our data can be protected and reaches its destination.

Review Of Cryptography



Cryptography is an ancient art.
It is first started in 1900 B.C.
It started from Egypt when an Egyptian Scribe used non-standard data in his inscription instead of using hieroglyphs.

Some scholars argue that cryptography is as old as the invention of writing.

While others indicate that, it is as old as when first military commanders planned war strategies.

It is also as old as diplomatic communications
when they attempted to code their communications.
The Most recent usage of cryptography began when people started digital communication using computers and technology.

Therefore, the need for protecting personal information was so great. Experts started to convert the plain text into unreadable codes Using mathematical concepts and Algorithm.

WHAT IS CRYPTOGRAPHY?

Copyright 1997 Hrana Janto
ALL RIGHTS RESERVED

Cryptography: to protect information

Cryptography is an artistic

transformation of data

Into an unreadable format

Only the intended

recipient

understand and use it.

Cryptography:

the art and science of hiding important and secret information from being infringed by unauthorized person. Cryptography dictates that it is about protecting and safeguarding information from cyber criminals.

Cryptography:

Enables people to communicate over internet

Transfer crucial and confidential information.

To do online shopping and evade being victimized by password sniffers.

Cryptography:

uses the latest technological advancement in computer science. Cryptography helps users and institutions to cipher and decipher their hidden messages.

So That It can be transmitted safely.

Cryptography:

Encryption and Decryption keys.
The process of coding and
transformation of plain text
Into unreadable format
is called **Encryption.**

The process of decoding and converting the unreadable text to readable information using a special digital key is called **Decryption.**

To protect our information, email, credit cards and personal data.

HOW DOES CRYPTOGRAPHY WORK?

Cryptography has two important techniques.

1. **Symmetrical Cryptography:**
2. **Asymmetrical Cryptography**

1. Symmetrical Cryptography

It uses the same digital key for encryption as well as decryption.

called secret-key, personal key, private key or shared key.

Symmetrical cryptography is a weak technique

2. Asymmetrical Cryptography:

This cryptography method uses different digital keys for encryption and decryption of information.

uses a pair of digital keys used by the end user.

One digital key is dedicated for encryption while another is assigned for decryption.

These digital keys are called public and private keys.

Both keys are different from each other.

Asymmetrical cryptography is reasonably safe and secure.

usage of a random digital key assigned by the public key keeper.

It is also called pair digital key that must be used to encrypt and decrypt the information.

BASIC PRINCIPLES OF CRYPTOGRAPHY

Encryption:

Message or information must be encrypted

Must be unreadable

The privacy of individuals is protected.

The recipient of information must decrypt

Authentication:

To identifying the origin of the information.

Authentication is only possible by providing special key exchange.

This key is performed in terms of an action

The sender must exhibit to prove identity.

Integrity:

The integrity of data by providing codes and digital keys.

What we are receiving is genuine.

It is from the intended person.

Therefore, information communicated is original and never been compromised.

Non Repudiation:

The sender of the information cannot deny the fact.

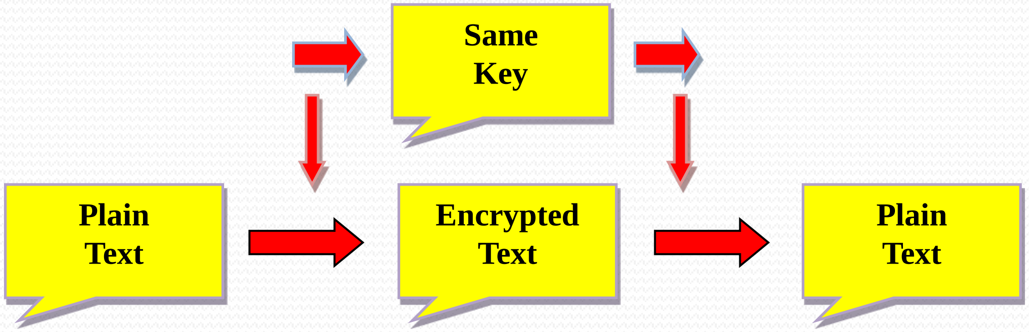
He/she never sent the information.

This principle uses digital signatures to Prevent the sender from denying the origin of the data.

TYPES OF CRYPTOGRAPHY

Secret key Cryptography:

This type of cryptography utilizes only one covert digital key. The same digital key is used for encryption and decryption.



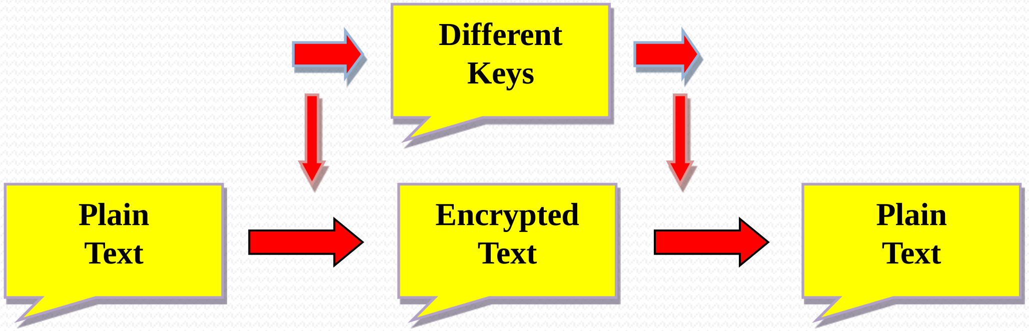
Public key Cryptography:

Public digital key utilizes a pair of digital keys.

Each communicating party has a pair of keys.

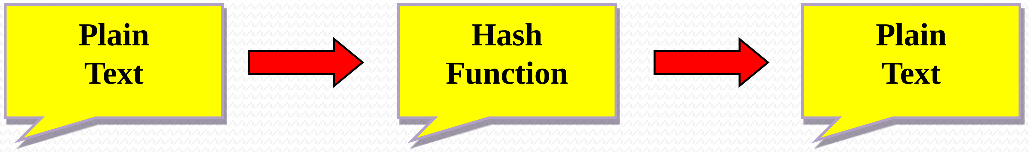
One key is secret while another is considered public.

The public key is shared among them. The public key is used to encrypt. Once the recipient gets the encrypted information. Uses secret key to decrypt the information.



Hash Functions:

This type of cryptography does not require any digital key. This type only utilizes a fixed length hash value encrypted into the plain text.



Remarks:

The concept of encryption and decryption is highly important in communicating highly sensitive information.

We need to convert our information into unreadable form.

Our data can be protected and reaches its destination safely.

شكرا