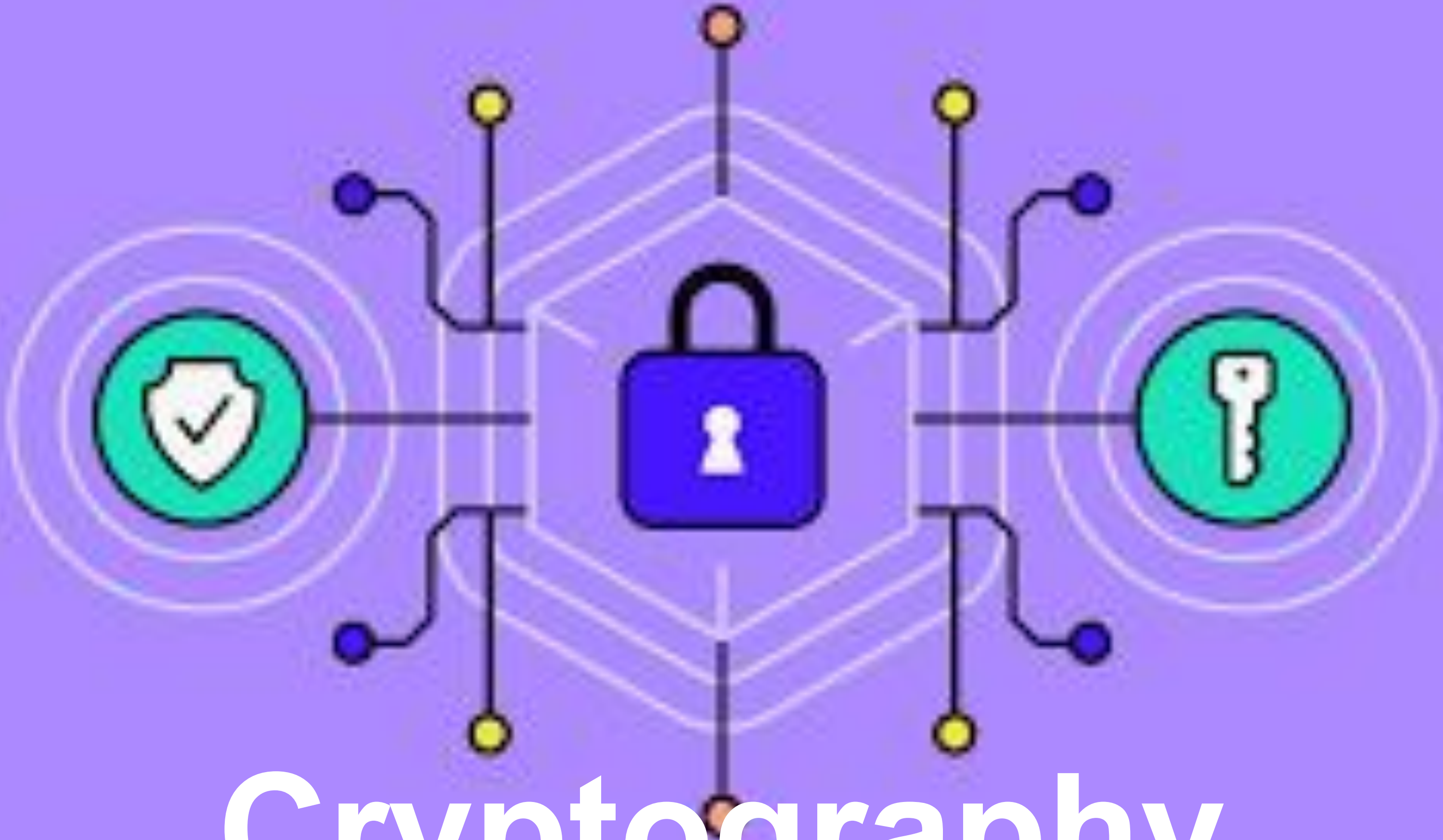


Cryptography

Cryptography

By

Rajan Nisargan

Email: rajannisargan66@gmail.com

OVERVIEW

- Cryptography
- Definition
- Terminology
- History
- Goal and Services
- Types of Cryptography
- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Functions

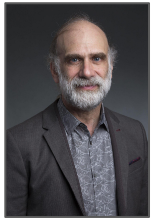
Definition

Cryptography is the science of using mathematics to encrypt and decrypt data.

(‘Phil Zimmermann’)

Cryptography is the art and science of keeping messages secure.

(‘Bruce Schneier’)



The art and science of concealing the messages to introduce
 secrecy in information
security is recognized as cryptography.

Terminologies

A message is plaintext (sometimes called cleartext). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is Cryptography A cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure.

Terminology

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system. The various components of a basic cryptosystem are as follows −

- Plaintext
- Encryption Algorithm
- Ciphertext
- Decryption Algorithm
- Encryption Key
- Decryption Key

Terminology

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

History of Cryptography

As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations.

Goal and Services

Goal: The primary goal of cryptography is to secure important data on the hard disk or as it passes through a medium that may not be secure itself. Usually, that medium is a computer network. Services: Cryptography can provide the following services:

•Confidentiality (secrecy)

•Integrity (anti-tampering)

•Authentication

•Non-repudiation.

Confidentiality (secrecy)

- Ensuring that no one can read the message except the intended receiver
- Data is kept secret from those without the proper credentials, even if that data travels through an insecure medium Integrity (anti-tampering)
- Assuring the receiver that the received message has not been altered in any way from the original.

Authentication Cryptography can help establish identity for authentication purposes The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)

Non-repudiation

A mechanism to prove that the sender really sent this message

Types of Cryptography

Symmetric Key Cryptography

Also known as Secret Key Cryptography or Conventional Cryptography, Symmetric Key Cryptography is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. The Algorithm use is also known as a secret key algorithm or sometimes called a symmetric algorithm

A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. The key for encrypting and decrypting the file had to be known to all the recipients. Else, the message could not be decrypted by conventional means.

Types of Cryptography

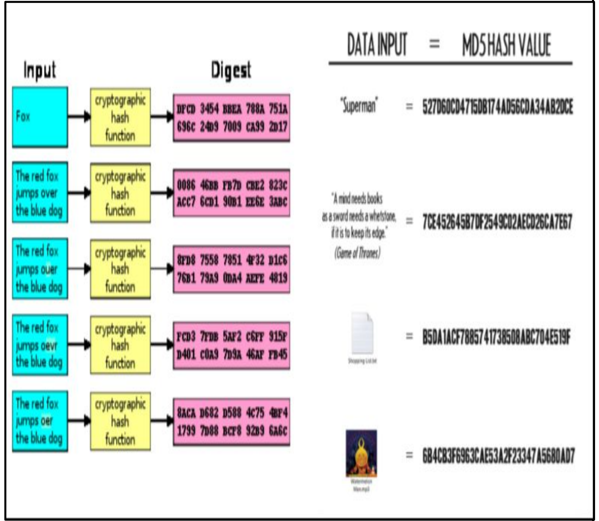
Asymmetric Key Cryptography

Symmetric-key systems are simpler and faster; their main drawback is that the two parties must somehow exchange the key in a secure way and keep it secure after that. Key Management caused nightmare for the parties using the symmetric key cryptography. They were worried about how to get the keys safely and securely across to all users so that the decryption of the message would be possible. This gave the chance for third parties to intercept the keys in transit to decode the top-secret messages. Thus, if the key was compromised, the entire coding system was compromised and a “Secret” would no longer remain a “Secret”.This is why the “Public Key Cryptography” came into existence.

Hash Functions

What is a Hash Function

A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest.


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C
DATA INPUT = MD5 HASH VALUE
"Superman" = 527D60CD4715DB174AD56CDA34AB2DCE
"A mind needs books as a sword needs a whetstone, if it is to keep its edge." (Game of Thrones) = 7CE452645B7DF2549C02AECD26CA7E67
Shopping List.txt
= B5DA1ACF788574173850 8ABC704E519F
Watermelon Man.mp3
= 6B4CB3F6963CAE53A2F23347A5680AD7

THANKS!

RAJAN N