LECTURE 8

CRYPTOGRAPHY

1. What is Cryptography?

* The science of disguising information, most commonly by encoding and decoding a secret code used to send messages.

What is the purpose of Cryptography?

* Confidentiality
* Integrity
* Availability
* Identity

Cryptography

* Protects data in transit
* Protect data in rest.
* Data in use cannot be encrypted

1. What are the three categories in Cryptography?

* Encrypt / Decrypt (Require algorithm and key)
* Hashing (Require algorithm and key sometimes)
* Encode / Decode (Require algorithm and no key)

1. What are Cryptographic Techniques?

* Reversible, symmetric (1Key - private key)
* Reversible, asymmetric (2 Key each)
* One-Way, hash

1. What is Symmetric Encryption?

* A two-way encryption scheme in which encryption and decryption are both using same key (Shared key encryption).

Common alternative names:

Secret key • Shared key • Private key

1. What is Asymmetric encryption?

* A two-way encryption scheme that uses paired public and private keys.

Private key:

* The component of asymmetric encryption that is kept secret by one party during two-way encryption.

Public key:

* The component of asymmetric encryption that can be accessed by anyone.

Key generation:

* The process of producing a public and private key pair by using a specific application.

1. What is the difference between symmetric and asymmetric key?

* Symmetric key both share the same key and asymmetric key two separate key
* Symmetric is faster and asymmetric is slower

1. What is Hashing?

* A process that transforms plaintext to ciphertext that cannot be directly decrypted.