Scribe: Cryptography and Network Security (Class.1)

Rutwik Pandit (20CS60R13)

September 2020

1 Introduction

The Transfer of Information is a fundamental component of human society.The role of cryptography has always been to help facilitate this transfer of information. A modern information system can be characterised as having three components.

- Sender: The sender who wants to send a piece of information through an available channel.
- Channel: The channel which is always assumed to be unsecured.
- Receiver: The receiver who cannot easily check the integrity of the received information.

Thus to ensure the transfer of information we use a cryptographic system.The use of any cryptographic system is to achieve the three fundamental goals of cryptography.

- Confidentiality: Hiding information from unauthorized access.
- Integrity: Preventing information from unauthorized modification.
- Availability: Should be easily available to authorized users.

A Cryptographic system has two major parts

- Encrption: It takes plaintext and key as input and outputs ciphertext.
- Decryption: It takes ciphertext and key as input and outputs plaintext.

There are two types of cryptographic systems , which depend on having access to a auxiliary secured channel of communication.
Symmetric Key cryptosystem is where the same key is used to encrypt and decrypt , but this kind of system requires the need for a secured auxiliary channel for the initial key exchange.

Asymmetric key cryptosystem is where there are two sets of keys , a public key and a private key. The sender uses a public key to encrypt the data and only the receiver with the private key can decrypt the data.The public key can be thought of as a lockbox mechanism where anyone can store information in the lockbox, but only the receiver has the keys to open that box thus asymmetric key cryptography does not need a secured channel for key exchange.

Kerckhoffs Principle talks about the assumptions in cryptography.

- The system is completely known to the attacker.
- Only the key is secret.

As counter-intuitive as it might seem the foundation of a strong cryptosystem is non-secrecy.The strength of cryptosystems rely not on security through obscurity , but through the use of cryptographic principles.

2 Cipher Techniques

2.1 Shift Cipher

The Shift cipher is a cipher technique where you add a constant factor (key) to your plain text and then take the modulus to encrypt.
eK(x) = x+K mod 26.
To decrypt the shift cipher the same procedure is done in reverse ie , subtract by the key value and take modulus.
dK(x) = y-K mod 26

2.2 Substitution Cipher

The Substitution cipher is a cipher technique where you create a table of mono-alphabetic substitution.Thus for 26 characters 26! permutations exist.

2.3 Affine Cipher

The Affine cipher is a cipher technique where the encryption function is given as:eK(x) = ax + b (mod 26). The value of b can be any number , but a has to be coprime with 26 for the function to be invertible.
The decryption function is given by : dK(y) = a^{-1} (y – b) (mod 26).

References

Lecture slides