

Goals of Network Security:

- Data Integrity
- Data Confidentiality (Secrecy)
- Availability
- Authentication
- Non-Repudiation
- Prevention of Unauthorized Access (Access Control)
- Securing Critical Data

Threat Model (The Evil Post-Office Analogy):

We can consider the network as an evil post office system, where nobody can be trusted.

Starting with this analogy, we can define the threat model for Network Security. An attacker can:

- Read a message not meant for him
- Alter the content of the message
- Know the destination/source addresses
- Alter the destination/source addresses
- Remove a message from the network
- Spam
- Inject his own message
- Delay a message
- Replay a message
- Re-order a sequence of messages
- Any combination of the above

History of Cryptography:

- The earliest uses for communicating chemical recipes
- Used for confidential communication during wars
- Caesar Cipher: Replace each letter of the alphabet by the fourth next to it, wrap around at the end
- Random substitution: Randomly substitute each letter in the message on the basis of a key. Frequency analysis still possible.
- Rotor machines: Mechanized substitution based on rotors rotating at varying speeds. Frequency analysis not possible. E.g. Enigma. Broken by Alan Turing

What is an Encryption Scheme:

An encryption scheme is a triple (G, E, D) where

G: Key Generator

E: Encryption Algorithm such that $E(\text{Key}, M) \rightarrow C$

D: Decryption Algorithm such that $D(\text{Key}, C) \rightarrow M$

For all Key, M: $D(K, E(K, M)) = M$

The Perfect Solution : The One Time Pad

- Invented in 1917 by Major Joseph Mauborgne and Gilbert Vernam. Proved secure by Claude Shannon.
- Use the key as long as the plaintext. The key is used only for one message and discarded after

that.

$$\text{len}(K) = \text{len}(M) = \text{len}(C)$$

$$K, M, C \leftarrow \{0,1\}^{\text{len}}$$

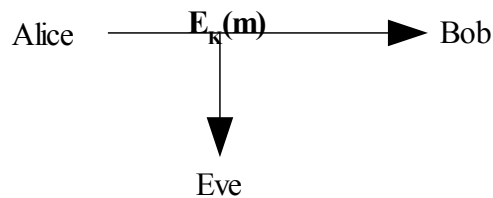
- The ciphertext is the XOR of the Key and the plaintext.

$$E(K, M) = K \text{ (XOR) } M = C$$

$$D(K, C) = K \text{ (XOR) } C = M$$

- If the key is reused, the attacker can take the XOR of the two ciphertexts and in effect he has the XOR of the two plaintexts.

Information Theoretic Security:



For a message of length l from the set $\{0,1\}^l$ where all the messages are equally likely, the probability that the given message is a particular message from the set $\{0,1\}^l$ is:

$$\Pr [M=m] = 2^{-l}$$

Then if the attacker has access to only the ciphertext the conditional probability of m should remain the same i.e. the presence of ciphertext should not reveal any information about the plaintext

$$\Pr [M=m | C=c] = 2^{-l}$$

Theorem:

Fact: If (G, E, D) is an information theoretically secure encryption scheme then:

$$|\mathbf{Keys}| \geq |\mathbf{M}|$$

Proof:

$$\text{Let } c \in C \text{ and } S = \{ D(K, C) | k \in \mathbf{KEYS} \}$$

$$\Rightarrow |S| \leq |\mathbf{Keys}|$$

Every plaintext must be in S because every plaintext must be a possible decryption of C . Hence

$$|\mathbf{M}| \leq |S| \leq |\mathbf{Keys}|$$

$$\Rightarrow |\mathbf{Keys}| \geq |\mathbf{M}|$$

Hence Proved.