**FUNDAMENTALS OF CRYPTOGRAPHY LEC 01**

**Information Security**

It is the protecting of information (using, viewing, modifying, destroying etc.)

**Confidentiality** – Information is only seen by authorised users.

**Integrity –** Modification is not permitted.

**Availability** – Information is available to legitimate users.

**Authentication** – Legitimate users can be verified.

**Non-Repudiation** – Requires that sender or receiver cannot deny the sending or receiving of a message.

**Access Control** – Authorisation is required for a particular user to get access to data.

**Symmetric/Asymmetric Ciphers**

A symmetrical cipher would use the same key for both encryption and decryption.

Symmetric – Conventional cryptography

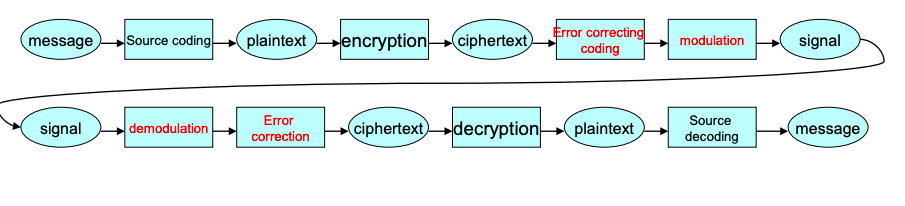
**Unconditional Security** – Security level is independent of the computational capacity of the attackers**.**

**Computational Security** – Security is measured in terms of the amount of computing.

**Theoretical Security** – Security can be proved

**Practical Security** – Security is based on an assumption

**Conventional Cryptosystem**

A message is encrypted with a key and sent on a public channel to the receiver. Along this public channel there is possibility of an attacker. The key which is used for encryption/decryption is send over a secure channel. 

**Plaintext ‘m’** – Normally a binary string converted from a message

**Cipher-text ‘c’** – Output of plaintext after encryption

**Encryption c = Ek(m)** – An algorithm transfers plaintext to cipher-text

**Decryption m = Dk(c)** – Inverse of c = Ek(m)

**Key ‘k’** – Secret information used in encryption/decryption

**Plaintext space (Set)** – set of all possible plaintext

**Cipher-text space (Set)** – set of all possible cipher-text

**Key Space** – set of all possible keys

**Key size** – size of memory required to store the key

**Passive Attacks**

Basic form of attack where the attacker doesn’t alter the information and instead read or analyse. They become threats if the attacker gains benefits. Eg. release of message contents, traffic analysis.

**Active Attack**

These sorts of attackers require the attacker to modify the information being transmitted. They become threats if they are undetectable.

* **Replay** – Re-use of message which has been expired or becomes unauthorised.
* **Masquerade** – An entity pretends to be a different entity
* **Modification** – Modifies the content of the message illegally
* **Denial of Service** – System is made to deny services for reasonable requests

**Shannon’s Theory**

A one-time-pad is theoretically secure and if it were to be used more than once would leak information. This is should be generated at random.

**Diffusion** – Messaged should be arranged in a totally random way after encryption. Only the message is mixed in order

**Confusion** – Message and key should be mixed completely. Both message and key is mixed.

**Caesar Cipher**

It’s a mono-alphabetic cipher where the letters a-z correspond to number 0-25.

Key is a number between these two numbers. In simple terms this cipher works by shifting the letters down a certain amount. (ie. A becomes B, B becomes C).

For encryption: c = (m + k) mod 26

For decryption: m = (c – k) mod 26… or m = (c + (26 – k)) mod 26

Where m mod p = the **residue** after m is divided by p.

The Caesar cipher has 26 possible keys and is not even secure to hand calculations.

**Affine Cipher**

It’s a mono-alphabetic cipher where the letters a-z correspond to number 0-25.

Key is two number 0 <= a, b <= 25 where a is a co-prime to 26.

For encryption: c = f(m) = (a m + b) mod 26

For decryption: m = f­-1(c) = a-1 (c – b) mod 26

(a-1 \* a) mod 26 = 1 is the definition of a-1. Ie. If a is equal to 5. The inverse is 21 since 21\*5=105 which modded by 26 is equal to 1.

There is only 12 possible options for a due to the necessity of it having to be inverse and thus there are 312 combinations of a and b (26\*12). This means it is easy to break with computers as there is few combinations of keys and can be brute forced.

**Permutation Cipher**

It is a generalisation of the Caesar cipher but you replace the cipher line with an arbitrary permutation of the 26 letters.

Number of possible keys is 26! Or 403291361126605625584000000

However, the key size is log226! Or 90 bits!