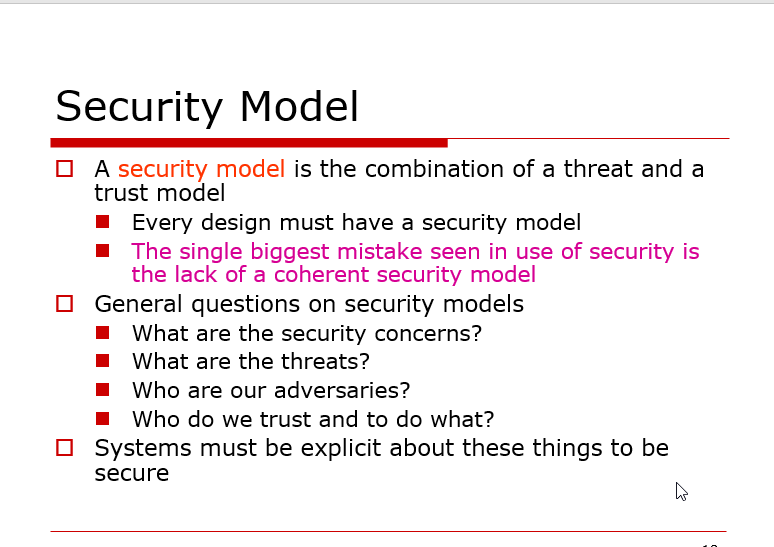
CIA:

Confidentiality, integrity and availability.

Confidentiality: prevent unauthrised read of information. Cryptography is used for this

Integrity:- detect un-Autharised write to file, i.e user shouldnot be able to change it own account balance. Crypto is used

Availablity : Data is available in a timely manner when needed. No DDOS



* A trust model describes, for a particular environment, who is trusted to do what?

Basic principle:

1. Principle of weakest link
2. Principle of effectiveness : conrols must be used and used properly

Krichoffs principle : all crypto algorithm and known to attacker, only key is secret

Simple substitution with shift by 3 **is Caesar’s cipher**

**Secure system requirement:**

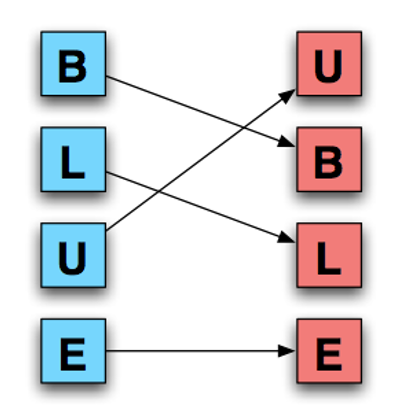
1. Large key space: exhaustive search takes too long
2. No shortcut attacks: no better then exhaustive search

**Cipher design principle:**

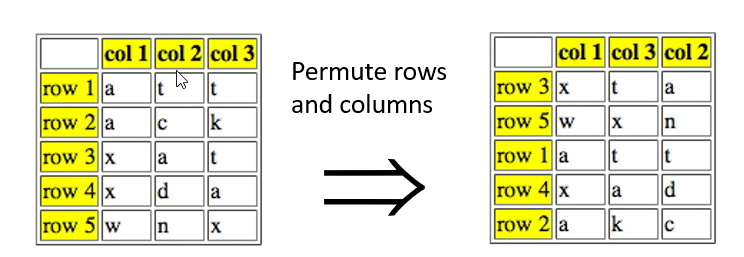
**Confusion**: making the relationship between the **cyphertext** and the **symmetric key** as complex and involved as possible.

Diffusion: *diffusion* refers to making the relationship between the **plaintext** and the **ciphertext** as complex and involved as possible **(so that the plaintext statistics are spread over the ciphertext**).

Classical substitution ciphers:

1. S-box 6x4 i.e substitution box
2. Permuation cyphers: scramble to produce output
   1. 

Double transposition



One time pad:

Public crypto provide:

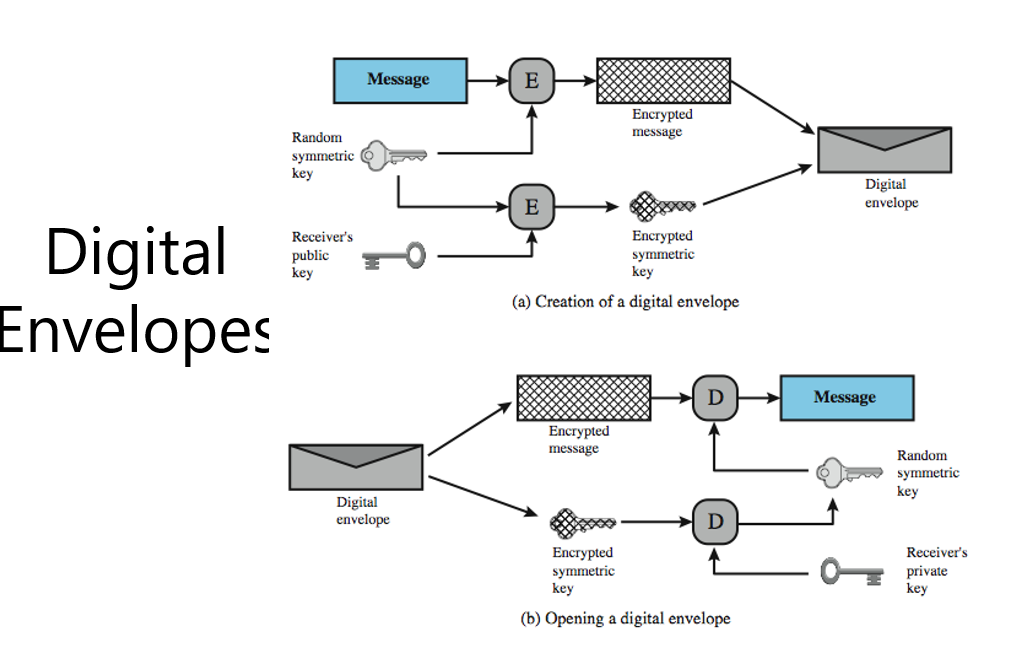
Confidentialty

Authentication

Digital signature provide integrity and non-repudiation

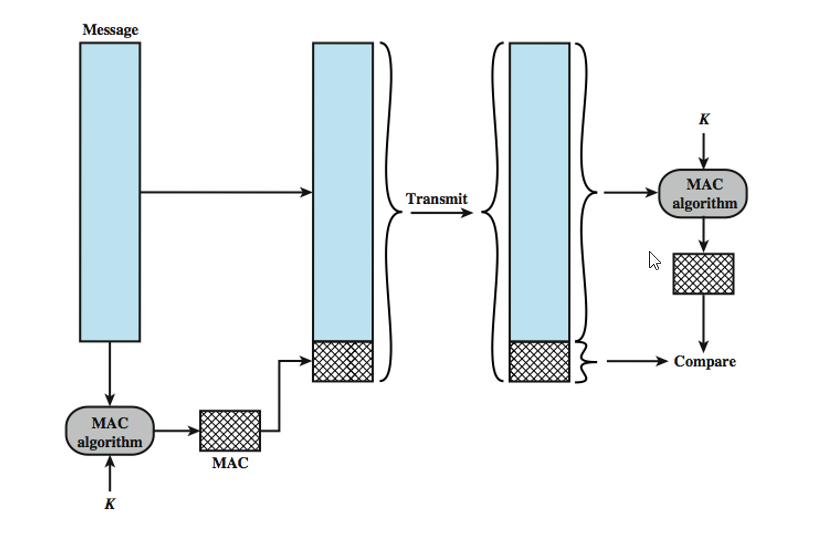
PKI trust model

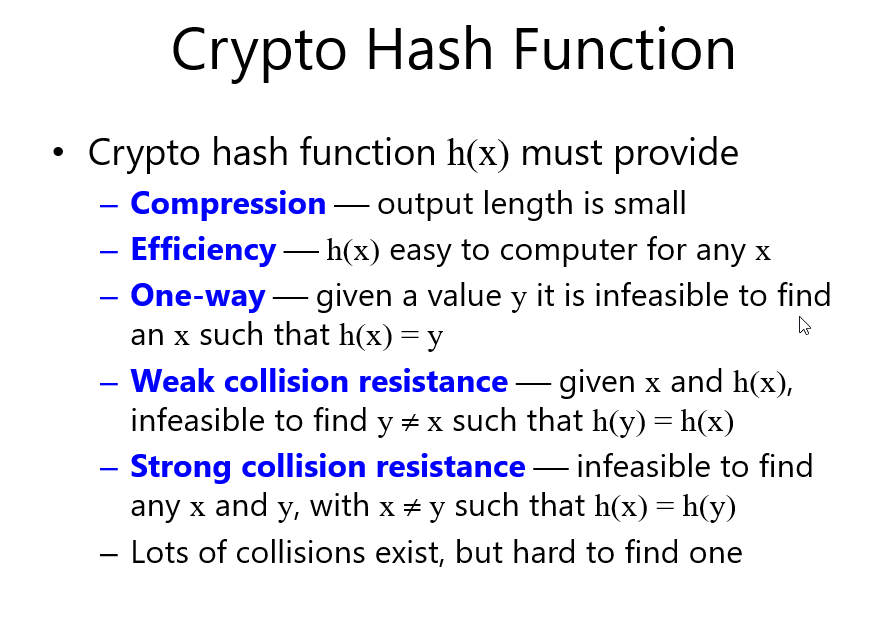
1. Monopoly model : universal single CA,
   1. Big problem: what if CA is compromised or we can’t trust CA
2. Oligarchy: multiple CA model, we can choose which one to choose
3. Anarchy model:
   1. Everyone is CA,
   2. User must decide which one to trust
   3. If I don’t know frank but I know bob and bob is vouching for frank the I can trust frank



Data integrity : Different from encryption

MAC :- message authentication code





Avalanch effect : change in 1 bit of input produce enterly different output

Information handling:

1. Stagnography: insert information in low order RGB
2. Watermark :
   1. Robust watermark
      1. Robust:- readable even if attacked
      2. Fragile : damaged if tried to modify

Authentication:

One way othernticatiion, where only one side authenticate.. but its not good

