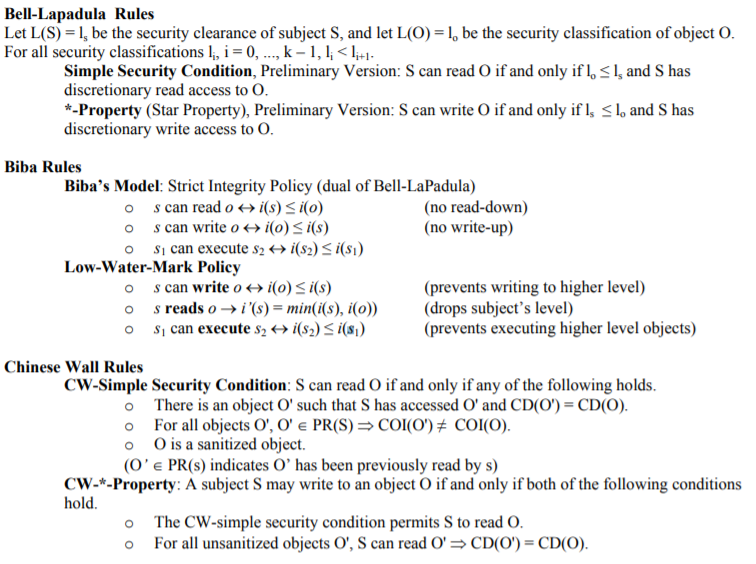
# Security Policy Models

* Low Mark Water vs High Mark Water: <http://www.cs.sjsu.edu/~stamp/CS265/SecurityEngineering/chapter8_SE/solutions8.html>
* Integrity Policy and Lattice policy and Bida model with, “no read down, no write up”
* Confidentiality Policy and Bell-LaPadula can be summarized as: No read up, no write down. (high mark water)
* Hybrid Policy Model
  + Chinese Wall (conflict of interest)
  + RBAC (the importance of role)
* Definitions: <http://www.sis.pitt.edu/jjoshi/IS2150/Fall07/definitions.pdf>



# Hash Functions

"One-way" means that given a function output, you cannot find a matching input, except by trying many potential inputs and getting lucky. A collision is about finding two distinct inputs which yield the same output, without any predefined constraint on said output.

There are three classical properties which a good (cryptographic) hash function should have:

1. *Preimage resistance*: Given H(x), it's hard to find x
2. *Second preimage resistance*: Given m1m1, it's hard to find another m2 such that H(m1)=H(m2)
3. *Collision resistance*: It's hard to find any two distinct messages m1, m2 such that H(m1)=H(m2)

# Public Key Cryptography:

Public crypto example:

1. Alice generates two prime numbers that have similar size : 53 & 59
   1. **n** = 53\*59 = 3127
   2. Phi of n : ɸ(n) = (53-1) (59 – 1) = 3016
   3. Pick **e** ( e is odd and doesn’t not share factor with n, or relative prime of n) : 3
   4. Private key for decryption: = = 2011
   5. Public key is made of **e** and **n**. They are sent to Bob.
2. Bob wants to send Alice a message “89”. Bob encrypts the message by doing:

c = 893 mod 3127 = 1394.

1. Alice uses private key **d** to decrypt the message:

cd mod n = 1394 2011 mod 3127 = 89