3.4 Another introduction to Hash Functions.

→ 3 main Requirements of Hash Algorithms.
i. Speed
ii. Avalanche Effect :- If one bit of Message changes whole hash changes.
iii. It ~~is~~ should avoid the Hash collision.

It is possible to check the bits and create hash collision. Example MD5.

→ Problems with MD5 are
→ Bad way to store passwords.
→ It is overy used in the web.
→ MD5 is mainly used in File transfers, Download,

3.5 Password Management : Hash and Salting

→ One should not ~~to~~ store passwords.
Bad ways of storing passwords.
1. Storing password as it is.
2. Encrypt the password & store it.
3. Only using the hashing and store it. Rainbow table helps to break these passwords.

→ Hashing and salting is the best way to store passwords.
→ salt is a random string of characters. which is different for every single user.