Chp 11:-

1) req. of strong hash f.n.

1- Variable input size
2- fixed output size
3- efficiency
4- preimage resistant (one-way property).
5- second preimage resistant (weak Collesion resistant)
6- Collision resistant (strong collesion resistant)

⇒ req. of weak hash f.n is the first 5 points in the strong hash f.n.

2). Since hashing generates a text that is not readable it can provide Confidentiality?

→ bec. in some message authentication techniques the encryption is applied to the entire message plus hash code ∴ So Confidentiality is provided

∴ while in other tech. only the hash code is encrypted
∴ no Confidentiality is provided.

3) hash func. requirements

1- Variable input size 2- fixed output size
3- efficiency 4- preimage resistant
5- second primage resistant 6- Collision resistant.
7- Pseudo randomness

4) what are the characteristics needed in Secure hash function? SHA

* they have variable input length and fixed output length
* they are one way functions, where it is infeasible to use the resultant hash value to generate the input text other than trying each possible input text (Computationally impossible for large inputs)
* if the same input message is fed to the SHA function, it will always generate the same resultant hash
* it's not possible to generate the same hash value, using two different input values, this called (Collision resistance)
* a small change in the input value, even a single bit. Completely changes the resultant hash value this called the (avelanche effect)

5) what is weak and strong Collision resistance?

- weak Collision resistance is bound to a particular input
- strong Collision resistance applies to any two arbitary inputs.

6) what are the three ways to do authentication??