Assignment-04

Answer to the Question-01

a. It's more secure to store hashed passwords because they are compared to y, and if $y = h(x)$ then the entered password is assumed to be correct and authenticated. So, even if someone gets the password file, they wont be able to authenticate or ~~log in~~ use the password in anyway.

b. It is much better idea to hash passwords stored in a file than to encrypt the password file because it is much easier to decrypt the file than to find the password from hashed password. If salt is used with Hash password, it beomes even more difficult for the ~~[illegible]~~ intruder as he has to re-compute dictionary washes for each user.

c. Salt is randomly choosen value that is only known to me. So, we choose a passoword and a random value which is salt in this case and store the 'hashed password. St is used whenever passwords are hashed because it makes the work of intruder harder while cracking the hashed password because he has to re compute dictionary hashes for ~~us~~ each user.

x

Answer to the Question-2

a) If an user A is authenticated as user B it is called fraud. The Rate of this fraud in biometrics is called fraud rate.

b) If an user A cannot authenticate as user A, then it is called insult. The rate of this insult in biometrics is called insult rate.

. The rate where fraud rate and insult rate are equal is called equal error rate It is used for ~~computing~~ comparing different biometric system

Answer to the Question-3

d(Alice, BOB) = d(BE439AD598EF5147,
9C8B7A14253695E4)

$$= \frac{15}{16}.$$

d(Alice, Charlie) = d(BE439AD598EF5147,
8855223366 99CCBB)

$$= \frac{16}{16} = 1$$

d(Bob, Charlie) = d(9C8B7A14253695E4,
88552233669 9CCBB)

$$= \frac{16}{16} = 1$$

Scanned with CamScanner

Answer to the Question-4

comparison between different authentication technike is given below:-

Password	Biometrics	smartcard
1. It is something we know.	1. It is something we are.	1. It is something we have.
2. passwords are free.	2. Some of the biometric system are expensive.	2. It is cheap ~~and maybe~~ compartively.
3. **Example:** PIN, Date of birth, social security no. etc	3. **Example:** Fingerprint, facial Recognition, Speech Recognition etc	3. **Example:** ATM: card and pin credit card: card and signature
4. password cracking is too easy and have many issues.	4. It is not easy to crack. But it has issues with fraudand insult rate.	4. If the possessod thing is lost, hacker can easily take control of accounts.