Assignment 4

Tasnim Sakib Apon
ID : 20241068
CSE 490

Tasnim Salib Apon Assignment - 4

20241068

1 a. Hash passwords that are stored in a file is a good idea than storing password in a file. In this hash password system we use store y=h(password) and the compared to y and if y=h(x) then the entered password is assumed to the connect and also authenticated.

b. It is a better idea because she doesn't obtain the password directly and something she has to do to verify password which is called ~~boo~~ for word search.

c. Salt is a random data that is used as an additional input to a one way function that hashes data, a password or passphrase. Salt are used to safegard passpword in a ~~stog~~ storage.

To prevent a forward search attack on public key encryption we append random bits to the message before encrypting. We can accomplish a ~~sim~~ similar affect with passwords by appending a non-secret random value named as salt to each password before hashing.

2 a. Fraud rate is when someone poses as someone and it authenticates.

b. Insult rate is when someone authenticates but the system denies.

c Equal error rate is when fraud rate and insult rate are equal and it is useful for balancing security and actually getting someone through the system.

3 $d(Alice, Bob) = \frac{29}{64}$

$d(Alice, charlie) = \frac{39}{64}$

$d(Bob, charlie) = \frac{39}{64}$

Alice ⇒ 10111100100000111 00110110 0101011 0011000
1110111010100010 00011.

Bob ⇒ 10011100 0001011 01111 01000010 10000100
10100110110110100101100001001.

charlie ⇒ 1000 10000101010100 0001000 1100
11011001101001100111011001011011

4

Finger Print Recognition	Facial Recognition	password.
(I) User consent is required.	(I) User consent is ~~required.~~ may not be required.	(I) User consent is not required.
(II) Highly accurate.	(II) Low accuracy.	(II) Accuracy depend on the password.
(III) Extensively used in identification and authetication	(III) Extenslely used in surveillance & public application	(III) Commonly used in all platform.
(IV) Subject can not be identified from a distance.	(IV) Subject can be identified from a distance.	(IV) Distance is not a issue.
(V) High cost	(V) High cost	(V) Low cost
(VI) Small template size.	(VI) Large template size	(VI) Not needed.