**Task 3.1 (theoretical): Authentication Beyond Pass-**

**Words**

**Part a**

**1. Biometrics:**

In this technique completely private information of a person is used to act as authentication media such as finger print, voice, heartbeat, eye, etc.

**Advantage:** Biometric information is unique. That is, two people can never have the same finger print but people can have same passwords.

**Disadvantage:** We can change a password thousand times but we cannot change our heartbeat or finger print. If somehow a hacker steals someone’s finger print then the person is as good as dead, he has to get new finger.

**Use:** Samsung Galaxy S6 edge. As a way to unlock the phone.

**2.Token:**

In this technique a user is provided with a unique piece of data such as, a picture, a sound clip etc. to act as authentication media.

**Advantage:** It can provide a second layer of authentication when used along with password which is easy and low cost and gives more security than using only password. The user can forget password but with token there is no chance for that.

**Disadvantage:** A digital media is required to carry the token.

**Use:** FlixBus (a travel bus company) provides its travelers with barcode tokens and authenticates them by reading the token with mobile phone camera. I know it as I use this bus service to travel every time.

**3.Temporary and single password:**

In this technology when a user wants to login to a service every time the service provider sends a temporary and new password directly to the user phone by SMS. This technology was proposed by Yahoo! In 2015.

**Advantage:** Users don’t need to remember their passwords and as the password is renewed every time a hacker cannot trace it.

**Disadvantage:** The phone which receives the password could be lost or stolen, then who ever have the phone can login as a real user.

**Use:** To access Yahoo ! mail from 3rd party apps like iOS mail, Android mail or Outlook Yahoo! Requires user to use this technology.

**Part b:**

**Two Factor:**

In this technique along with password a second media is used to provide strong authentication.

**Advantage:** Hackers may get my password but he/she cannot get the code number which is directly sent to my phone by the website or server of a particular organization as a second factor of my authentication.

**Disadvantage:** If the media that carries the second factor after password is somehow not accessible then a user cannot login to the particular service which can cause a big issue. However, in pure password based authentication the users carry their passwords in their mind which they can access any time if they are alive.

**Use:** While transferring money online, a user needs to use both of his/her bank pin code and TAN.

**Task 3.5**

**Part a:**

**Is this method secure?**

Yes this method seems secure to me because every time when the secret box is traveling, it is protected with at-least one padlock.

**Does it also work with cryptographic means?**

It works with cryptographic means.

**Which problems could arise?**

From my point of view, the main problem is time that it takes to complete the whole process.

Also, to transfer the box between the sender and receiver two times will include more cost.

**Part b:**

Does it work?

Yes.

Example:

Assume,

Digital data = 11 00 00 01

Bob’s key = 11 11 00 00

Alice’s key = 00 00 11 11

**Step 1:** Bob sends the data by doing a bitwise XOR with his key to Alice

Digital data ^ Bob’s key = 11 00 00 01 ^ 11 11 00 00 = 00 11 00 01= Encrypted data.

**Step 2:** Alice receives the encrypted data and performs again a bit wise XOR on it with her key

Encrypted data ^ Alice’s key=00 11 00 01 ^ 00 00 11 11= 00 11 11 10 = Encrypted data with both keys.

**Step 3:** Now Alice sends the double-key-encrypted data to Bob again so that, he can remove his lock by doing bit wise XOR on it again with his key.

Encrypted data with both keys ^ Bob’s key = 00 11 11 10 ^ 11 11 00 00 = 11 00 11 10 =Encrypted data with only Alice’s key.

**Step 4:** Now Bob sends the data back to Alice again where she performs bitwise XORs on it with her key and gets the actual data.

Encrypted data with only Alice’s key ^ Alice’s key = 11 00 11 10 ^ 00 00 11 11 =

11 00 00 01 = Actual Digital Data.

**Can confidentiality be assured?**

From my point of view not completely. Because a hacker can pose as Alice and perform her role and Bob has no way to identify Alice because Bob doesn’t have any information about Alice’s key.

**Can integrity be assured?**

Yes, because during transmission no bit of the data is lost. Otherwise, while performing XORs with a key, the decrypted data will not match the right data.

**Would choosing different random keys for each message have an impact?**

Choosing random key for each message will increase the security because then the hacker cannot trace them. Hackers can only know the key length as it is same as the data size.