FCS Assignment 1

-Dewangee Agrawal (2016034)

Question 1 :

1) Alice -
    a) Very Weak
    b) Since the password of the user is her name, this can be guessed by the hacker easily via Brute Force (No numbers or symbols)
2) Qwerty1234 -
    a) Weak
    b) This password can also be guessed even though it has both letters and numbers.
3) Rat$you -
    a) Neutral
    b) Has both letters and a symbol in the middle which can't be cracked easily. (But no number).
4) Elppa -
    a) Very Weak
    b) It has only letters and no symbols or numbers.
5) Mumbai -
    a) Very weak
    b) It has only letters and no symbols or numbers.
6) Mfiical4W
    a) Neutral
    b) Has both letters and a number in the middle which can't be cracked easily. (But no symbol)
7) Tif#hom&851@ -
    a) Very Strong
    b) Has letters (upper and lower case), numbers and special characters in the middle and end of the string.
8) #$\%@$^$^@$@# -
    a) Neutral
    b) Contains only special characters
9) ecila!0987 -
    a) Strong
    b) Contains letters (not upper case)
    c) Numbers and special characters at the end of the string
10) 45649243 -
    a) Very weak

b) Contains only numbers
c) Can be guessed by Brute Force.

Question 2 :

For gaining access to the various portals of the college, and accessing the resources/ data offered, the following components are used to design a system for the students, faculty, employees and visitors.

- **Students, Faculty and Employees**
    - A unique roll number or identification number is assigned by the college administration to the students, faculty and employees.

      Physical Access -

    - A college ID must be issued to each member with their respective identification. This can be used for entry to the college.
    - For access to labs, classrooms and meeting rooms, the use of biometrics is favourable. Fingerprints of authorized users must be recorded and only them should they be allowed entry for the same.

      Internet Access -

    - An email address is assigned to each of the above members in the IIIT domain and a random password is generated for the same. These email addresses would be used to access all IIIT portals.
    - Each member is assigned access to different databases and information according to their role - students, faculty and employees.
    - The email address can be created using-
        - A BTech student's first name and roll number.
        - An MTech student's first name and Mtech roll number.
        - A PhD student's first name and PhD serial number.
        - A faculty or employee's first name and last name (identification number in case of same names)
    - The passwords generated must be changed by the individual users to ensure security. To avoid password guessing etc, the passwords must be strong and checked for the following-
        - Must be 8 letters or more
        - Uppercase and lower letters

        - Numbers
        - Special Characters
    - The users will need to enter an OTP every time they log in with their email addresses into a new system or browser. This OTP will be sent to their mobile number for a two-factor authentication.
    - All members must be assigned network IDs via which they can access the IIIT wifi. These network IDs can be their email addresses. The password generated for this is also random and needs to be changed by the user.
    - The users must also get their device (phone and laptop) mac addresses registered by the IT department, so that even if someone gains unauthorised access of the network information, they cannot access it via a different device.
    - The users are responsible for all of their logged in sessions. Hence, for any breach of security within that logged in session, the user is held accountable. Hence, it is necessary for them to keep their passwords confidential.
    - For any instance of compromise of their password, they must report to the IT department immediately.
    - The IIIT portals can be accessed only by the college wifi and with correct authentication via network IDs. This prevents remote attacks.
    - The email addresses and network IDs would be revoked when a students passes out or leaves college and a faculty or an employee leaves college. They can also be revoked when a student/ employee is to be suspended of college privileges.
    - When a password is entered by the user, it must not be saved as clear text. The file can be encrypted via an encryption key and decrypted accordingly. However, a safer version for the same is storing the passwords in hash tables. These hash functions are one-way functions which cannot be reverted to form the password and the attacker can not guess it.

- **Visitors**

    Physical Access -

    - Visitors are allowed access to the restricted areas of the campus by permission from the concerned authority.

    Internet Access -

    - Visitors are required to Sign-up to the IIIT website via their email address, phone number and a reference by a member with a network ID.
    - An OTP is then sent to both the referee and the visitor's email addresses.
    - The visitor is allowed access only after both of these are entered correctly and for a limited time period of 3 hours.

Attacks -

- Password Cracking -
    - Threat -
        - The various techniques of password cracking include password guessing via social engineering, dictionary attacks and brute force attacks. If the password of the user includes his name or digits at the end, it is easy for the hacker to guess it by the given methods. The passwords can be guessed even if they're saved in a clear text format.
    - Measure -
        - To prevent the hacker from guessing the passwords, we put a check to make sure the password is strong. The password file is either encrypted or hashed to save into a hash table via a one-way function.
        - Even if the hacker manages to guess the password, while logging into a new device, he would require an OTP.

- Keyboard logging -
    - Threat -
        - The hacker can monitor the keyboard activity of the users without their knowledge to gain access to their passwords and sensitive information.
    - Measure -
        - The use of virtual keyboard is encouraged and the network firewall prevents hackers to gain access to devices (keyboards) within the network.

- Packet Sniffing -
    - Threat -
        - Across a network, the packets can be sniffed by a hacker using several tools. These packets might store sensitive information like credit card details.
    - Measure -
        - The IIIT firewall prevents packet sniffing by hackers and the packets are encrypted during transmission.

Question 3 :

Part a

- The **plain text** - Legislature shall make no law respecting an establishment of religion or prohibiting the free exercise thereof or abridging the freedom of speech or of the press or the right of the people peaceably to assemble and to petition the government for are dress of grievances game of thrones season eight spoilers jon snow and daenerys targaryen to kill each other

- The **methodology** is -
    - Monoalphabetic Caesar cipher by substitution has been used in this case.
    - Each letter is mapped to another unique letter by a shift of 7.
    - Thus, the key turns out to be "HIJKLMNOPQRSTUVWXYZABCDEFG"
    - To reverse the cipher text the key is found out by shifting the letters by 7 and then the key is mapped to the ciphertext to find the plain text.

- The **code** is submitted in file - Parta.java
    - Instructions to run : Give the cipher text as input in a single line and run the code.

- The **random added cipher text** -
    - nhtl vm aoyvulz zlhzvu lpnoa zwvpslyz qvu zuvd huk khlulyfz ahynhyflu av rpss lhjo vaoly
    - This can be converted to - game of thrones season eight spoilers jon snow and daenerys targaryen to kill each other
    - The **security policy violated** is **integrity**. This is because the data has been tampered by the TA and the original plain text is not available to the authorised users.

Part b

- The **plain text** - The Indian paradise flycatcher (Terpsiphone paradisi) is a medium-sized passerine bird native to Asia that is widely distributed. As the global population is considered stable, it has been listed as Least Concern on the IUCN Red List since 2004. It is native to the Indian subcontinent, Central Asia and Myanmar.

- The **code** is submitted in file - Partb.java
    - Instructions to run : Give the cipher text as input in a single line and run the code.

Question 4 :

Browsers like Google Chrome take in user information in the form of user-id and password and save all the information against the same login in the form of cookies etc. For example, if a user is logged in with an email address, and he uses youTube, github, Netflix etc, all the cookies related to these websites is saved as plugins to the same email address. So, when we log in to the same account from a different device, all the information gets imported automatically.
So, in case a hacker gets hold of a person's username and password, he can get access to all the data attached with the account.,

The information at risk is -

- The browsing history of an individual. The websites he visits regularly and his online activities.
- The cookies attached to the different websites are also saved.
- His saved passwords. These may include saved card details and username and passwords of various accounts. This is highly confidential information and leads to a severe breach of an individual's privacy.
- His bookmarks and the saved information about every website.
- In the case of Google, one account is used to link different platforms like Drive, Photos, Contacts etc. So, all this information saved in these platforms is at risk including a person's sensitive information, his pictures, projects etc.

This breach can lead to -

- Compromise of a user's personal information saved in Drive. This information can be misused against him. This can lead to phishing attacks too.
- The pictures, if leaked can be also be misused.
- Google also sells this data/ information to advertisers.
- This is a massive invasion of someone's privacy and can breaks all codes for security.

To solve this issue of invasion of privacy, the following steps can be taken -

- Passwords must be made strong so that they cannot easily be guessed by hackers.
- Two factor authentication must be introduced every time the user logs into a new device. The OTP must be sent to the phone number registered. This prevents hackers from logging in and stealing private sensitive information.
- Ask for a confirmation from the user whether they want their bookmarks, cookies and saved passwords to be imported when they log in from a new mac address device
- They should not sell a user's personal information to the advertisers and instead encrypt the information when a user uploads it so that even the google employees can't access the data.