Assignment 1

-Suraj Prathik Kumar (2016101)

Question 1:

1. Alice - **Very weak** as it has no numbers or special characters(the hacker can guess it through Brute force attack)

2. Qwerty1234 - **Weak** as it has no special characters and first 4-6 straight words of the keyboard(the hacker can guess it through Brute force attack)

3. Rat$you - **Neutral** as it has only 1 special character and a random string with capital

4. Elppa - **Very weak** as it has no it has no numbers or special characters.

5. Mumbai - **Very weak** as it has no it has no numbers or special characters(the hacker can guess it through Brute force attack)

6. Mfiical4W - **Strong** as it has a number in between and 2 capital letters but no special character.

7. Tif#hom&851@ - **Very Strong** as it has all:capital letter,special character and numbers.

8. #$\%@$^$^@$@# - **Neutral** as it has no letter and numbers.

9. ecila!0987 - **Strong** but it has no Capital letter.

10. 45649243 - **Very Weak** as it has no special character or letters.

Question 2:

All users of IIITD will be assigned a unique identity to gain secure access to College IT resources that they have been authorized to.

Physical Access -

- For access into college the user must show his identification card to the guard.The identification will be created at the time of joining.These cards will have an RFID chip which they can use to gain access into the labs and restricted areas if they have authority.
- For Visitors they won't be given any access to labs or restricted areas until they have permission by the authority.

Internet Resources -

- A registration number (8 digit) will be unique to all the users, which will be assigned to them at the time of their joining.

- All the users (**students, faculty, and employees**) will be given an email id which will have a registration number. This can be used to gain access to authorized IIIT portals and resources.
- The email id for users can be created with their firstname and last 4 digits of their registration number.
- If the email is logged in from any other device the user will get an email or message on the phone regarding the same.
- Initially they will be sent a mail on their personal IDs with their email IDs and a random-generated password which will be mandatory for them to change. When the users change the password, we can keep a track for strong password creation (minimum 7 letters, atleast a capital letter, not first name in password, a special character and a digit) .
- Password must not be saved as clear text by the IT authority.They should be hashed with a one-way function and saved in the database and at the time of authentication the user password should be hashed and matched with the hashed value from the database.
- For **Visitors** they have to personally go to the IT authority and get their email id verified. They can get access only for a specific time period.
- To connect into the IIITD network all the users need to get their devices mac address and phone numbers verified and registered. Users can access through their email id and a OTP which will be sent to their phone.Which they have to refresh everyday.
- Users will be held accountable for their logged in sessions.Hence they should maintain the confidentiality of their passwords and do not give id cards to other users. For compromise of anyone's passwords or loss of id cards they should immediately report to IT authority.
- All the users at the time of registration will be given certain privileges according to role (For eg, students won't be given access to admin data). For furthermore privileges, the user must request the IT desk for permission.
- The emails addresses will be dissolved when a member leaves college and re-invoked when they join back.

Threats

1. **Keyboard Logging or Sniffing** where the hacker can record the action of logging the keys struck on a keyboard and the person using the keyboard is unaware that their actions are being monitored.
2. **Password Cracking** where the hacker can perform Password Resetting, Dictionary Attack, Brute Force Attack.
3. **Taken to a fake website pretending to be genuine one**

Measures

1. For this even if the password is guessed by the hacker there is a 2 factor authentication where in the user has to add an OTP which he will receive on the phone so the hacker can't access it.
2. The Users have to follow these measures while creating a password : minimum 7 letters, atleast a capital letter, no first or last name in password, a special character and a digit. While creating Strength of the password should minimum be strong And in case of a breach in the password and the hacker logs in from any other device the user will get a message or a mail for the same.
3. CA certified websites will only be allowed to access in IIITD network.The network makes sure that you are not redirected to a fake one.

Question 3:

a) **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

Code:

```
import java.util.HashMap;
import java.util.Scanner;


public class Question3a
{
  public static void main(String args[])
  {
     String letter="ABCDEFGHIJKLMNOPQRSTUVWXYZ";
     int shift=7;

     HashMap<String, String> Hash = new HashMap<>();

     for(int i=0;i<letter.length();i++)
     {
        int ascii=letter.charAt(i) + shift;
        if(ascii>90)
           ascii=ascii-26;


        String key=String.valueOf((char)(ascii));
        Hash.put(key,String.valueOf(letter.charAt(i)));

     }

     Scanner sc=new Scanner(System.in);  // For input

     String crypt=sc.next();
     crypt+=sc.nextLine();

     String decrypt="";

     for(int j=0;j<crypt.length();j++)
     {
        char val=crypt.charAt(j);
        String temp=Hash.get(""+Character.toUpperCase(val));
        if(temp!=null)
        {
```

```
            if (Character.isLowerCase(val))
                decrypt += String.valueOf(temp).toLowerCase();

            else
                decrypt += String.valueOf(temp);
        }
        else
        {
            decrypt+=val;
        }

    }
    System.out.println(decrypt);
  }
}
```

How to run the code:

Input the cipher-text as the input for the java code and run it.

Methodology;

Monoalphabetic Caesar cipher is used where each letter is mapped with a unique letter with a shift. In this case the shift is of 7 and thereby the key generated is “HIJKLMNOPQRSTUVWXYZABCDEFG”. To reverse the cipher you need to find the shifting of letters and then find out the key and then use key mapping to cipher the plain text.

Randomly added cipher-text:

game of thrones season eight spoilers jon snow and daenerys targaryen to kill each other(nhtl vm aoyvulz zlhzvu lpnoa zwvpslyz qvu zuvd huk khlulyfz ahynhyflu av rpss lhjo vaoly)

Security policy is violated:

Integrity – Original data has been altered by the TA and it affects the receivers of ciphertext as the extra lines are added.

b) 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

Code:

```
import java.util.HashMap;
import java.util.Scanner;

public class Question3b
{
  public static void main(String args[])
  {
     String key="BIRDWATCHNGEFJKLMOPQSUVXYZ";
     String letter="ABCDEFGHIJKLMNOPQRSTUVWXYZ";

     HashMap<String, String> Hash = new HashMap<>();

     for(int i=0;i<letter.length();i++)
     {
        Hash.put(String.valueOf(key.charAt(i)),String.valueOf(letter.charAt(i)));
     }

     Scanner sc=new Scanner(System.in);

     String crypt=sc.next();
     crypt+=sc.nextLine();                  // For input

     String decrypt="";

     for(int j=0;j<crypt.length();j++)
     {

        char val=crypt.charAt(j);
        String temp=Hash.get(""+Character.toUpperCase(val));
        if(temp!=null)
        {
           if (Character.isLowerCase(val))
              decrypt += String.valueOf(temp).toLowerCase();

           else
              decrypt += String.valueOf(temp);
        }
        else
        {
           decrypt+=val;
        }

     }
     System.out.println(decrypt);
  }
}
```

Question 4:

Paytm is one of the apps which I use regularly for ordering food,canteen payments or any only payment. The initial phase of login and verifying of the app while creating an account is to add a phone number and enter an OTP.

- After that it saves a cookie and for subsequent logins, it doesn't even send an OTP on the phone most of the times.
- Most of the time there are issues with card details as it automatically saves the card details and by just one click money can be added to the device.
- Further there are no check so as to whom you are sending the money and if the number is incorrect it will directly send the money to that wrong number.
- If someone gets hold of the device and unlocks it the person can send the money from the devices paytm to his paytm. Further if the card details are added on UPI payment the user just have to press a click and add money to paytm wallet.

This causes a credit card fraud and leads to invasion of a person's private information.

To prevent these problems-

- The app should not add cookies for fast access and ask for OTP or may incorporate 2 factor authentication for login everytime.
- The app should never save the card details or should delete them when logged in from any other device or when logged out.
- The app should always have a password system while sending money when QRCode is not used and double check before sending. For large amounts, the app should send an OTP too.
- The app should also send an OTP when money is being transferred from the bank even in the case of UPI payments.