Name:- Tanmay Chauhan

Course:- BCA

Section:- C

Roll No:- 39

University Roll N:- 1121154

Subjects:- IT Security And Cyber Laws.

1. Find any 3 security aspects of the Google accounts.

Ans. Objective: A google account is the key to accessing all of google's products and services, may of which are free. Signing up for a google account is a quick process.

Activity

(A) Create a google Account to access to many google product.

step1: Go to the official site of google account for sign in.

step2: Click on create Account and create and your google account by filling necessary details.

Step 3:- Create password for your account.

Step 4:- Account Created Successfully.

My email id is tanmaychauhan@gmail.com.

(B) Change your google Account Password.

1. Open your google Account. You might need to sign in.
2. Under "security," select signing in to Google.
3. Choose password.
4. Enter your new password, then select change password.

(C) Check Google Privacy Policies.

You can take a privacy checkup and choose the setting that are right for you:-

1. Automatically delete Web and App Activity.
2. Automatically delete Location History.
3. Make a plan ~~for~~ for your account.
4. Review setting for face grouping.

5. Check third-party access.

6. Review your ad settings.

2. Write and 3 security aspects of the browsers.

Ans. (A) Safe Browsing:

Safe Browsing protects you and your devices from dangerous sits.

Step 1. open Google Chrome.

Step 2: Go to the setting.

Step 3: Now, click on show Advanced settings.

Step 4: Check "Protects you and your devices and from dangerous sites".

(B) Check information and page content to Google

Step 1: open Google chrome,

step 2: Go to the settings.

Step 3: Now, click on Show Advanced settings.

Step 4:- Go to content settings. Here you have many options like location, camera, microphone etc.

Step 5:- Now, you can on/off the access of these options.

(c) check and use of "Do Not Track" request with your brows traffic.

Step 1:- open Google chrome.

Step 2:- Go to the settings.

Step 3:- Now, click on show Advanced settings.

Step 4:- Now, you can on/off this service if you want.

4. Write a program to implement OTP (one time Password)

Ans.

```
import random
def generateOTP(length):
    str = "abcdefghijklmnopqrstuvwxyzABCD
    EFGHIJKLMNOPQRSTUVWXYZ0123456
    789";
    n = len(str);
```

```
OTP = " ";
for i in range ( 1, length + 1):
OTP += str [int ( random. random ( ) * 10) % n];
return (OTP);
if -- name -- == '-- main --';
length = 6;
print (" Your OTP is -", generateOTP (length));
```

5. Encryption and decryption using caeser cipher

Ans. Encryption :

```
def encrypt ( string, shift):
cipher = ''
for char in string :
if char == ' ';
cipher = cipher + char
elif char. isupper ( );
cipher = cipher + chr (( ord (char) + shift - 65) %
26 + 65)
```

```
    else:
        cipher = cipher + chr((ord(char) + shift - 97) % 26 + 97)
    return cipher

text = input("enter string:")
s = int(input("enter shift number:"))
print("original string:", text)
print("after encryption:", encrypt(text, s)).
```

Decryption

```
def decrypt(ciphertext, key):
    result = ''

for i in range(len(ciphertext)):
    char = ciphertext[i]

    if(char.isupper()):

    result += chr((ord(char) - key - 65) % 26 + 65)

    else
    result += chr(ord(char) - key - 97) % 26 + 97)
    return result
```

```
ciphertext = ''
key = 2
Print ("Text :" + ciphertext)
Print ("shift :" + str(key))
Print ("cipher :" + decrypt (ciphertext, key))
```

3. Encryption and decryption of the vigenere ciphere.

```
def generatkey ( string, key);
    key = list (key)
    if len (string) == len (key):
        return(key)
    else:
    for i in range (len (string) - len (key)):
        key. append (key [ i %. len (key)] )
    return ("". join (key))

def encryption (string, key):
    encypt_text = [ ]
    for i in range ( len ( string)):
```

```
    x = (ord(string[i]) + ord(key[i])) % 26
    x += ord('A')
    encrypt_text.append(chr(x))
    return("".join(encrypt_text))

def decryption(encrypt_text):
    orig_text = []
    for i in range(len(encrypt_text)):
        orig_text = []
        x = (ord(encrypt_text[i]) - ord(key[i]) + 26) % 26
        x += ord('A')
        orig_text.append(chr(x))
    return("".join(orig_text))

if __name__ == "__main__":
    string = input("Enter the message:")
    keyword = input("Enter the keyword:")
    key = generatekey(string, keyword)
```

```
encrypt_text = encryption(string, key)
print("Encrypted message:", encrypt_text)
print("Decrypted message:", decryption(encrypt_text
                                ,key)).
```