Shaniya Chauhan BCA-VI 'C' Univ-No => 1121176 PBC-601

Information security practical (lab) (MCQ)

1. PGP uses - (b) Assymetric key encryption with sender public key.

2. Keyloggers are a form of - (c) Spyware

3. A digital signature is (c) An authentication of an electronic record.

4. "NETIQUETTES" deals with (b) Cyber Security

5. Encryption can be done (b) Only on ASCII coded data

6. (c) All does not come under the copyright law infringement.

7. MD5 is a (a) hash value

8. In Affine cipher - (b) The identity of the character is changed while its position remains unchanged

9. The reason behind appending 'x' in Playfair cipher is - (b) To make even no. of letters.

10. Module m taken as 26 substitution cipher because of (a) Total length of word

Shaniya Chauhan BCA-VI 'C' 1121176 PBC-601

Info. Security (Lab.)

Q1 Step1 - Go to security checkup to get personalized security recommendations for your Google account, including:

⇒ Add or update account recovery options—
Your recovery phone number and email address are powerful security tools.

This contact info can be used to help:
- Block someone from using your account without your permission.
- Alert you if there's suspicious activity on your logged account.
- Recover your account if you've ever ~~locked~~ out

2-Step verification helps prevent a hacker from getting into your account, even if they steal your password. To avoid common phishing techniques associated with text message codes, choose a stronger second verification step.
- Security keys (Most secure), Google prompts.

Step2 - Update your software if your browser, operating system, or apps are out of date, the software might not be safe from hackers. Keep your software updated to the latest version to help protect your account.

=> Update to the latest version.
=> Update Android devices.
=> Update chrome books.

Step 3- Use unique strong password.

It's risky to use the same password on multiple sites. If your password for one site is hacked, it could be used to get into your accounts for multiple sites. Make sure to create a strong, unique password for each account.

Shaniya Chauhan BCA-VI 'C' 1121176 PBC-601

Info. Security (lab)

Q4

```
#include <stdio.h>
#include <ctype.h>
#include <string.h>
int main()
{
    char plaintext[100], otp[100];
    printf("Enter plain text\n");
    fflush(stdin);
    fgets(plaintext, sizeof(plaintext), stdin);
    printf("Enter otp text of length %d\n",
                strlen(plaintext));
    fflush(stdin);
    fgets(otp, sizeof(otp), stdin);
    for(int i=0; i<strlen(plaintext); i++)
    {
        if(isupper(plaintext[i]))
        {
            otp[i]= toupper(otp[i]);
if(plaintext[i]+(otp[i]-'A')>'Z') {plaintext[i]=
    plaintext[i]+(otp[i]-'A')-26;}
if(plaintext[i]+(otp[i]-'A')<='Z')
    {
        plaintext[i] = plaintext[i]+otp[i]-'A';
    }
}
```

```
else if (islower (plaintext[i]))
{
    otp[i] = tolower(otp[i]);
if (plaintext[i] + (otp[i]-'a' > 'z')
{
    plaintext[i] + (otp[i]-'a') - 26;
}
if (plaintext[i]+otp[i]-'a') <= 'z')
{
    plaintext[i] = plaintext[i]+(otp[i]-'a');
}
}
else { plaintext[i] = plaintext[i]; }
}
printf ("Cipher text \t %s \n",
                plaintext);

return 0;
}
```

Shariya Chauhan BCA-VI 'C' 112176 PBC-601

Infor. Security (lab)

Q5

```
#include<stdio.h>
#include<string.h>
int main()
{
    char message="Attack from North", ch, message;
    int i, key;
    printf("Enter key:");
    scanf("%d", &key);
    for(i=0; message[i]!='\0'; i++)
    {
        ch = message[i];
        if(ch>='a' && ch<='z')
        {
            ch = ch+key;
            if(ch>'z')
            {
                ch = ch-'z'+'a'-1;
            }
            message[i] = ch;
        }
        else if(ch>='A' && ch<='Z')
        {
            ch = ch+key;
            if(ch>'Z')
            {
                ch = ch-'Z'+'A'-1;
            }
            message[i] = ch;
        }
    }
```

```
printf("Encrypted message is %s\n", message);
for(i=0; message[i] != '\0'; i++)
    {
      ch = message[i];
    if (ch >='a' && ch <='z')
     {
        ch= ch- key;
      if (ch<'a')
       {
         ch = ch+'z'-'a'+1;
       }
       messaged[i]= ch;
     }
   else if (ch >='A' && ch <='Z')
    {
        ch= ch-key;
      if (ch <'A')
       {
         ch= ch+'z'-'A'+1;
       }
      messaged[i]=ch;
    }
printf("Decrypted message is %s", messaged);
      return 0;
    }
```