NAME- AYUSH KUMAR COURSE- B.SC(IT) SEM-VI
Roll NO- 1022730(20) SUBJECT- INFORMATION SECURITY
& CYBER LAWS

Q1

(i) CROSS. SITE SCRIPTING (XSS)

Cross site scripting targets an application. users by injecting code usually a client-side Script such as JavaScript. into a web applications output. The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the attacker. XSS allow attackers to execute scripts in the victim browser which can hijack user sessions.

(ii) SQL INJECTION

sql injection is a type of web application. security vulnerability in which an attacker attempts to use application code to access

Kumar

or corrupt database content. If successful this allows the attacker to create, read, update, alter, or delete data stored in the back-end database.

(iii) BROKEN AUTHENTICATION & SESSION MANAGEMENT

Broken authentication & session management. emcopass several security issues, all of them having to do with maintaing the idenkify of a user. credentials and session identifiers are not protected an attacker can higack them.

(iv) CROSS-SITE REQUEST FORGERY (CSRF)

CRSF is a malicious ~~tteek~~ attack where a user is tricked into performing an action he or she didn't intend to do. A third-party website will send a request to a web application that a user is already authenticated against

NAME- AYUSH KUMAR. Roll No- 1022730(20).

COURSE- B.Sc (IT)

Q2

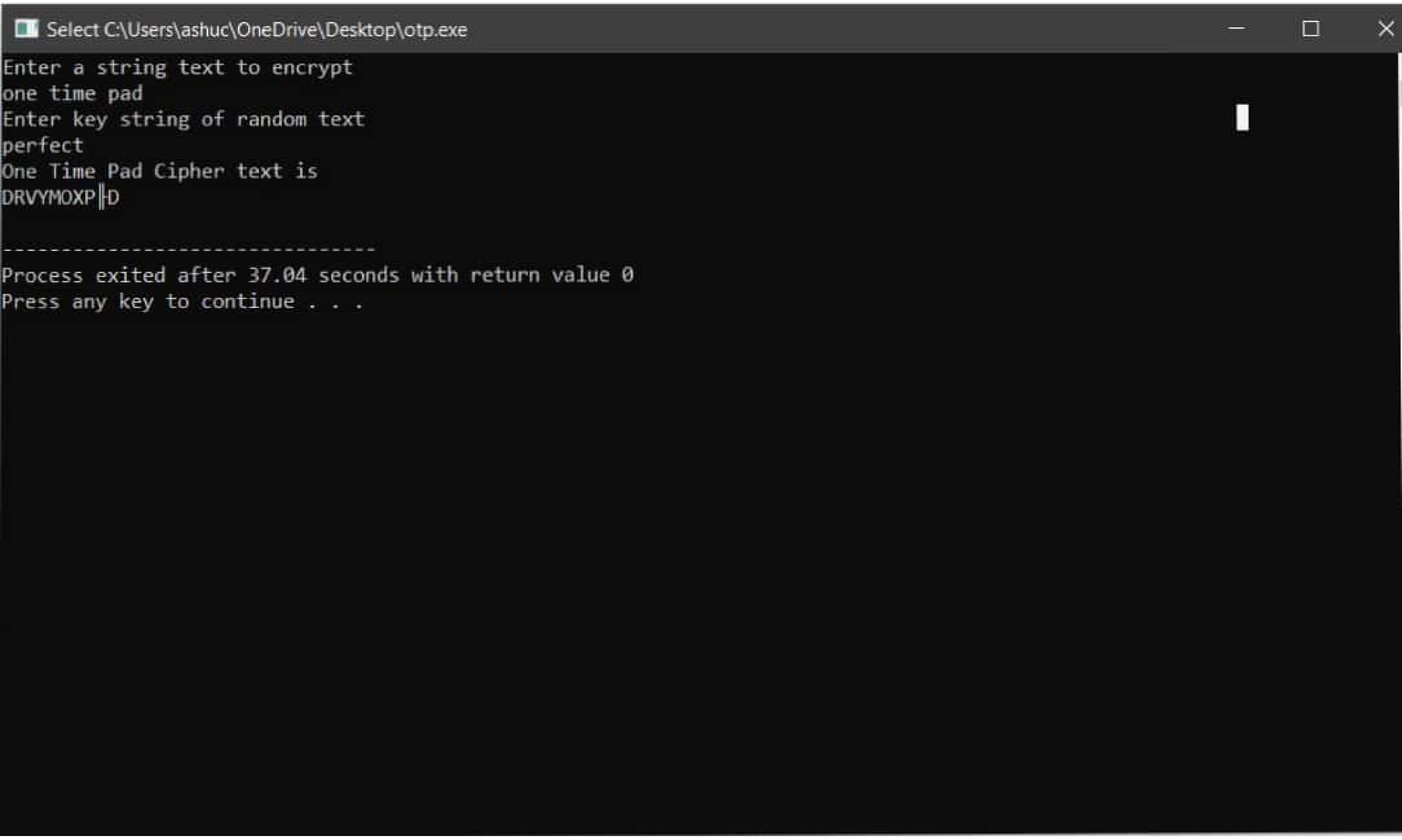
```
#include<stdio.h>
#include< string.h>
#include <ctype.h>

main()
{
 int i,j, len2,numstr[100] ,numkey[100],
numcipher[100];
char str[100], key[100] ,cipher[100];
printf("Enter a string text to encrypt \n");
get (str);
for (i=0,j=0; i<strlen (str) ;i++)
{
 if (str[i]!=' ')
 {
   str[j]= toupper (str[i]);
   j++;
  }
 }
str[j]='\0';
for (i=0 ; i<strlen(str);i++)
{  numstr [i]= str [i]-'A';
 }
```

```
printf(("Enter key string of random text \n");
gets(key);
for(i=0,j=0;i<strlen(key);i++)
{
  if(key[i]!=' ')
   {
     key[j]=toupper(key[i]);
     j++;
    }
  }
 key[j]='\0';
 for(i=0;i<strlen(key);i++)
   {
     numkey[i]=key[i]-'A';
    }
  for(i=0;i<strlen(str);i++)
   { numcipher[i]=numstr[i]+numkey[i];
   }
  for(i=0;i<strlen(str);i++)
   { if(numcipher[i]>25)
     { numcipher[i]=numcipher[i]-26;
      }
     }
  printf("one time pad cipher text is \n");
```

AKumar

```
for(i=0;i<strlen(str);i++)
{
   printf("%c",(numcipher[i]+'A'));
 }
   printf("\n");
}
```



```
Enter a string text to encrypt
one time pad
Enter key string of random text
perfect
One Time Pad Cipher text is
DRVYMOXP D

--------------------------------
Process exited after 37.04 seconds with return value 0
Press any key to continue . . .
```

NAME- AYUSH KUMAR RollNo-1022730

Q4

PASSWORD MANAGEMENT- Password are a set of strings provided by users at the authentication prompts of web accounts. Although password still remain as one of the most secure methods of authentication available to date. The role of password management comes in handy there. password management is a set of principles and best practices to be followed by users while storing and managing passwords in an efficient manner to secure passwords as they prevent unauthorized access.

PASSWORD MANAGEMENT USING FREE ONLINE TOOLS

1. LastPass - This is free password manager. It offers unlimited storage on multiple devices It offers password auditing. 2FA compatibility password sharing and buit-in authenticator

NAME- AYUSH KUMAR Roll No- 1022730(20)

Q4

2. Roboform - It is user-friendly with an excellent form filler and unlimited password ~~Sto~~ storage one one device. check the vault for weak passwords, receive emergency access, organise bookmark, and send login to other users.

3. Bitwarden - Bitwarden uses AES-256 encryption to protect the data stored in your password vault. Your information is only unencrypted, and only locally on your device, once you've logged into your vault with master key.

4. sticky password - It provides USB portability and biometric login, but we have to upgrade for multi-device sync.

5. Avira Password Manager - It includes biometric logins, a buit-in 2FA authenticator, and a well-functioning auto-saving and auto-filling capability.