



# Graphic Era

HILL UNIVERSITY

Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)  
University under section 2(f) of UGC Act, 1956

**LAB MANUAL**  
**Information Security**  
**TBI 601**  
**SCHOOL OF COMPUTING**



**GRAPHIC ERA HILL UNIVERSITY**

**Prepared By**

Tanishq Singh

BSc (it)

61 (1022771)

**Submitted to**

Ms. Nidhi Joshi



# Graphic Era

HILL UNIVERSITY

Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)  
University under section 2(f) of UGC Act, 1956

## ACKNOWLEDGEMENT

I would like to convey my gratitude to Ms. Nidi Joshi Ma'am, my teacher , for her immense help and guidance in the completion of my term work . It is only due to her efforts that my term work could be completed successfully . She gladly accepted all the pain in going through ,and participated in enlightening and motivating discussions , which were extremely fruitful.



# Graphic Era

HILL UNIVERSITY

Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)  
University under section 2(f) of UGC Act, 1956

## CERTIFICATE

This is to certify that the Term work of Information Security and Cyber Laws has satisfactory completed by TANISHQ SINGH in 6<sup>th</sup> semester prescribed by GRAPHIC ERA HILL UNIVERSITY ,DEHRADUN during the year 2020-21.

**SCHOOL OF COMPUTING**  
**STUDENT LAB REPORT SHEET**

Information Security and Cyber Laws

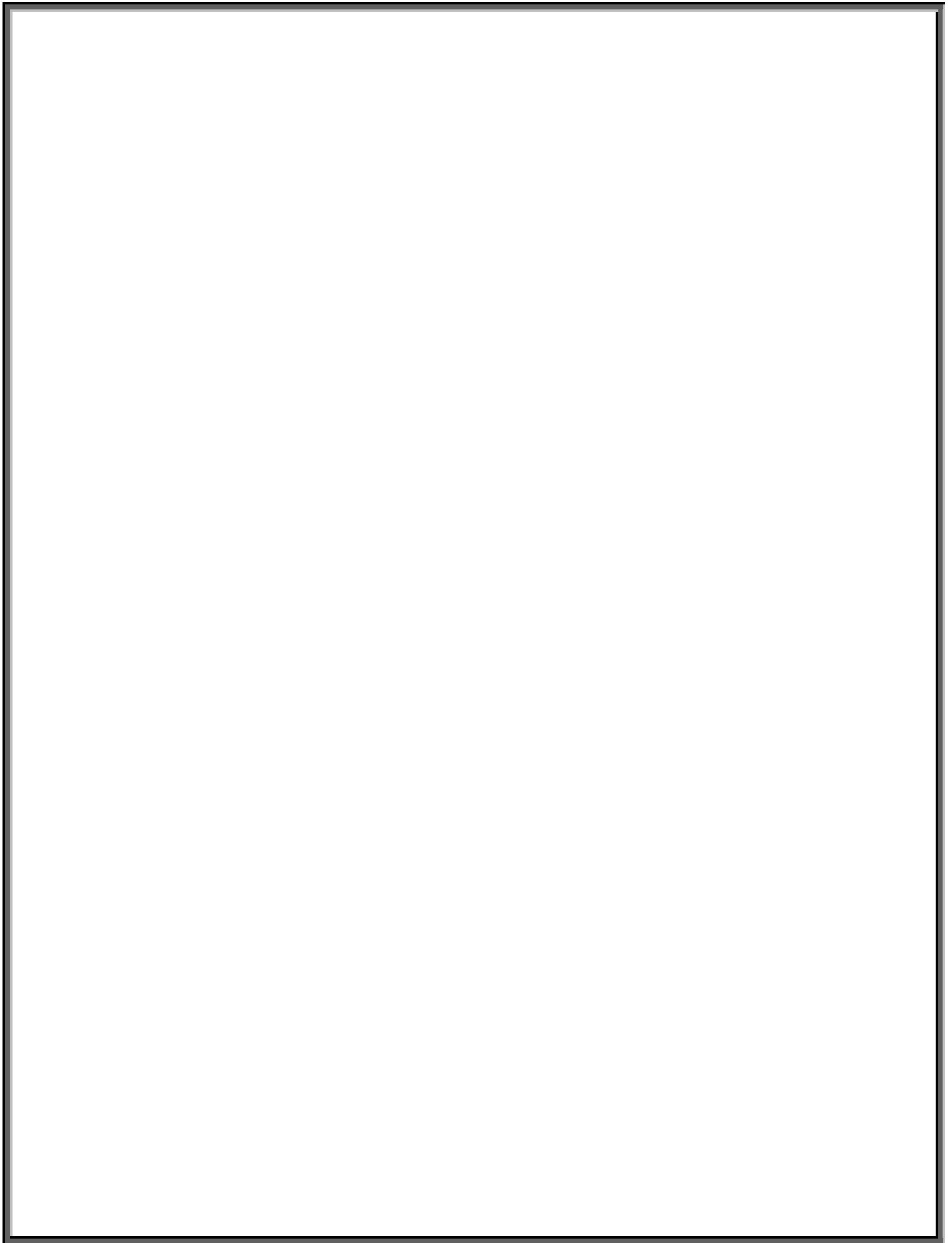
Name of Student:- TANISHQ SINGH

Course :- BSc IT 6<sup>th</sup> sem

Roll no :- 61 (1022771)

<u>List of Programs</u>								
S N	Description	Date of program	Date of submis sion	Grade viva	Grade file	Total mark s	Studen t's Sign	'Teac her's Sign
1	Analyze the security aspect of your Google account						Tanish q	
2	Analyze the security aspect of any two browser						Tanish q	
3	Write a program to implement Ceaser Cipher (encryption and decryption)						Tanish q	
4	Write a c program for encryption and decryption using playfair cipher.						Tanish q	
5	Write a c program to implement encryption and decryption using affine cipher.						Tanish q	
6	Write a c program to implement encryption and decryption using vigenere cipher.						Tanish q	
7	Critical Evaluation of 'Gleevec' drug case in India						Tanish q	
8	Write a c program to implement vernam cipher(OTP) for encryption and decryption.						Tanish q	
9	Write a c program to implement Route cipher for encryption and decryption.						Tanish q	
10	Case study						Tanish q	

11	Write a c program to implement Hill cipher for encryption and decryption.						Tanish q	
12	Write a c program to implement des cipher for encryption and decryption.						Tanish q	



## PRACTICAL -1

### PROBLEM STATEMENT

Analyze the security aspects of your Google account.

### OBJECTIVE

A Google account is the key to accessing all of Google's products and services, many of which are free. Signing up for a Google account is a quick process, but need to give out some personal information. So the main objective is to control the information for Google account holder.

### ACTIVITY

#### (A) Create a Google Account to access to many Google products.

STEP1: Go to the official site of Google account for sign in.

STEP 2: Click on Create Account and create your google account by filling necessary details.

STEP 3: Create Password for your account.

STEP 4: Account Created Successfully.

My email id is tansh7n7@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. You might need to sign in again.
4. Enter your new password, then select Change Password.

Few things to remember before changing the current password:

Password should be unique.

Password should have special characters.

### **(C) Control what others see about you across Google services.**

1. Go to your Google Account.
2. On the left, click Personal info.
3. Under “Choose what others see,” click Go to About me.
4. Change your info:

->Add: For each category you want to add info to, click Add.

->Edit: Click the info you’d like to change and then click Edit.

\*Tip: If you've changed your name recently, you might need to wait before you can change it again.

->Remove: Click the info you’d like to remove and then click Remove.

5. Follow the on-screen steps.

#### Choose what info to show

Your name and profile picture can be viewed by other people who use Google services, including when you communicate or share content.

Tip: For other info that you add, you can choose if it's private or visible to anyone.

1. Go to your Google Account.
2. On the left, click Personal info.

3. Under “Choose what others see”, click Go to About me.
4. Below a type of info, you can choose who currently sees your info.
5. Choose one of the following:
  - \*To make the info private, click Only you .
  - \*To make the info visible to anyone, click Anyone .

#### **(D)See control and delete the info in your Google Account.**

Use Activity Control to choose what kinds of activity get saved in your account.  
Examples of activity include:-

- Searches you do
- Websites you visit
- Videos you watch
- Places you go

Activity data helps bring you a better experience through quicker search and a more customized experience on Google products.

#### **Track & delete your info:-**

These resources helps you review and control the activity saved in your Google Account.

- Delete history and cookies from chrome
- See other Google activity
- Delete a product from your account
- See and delete places you've been
- See and delete your activity and files
- See an Overview of your data

### **(E) Check Google Privacy Policies.**

You can take a Privacy Checkup and choose the setting that are right for you:-

- Automatically delete Web and App Activity
- Automatically delete Location History
- Automatically delete YouTube History
- Make a plan for your account
- Review setting for face grouping
- Check third-party access
- Review your ad settings

### **(F) Check for Account Recovery.**

If you forgot your password or username, or you can't get verification codes, follow these steps to recover your Google Account. That way, you can use services like Gmail, Photos, and Google Play.

Tip: If you use an account through your work, school, or other group, these steps might not work. Check with your administrator for help.

Forgot your password

1. Follow the steps to recover your Google Account or Gmail.
  - You'll be asked some questions to confirm it's your account. Answer as best you can.
  - If you have trouble, try the tips to complete account recovery steps.
2. Reset your password when prompted. Choose a strong password that you haven't already used with this account. Learn how to create a strong password.

Forgot the email address you use to sign in

1. Follow the steps to find your username. You'll need to know:
  - A phone number or the recovery email address for the account
  - The full name on your account
2. Follow the instructions to confirm it's your account.
3. You'll see a list of usernames that match your account.

Someone else is using your account

If you think someone is using your Google Account without your permission, follow the steps to recover a hacked or hijacked Google Account or Gmail.

Can't sign in for another reason

If you have another problem, get help signing in.

Recover a deleted Google Account

If you recently deleted your Google Account, you can follow the steps to recover your account.

Still can't sign in

Create a new account

If you can't sign in, try these tips for account recovery.

If you still can't recover your account, you can create a new Google Account.

Avoid account & password recovery services

For your security, you can't call Google for help to sign into your account. We don't work with any service that claims to provide account or password support. Do not give out your passwords or verification codes.

## (G) Check for Account Security

## Make your account more secure

At Google, we take online security seriously. To protect your Google Account, we strongly recommend following the steps below regularly.

Note: If you're a journalist, activist, or someone else at risk of targeted online attacks, learn about the Advanced Protection Program.

### Step 1: Do a Security Checkup

Go to [Security Checkup](#) to get personalized security recommendations for your Google Account, including:

*Add or update account recovery options*

Turn on 2-Step Verification

*Remove risky access to your data*

*Turn on screen locks*

### Step 2: 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 help protect your account.

*Update your browser*

*Update your operating system*

*Update your apps*

### Step 3: Use unique, strong passwords

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.

*Manage your passwords*

*Help protect your password from hackers*

Step 4: Remove apps & browser extensions you don't need

As more apps are installed on a device, it can become more vulnerable. Install only essential apps and browser extensions on devices that have access to sensitive information. Avoid installing unknown apps or apps from unknown sources to protect your device and personal info.

Learn how to:

- Delete or disable apps on Android devices
- Uninstall extensions on Chrome
- Uninstall apps or extensions on Chromebooks

Note: For info on removing apps and extensions from other devices and browsers, visit the applicable support site.

Step 5: Protect against suspicious messages & content

Hackers can use emails, text messages, phone calls, and web pages to pretend to be institutions, family members, or colleagues.

*Avoid suspicious requests*

*Avoid suspicious emails*

*Avoid suspicious web pages*

## **(H) Check out for google safety tips.**

Strengthen your account safety/security:-

- Taking the security Checkup

- Creating strong password
- Using unique passwords for every account
- Keep track of multiple passwords
- Defend against hackers with 2-Step Verification
- Log to your Google Account.
- Go to Help Option where you find tips related to your google account.
- Following are the options comes under in help:
  1. Help with common issues like control and recover of data.
  2. Guiding steps for adding privacy, account protection and finding your device.
  3. Discuss your problems related to your google account with other peoples who use the same service as you.
  4. You can report your issues and get solution for that.
  5. You can also give feedback to your google services.

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

## PRACTICAL-2

### PROBLEM STATEMENT

Analyse the security aspects of any two browsers.

### OBJECTIVE

To understand the security aspects of web browsers.

### ACTIVITY

#### **Why secure your web browsers?**

Web browsers are used so frequently, it is vital to configure them securely. Often, the web browser that comes with an operating system is not set up in a secure default configuration. Not securing your web browser can lead quickly to a variety of computer problems caused by anything from spyware being installed without your knowledge to intruders taking control of your computer.

#### **1. Google Chrome:**

##### **(a) Web Browsers Features and Risks.**

###### **Features:**

## **1. Task manager**

Chrome has its own Task Manager that shows you how much memory and CPU usage each tab and plug-in is using. You can open it by clicking Shift-Esc from within Chrome. You can get more details by clicking the "Stats for nerds" link on the Task Manager and it will open a page with a full breakdown of memory and CPU usage for each process within the browser.

## **2. One box for search, address, and history**

Instead of having separate input boxes for the search bar and the address bar, Google has united the two in Chrome. Google also added history to the equation. So you can type something like "techrepublic" in the box and it will suggest the [techrepublic.co](http://techrepublic.co) home page as well as other recently visited TechRepublic pag

## **3. Upgraded tabs**

In Chrome you can drag a tab into its own window, and drag it back to the main window. This is called "Dynamic Tabs." Also, by default, the "New Tab" page in Chrome features a page that shows thumbnails of your most visited Web sites, a list of your recent bookmarks, and a search box that allows you to search your histor

### **Risks:**

- Google gets access not just to your search history, but also your browser history
- They could serve annoying ads via Chrome
- The could use Chrome to spy on computer usage habits

- Google could choose to sell the data they collect instead of protecting it and sometimes using it for useful things
- They could use your webcam/microphone to spy on you, or collect more data
- They could parse the web pages you visit and get a sense of **exactly** what you do on the internet (e.g. “bought a ninja sword” vs. “browsed amazon”).

#### **(b)Need of Chrome sign-in.**

By signing through google account in Chrome you can easily access all the facilities provided by Chrome like Net Banking.

#### **(c)Use a web services to help resolve navigation errors.**

If a connection to a website cannot be made for whatever reason, Chrome may retrieve alternative web pages similar to the one you are trying to reach. To achieve that goal, the website you are trying to open is submitted to Google.

STEP 1: Open Google Chrome.

STEP 2: Go to the Settings.

STEP 3: Now, Click on Show Advanced Settings.

STEP 4: Now, check "Use a web service to help resolve navigational errors".

#### **(d)Safe Browsing**

Safe Browsing protects you and your devices from dangerous sites.

STEP 1: Open Google Chrome.

STEP 2: Go to the Settings.

STEP 3: Now, Click on Show Advanced Settings.

STEP 4: Check “Protects you and your devices from dangerous sites.”

**(e)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.

**(f)Use a web service to help resolve spelling errors.**

STEP 1: Open Google Chrome.

STEP 2: Goto the Settings.

STEP 3: Now, Click on Show Advanced Settings.

STEP 4: Now, On/off the spelling check option to resolve spelling errors.

**(g) Check and use of “Do Not Track” request with your browsing traffic.**

“Do Not Track” is a service provided by chrome which included with your browsing traffic. Any effect depends on whether a website responds to the request and how the request is interpreted.

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.

#### **(h)Check your payment methods saved in browsers.**

In this option you can allow the sites to check if you have payments method saved.

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.

#### **(i)Manage Certificates**

In this option you check the certificates issued by the sites whenever you access those sites.

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.

**(j) Manage HTTPS/SSL certificates and settings and explain few of the certificates.**

STEP 1: Open Google Chrome.

STEP 2: Go to the Settings.

STEP 3: Now, Click on Show Advanced Settings.

STEP 4: Now, Click on Manage Certificates where you see many different certificates which is issued by the different sites and organisation.

Few of certificates are:

1-Global Certificate:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time
- Allows data on disk to be encrypted
- Allows secure communication on the Internet
- All issuance policies

2- Oracle Certification

- Ensures software came from software publisher
- Protects software from alteration after publication

3- Certum CA

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data to be signed with the current time

- All issuance policies
- OCSP Signing

### **(k)Clear browsing data**

STEP 1: Open Google Chrome.

STEP 2: Go to the Settings.

STEP 3: Now, Click on Show Advanced Settings.

STEP 4: Now, Click on the Clear browsing data option.

STEP 5: In this option you find two types of data clearing option i.e, Basic and Advanced.

STEP 6: Now, You can clear the browse data also you can delete cached image files and files for free up the memory space for better performance.

### **(l)Block pop-ups and script**

STEP 1: Open Google Chrome.

STEP 2: Go to the Settings.

STEP 3: Now, Click on Show Advanced Settings.

STEP 4: Now, Click on the content settings option, under this option you find the option of pop-ups and script.

STEP 5: Now, You can block and allow the sites for both options.

### **(m)How to use VPN or Proxy Server**

STEP 1: Open Google Chrome.

STEP 2: Go to the Settings.

STEP 3: Now, Click on Show Advanced Settings.

STEP 4: Now, Click on the system option, under this option you find proxy setting option where you can add proxy server for your VPN easily.

## **Mozilla Firefox:**

### **(a) Web Browsers Features and Risks.**

#### **Features**

##### **Web Technologies Support**

Firefox supports most basic Web standards including HTML, LXML, XHTML, CSS, JavaScript, DOM and etc.

Cross Platform Services

Firefox is open source and Mozilla actively develops a platform independent abstraction for its graphical front end, it can also be compiled and run on a variety of other architectures and operating systems. Thus, Firefox is also available for many other systems.

##### **Private Browsing**

Private browsing was introduced in Firefox 3.5, which released on June 30, 2009. This feature lets users browse the Internet without leaving any traces in the browsing history.

### **(b) Need of Chrome sign-in.**

By sign in with Firefox account you can access Mozilla services easily.

### **(c) Use a web services to help resolve navigation errors.**

STEP 1: Open Mozilla Firefox.

STEP 2: Go to the Settings.

STEP 3: Uncheck "Use a prediction service to help complete searches and URL's typed in the address bar.

#### **(d)Safe Browsing**

STEP 1: Open Mozilla Firefox.

STEP 2: Go to the Tools Menu, here you find the option of Safe Browsing.

STEP 3: Enable Safe Browsing by clicking on it.

#### **(e) Information and page content to Google**

STEP 1: Open Mozilla Firefox.

STEP 2: Go to the Privacy and Security option.

STEP 3: Here you find the option named as Content Blocking.

STEP 4: Now, you select one of the option from three options named as standard, strict, custom.

#### **(f)Use a web service to help resolve spelling errors.**

STEP 1: Open Mozilla Firefox.

STEP 2: Go to the Options.

STEP 3: Here you find the option named as Language.

STEP 4: Now, Check the option "**Check your spelling as you type**" to resolve spelling errors.

#### **(g)Check and use of “Do Not Track” request with your browsing traffic.**

STEP 1: Open Mozilla Firefox.

STEP 2: Go to the Options.

STEP 3: Here you have choice for use the “Do Not Track” option (i.e always and only when Firefox is set to block known trackers).

STEP 4: You can choose only one option among them at a time.

#### **(h)Check your payment methods saved in browsers.**

STEP 1: Open Mozilla Firefox.

STEP 2: Click the menu button and choose Preferences.

STEP 3: Click the Privacy & Security panel.

STEP 4: Click **Saved Logins...** under Forms & Passwords. The Password Manager will open.

#### **(i)Manage Certificates**

STEP 1: Open Mozilla Firefox.

STEP 2: Now click on Privacy and Security option.

STEP 3: Under this you find the Certificates option. With this option you can see the issued certificates by different sites to the browser.

#### **(j)Clear browsing data**

STEP 1: Open Mozilla Firefox.

STEP 2: Now click on Privacy and Security option.

STEP 3: Under this you find the History option. With this option you can clear the browsing history and also set the time range for clearing the browsing history.

#### **(k)Block pop-ups and script**

STEP 1: Open Google Chrome.

STEP 2: Now click on Privacy and Security option.

STEP 3: Under this you find the Permissions option.

STEP 4: With this option you find the option of pop-ups and script.

STEP 5: Now, You can block and allow the sites for both options.

### **(I)How to use VPN or Proxy Server**

STEP 1: Open Google Chrome.

STEP 2: Now click on Privacy and Security option.

STEP 3: Under this you find the Network Settings option this option

STEP 4: Under you can add VPN or Proxy Server to the network.

## Assignment 3

Wacp to implement ceaser cipher

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

int main(){
    int key=3,ch=0;
    start:
    printf("enter choise
\n1:ENCRYPTIONe\n2:DECRYPTION\n3:EXIT\n");
    scanf("%d",&ch);
    int VAR ,var;
    if(ch==1){key=key; var='a'; VAR='A'; printf(" enter plan txt
\n"); }
```

```
else if(ch==2){key=-key; var='a'+26-1; VAR='A'+26-1;
printf(" enter cypher txt \n");}

else if(ch==3) return 0;

else goto start;

fflush(stdin);

char plantxt[100];
fgets(plantxt,sizeof(plantxt),stdin);

for(int i = 0 ;i<strlen(plantxt) ;i++ )

{
    if(isupper(plantxt[i]))
        {plantxt[i]=(plantxt[i] -VAR+key)%26 +VAR;  }
    //{plantxt[i]=((plantxt[i] -'A' +key) %26) +'A'; //FOR
ENCRYPTION

    //{plantxt[i]=((plantxt[i] -'A'+26-1' +(-key))%26) +'A'; //
FOR DECRYPTION
```

```
else
    if(islower(plantxt[i]))
        {plantxt[i]=(plantxt[i] -var +key)%26 +var;  }
        //{plantxt[i]=((plantxt[i] -'a' +key) %26) +'a'; //FOR
ENCRYPTION
        //{plantxt[i]=((plantxt[i] -'a'+26-1' +(-key))%26) +'A'; //
FOR DECRIPITION
}
printf("result text is %s\n",plantxt);
goto start;
return 0;
}
```

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

/\*OUTPUT

enter choise

1:ENCRYPTIONe

2:DESCRIPTION

3:EXIT

1

enter plan txt

helloabzx

result text is khoordecA

enter choise

1:ENCRYPTIONe

2:DESCRIPTION

3:EXIT

2

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

enter cypher txt

khoordeca

result text is helloabzx

enter choise

1:ENCRYPTIONe

2:DECRYPTION

3:EXIT

\*/

## Lab Assignment 4

Write a c program for encryption using playfair cipher.

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

int removerepeated(int size,int a[]);
int insertelementat(int position,int a[],int size);

main()
{
    int
    i,j,k,numstr[100],numcipher[100],numkey[100],lenkey,templen,tempkey[100],flag
    =-1,size,cipherkey[5][5],lennumstr,row1,row2,col1,col2;

    char str[100],key[100];

    printf("Enter a string\n");
    gets(str);

    for(i=0,j=0;i<strlen(str);i++)
    {
        if(str[i]!=' ')
        {
            str[j]=toupper(str[i]);
            j++;
        }
    }
}
```

```
 }

}

str[j]='\0';

printf("Entered String is %s\n",str);

size=strlen(str);

for(i=0;i<size;i++)

{

if(str[i]!=' ')

numstr[i]=str[i]-'A';

}

lenumstr=i;

printf("Enter the key (Non repeated elements if possible)\n");

gets(key);

for(i=0,j=0;i<strlen(key);i++)

{

if(key[i]!=' ')

key[j]=toupper(key[i]);

j++;

}
```

}

key[j]='\0';

printf("%s\n",key);

k=0;

for(i=0;i<strlen(key)+26;i++)

{

if(i<strlen(key))

{

if(key[i]=='J')

{

flag=8;

printf("%d",flag);

}

numkey[i]=key[i]-'A';

}

else

{

if(k!=9 && k!=flag)

{

numkey[i]=k;

}

k++;

```
 }

}

templen=i;

lenkey=removerepeated(templen,numkey);

printf("Entered key converted according to Play Fair Cipher rule\n");

for(i=0;i<lenkey;i++)

{

    printf("%c",numkey[i] +'A');

}

printf("\n");

k=0;

for(i=0;i<5;i++)

{

    for(j=0;j<5;j++)

    {

        cipherkey[i][j]=numkey[k];

        k++;

    }

}

printf("Arranged key\n");

for(i=0;i<5;i++)

{
```

```
for(j=0;j<5;j++)  
{  
printf("%c ",cipherkey[i][j] +'A');  
}  
printf("\n");  
}  
  
for(i=0;i<lennumstr;i+=2)  
{  
if(numstr[i]==numstr[i+1])  
{  
insertelementat(i+1,numstr,lennumstr);  
lennumstr++;  
}  
}  
if(lennumstr%2!=0)  
{  
insertelementat(lennumstr,numstr,lennumstr);  
lennumstr++;  
}  
printf("Entered String/Message After Processing according to Play fair cipher  
rule\n");  
for(i=0;i<lennumstr;i++)
```

```
{  
printf("%c",numstr[i] +'A');  
}  
for(k=0;k<lennumstr;k+=2)  
{  
for(i=0;i<5;i++)  
{  
for(j=0;j<5;j++)  
{  
if(numstr[k]==cipherkey[i][j])  
{  
row1=i;  
col1=j;  
}  
if(numstr[k+1]==cipherkey[i][j])  
{  
row2=i;  
col2=j;  
}  
}  
}  
}  
if(row1==row2)
```

```
{  
    col1=(col1+1)%5;  
    col2=(col2+1)%5;  
    if(col1<0)  
    {  
        col1=5+col1;  
    }  
    if(col2<0)  
    {  
        col2=5+col2;  
    }  
    numcipher[k]=cipherkey[row1][col1];  
    numcipher[k+1]=cipherkey[row2][col2];  
}  
if(col1==col2)  
{  
    row1=(row1+1)%5;  
    row2=(row2+1)%5;  
    if(row1<0)  
    {  
        row1=5+row1;  
    }
```

```
if(row2<0)

{
    row2=5+row2;

}

numcipher[k]=cipherkey[row1][col1];

numcipher[k+1]=cipherkey[row2][col2];

}

if(row1!=row2&&col1!=col2)

{
    numcipher[k]=cipherkey[row1][col2];

    numcipher[k+1]=cipherkey[row2][col1];

}

printf("\nCipher Text is\n");

for(i=0;i<lenumstr;i++)

{
    if((numcipher[i]+'&')!='X')

        printf("%c",numcipher[i]+'&');

}

printf("\n");

}

int removerepeated(int size,int a[])
{
```

{

int i,j,k;

for(i=0;i<size;i++)

{

for(j=i+1;j<size;)

{

if(a[i]==a[j])

{

for(k=j;k<size;k++)

{

a[k]=a[k+1];

}

size--;

}

else

{

j++;

}

}

}

return(size);

}

```
int insertelementat(int position,int a[],int size)
```

```
{
```

```
    int i,insitem=23,temp[size+1];
```

```
    for(i=0;i<=size;i++)
```

```
    {
```

```
        if(i<position)
```

```
        {
```

```
            temp[i]=a[i];
```

```
        }
```

```
        if(i>position)
```

```
        {
```

```
            temp[i]=a[i-1];
```

```
        }
```

```
        if(i==position)
```

```
        {
```

```
            temp[i]=insitem;
```

```
        }
```

```
    }
```

```
    for(i=0;i<=size;i++)
```

```
    {
```

```
        a[i]=temp[i];
```

```
    }
```

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

```
C:\Users\tansh\Desktop\New folder (4)\playfai.exe
Enter a string
SINGH
Entered String is SINGH
Enter the key (Non repeated elements if possible)
TANISHQ
TANISHQ
Entered key converted according to Play Fair Cipher rule
TANISHQBCDEFGKLMOPRUVWXYZ
Arranged key
T A N I S
H Q B C D
E F G K L
M O P R U
V W X Y Z
Entered String/Message After Processing according to Play fair cipher rule
SINGHX
Cipher Text is
TSBPBV

-----
Process exited after 10.31 seconds with return value 0
Press any key to continue . . .
```

Write a c program for decryption using playfair cipher.

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

int removerepeated(int size,int a[]);
int insertelementat(int position,int a[],int size);

main()
{
    int
    i,j,k,numstr[100],numcipher[100],numkey[100],lenkey,tempkey[100],flag
    =-1,size,cipherkey[5][5],lenumstr,row1,row2,col1,col2;

    char str[100],key[100];
    printf("Enter a string\n");
    gets(str);
    for(i=0,j=0;i<strlen(str);i++)
    {
        if(str[i]!=' ')
        {
            str[j]=toupper(str[i]);
            j++;
        }
    }
}
```

}

str[j]='\0';

printf("Entered String is %s\n",str);

size=strlen(str);

for(i=0;i<size;i++)

{

if(str[i]!=' ')

numstr[i]=str[i]-'A';

}

lenumstr=i;

printf("Enter the key (Non repeated elements if possible)\n");

gets(key);

for(i=0,j=0;i<strlen(key);i++)

{

if(key[i]!=' ')

{

key[j]=toupper(key[i]);

j++;

}

}

key[j]='\0';

printf("%s\n",key);

```
k=0;  
  
for(i=0;i<strlen(key)+26;i++)  
{  
if(i<strlen(key))  
{  
if(key[i]=='J')  
{  
flag=8;  
printf("%d",flag);  
}  
numkey[i]=key[i]-'A';  
}  
else  
{  
if(k!=9 && k!=flag)  
{  
numkey[i]=k;  
}  
k++;  
}  
}  
}
```

```
templen=i;  
  
lenkey=removerepeated(templen,numkey);  
  
printf("Entered key converted according to Play Fair Cipher rule\n");  
  
for(i=0;i<lenkey;i++)  
  
{  
  
    printf("%c",numkey[i] +'A');  
  
}  
  
printf("\n");  
  
k=0;  
  
for(i=0;i<5;i++)  
  
{  
  
    for(j=0;j<5;j++)  
  
    {  
  
        cipherkey[i][j]=numkey[k];  
  
        k++;  
  
    }  
  
}  
  
printf("Arranged key\n");  
  
for(i=0;i<5;i++)  
  
{  
  
    for(j=0;j<5;j++)
```

```
{  
  
    printf("%c ",cipherkey[i][j] +'A');  
  
}  
  
printf("\n");  
  
}  
  
for(i=0;i<lennumstr;i+=2)  
  
{  
  
    if(numstr[i]==numstr[i+1])  
  
    {  
  
        insertelementat(i+1,numstr,lennumstr);  
  
        lenumstr++;  
  
    }  
  
}  
  
if(lennumstr%2!=0)  
  
{  
  
    insertelementat(lennumstr,numstr,lennumstr);  
  
    lenumstr++;  
  
}  
  
printf("Entered String/Message After Processing according to Play fair cipher  
rule\n");
```

```
for(i=0;i<lennumstr;i++)  
{  
printf("%c",numstr[i]+"'A');  
}  
  
for(k=0;k<lennumstr;k+=2)  
{  
for(i=0;i<5;i++)  
{  
for(j=0;j<5;j++)  
{  
if(numstr[k]==cipherkey[i][j])  
{  
row1=i;  
col1=j;  
}  
if(numstr[k+1]==cipherkey[i][j])  
{  
row2=i;  
col2=j;  
}  
}  
}
```

```
}

if(row1==row2)

{

col1=(col1-1)%5;

col2=(col2-1)%5;

if(col1<0)

{

col1=5+col1;

}

if(col2<0)

{

col2=5+col2;

}

numcipher[k]=cipherkey[row1][col1];

numcipher[k+1]=cipherkey[row2][col2];

}

if(col1==col2)

{

row1=(row1-1)%5;

row2=(row2-1)%5;

if(row1<0)

{
```

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

```
row1=5+row1;  
}  
  
if(row2<0)  
{  
    row2=5+row2;  
}  
  
numcipher[k]=cipherkey[row1][col1];  
  
numcipher[k+1]=cipherkey[row2][col2];  
}  
  
if(row1!=row2&&col1!=col2)  
{  
    numcipher[k]=cipherkey[row1][col2];  
  
    numcipher[k+1]=cipherkey[row2][col1];  
}  
}  
  
printf("\nCipher Text is\n");  
  
  
for(i=0;i<lennumstr;i++)  
{  
    if((numcipher[i]+'&')!='X')  
        printf("%c",numcipher[i]+'&');  
}
```

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

```
printf("\n");
```

```
}
```

```
int removerepeated(int size,int a[])
```

```
{
```

```
int i,j,k;
```

```
for(i=0;i<size;i++)
```

```
{
```

```
for(j=i+1;j<size;)
```

```
{
```

```
if(a[i]==a[j])
```

```
{
```

```
for(k=j;k<size;k++)
```

```
{
```

```
a[k]=a[k+1];
```

```
}
```

```
size--;
```

```
}
```

```
else
```

```
{  
    j++;  
}  
}  
}  
return(size);  
}
```

```
int insertelementat(int position,int a[],int size)
```

```
{  
    int i,insitem=23,temp[size+1];  
    for(i=0;i<=size;i++)  
    {  
        if(i<position)  
        {  
            temp[i]=a[i];  
        }  
        if(i>position)  
        {  
            temp[i]=a[i-1];  
        }  
        if(i==position)
```

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

```
{  
    temp[i]=insitem;  
}  
  
}  
  
for(i=0;i<=size;i++)  
{  
    a[i]=temp[i];  
}  
}
```

```
C:\Users\tansh\Desktop\New folder (4)\playfairdecr.exe  
Enter a string  
TSBPBV  
Entered String is TSBPBV  
Enter the key (Non repeated elements if possible)  
tanishq  
TANISHQ  
Entered key converted according to Play Fair Cipher rule  
TANISHQBCDEFGKLMOPRUVWXYZ  
Arranged key  
T A N I S  
H Q B C D  
E F G K L  
M O P R U  
V W X Y Z  
Entered String/Message After Processing according to Play fair cipher rule  
TSBPBV  
Cipher Text is  
SINGH  
-----  
Process exited after 18.37 seconds with return value 0  
Press any key to continue . . .
```

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

## Lab Assignment 5

Write a c program to implement encryption and decryption using affine cipher.

```
#include<bits/stdc++.h>

using namespace std;

const int a = 17;
const int b = 20;

string encryptMessage(string msg)

{

    string cipher = "";
    for (int i = 0; i < msg.length(); i++)

    {

        if(msg[i]!=' ')
            cipher = cipher +
                (char) (((a * (msg[i]-'A') ) + b) % 26) + 'A';
        else
            cipher += msg[i];
    }
}
```

```
return cipher;  
}  
  
string decryptCipher(string cipher)  
{  
    string msg = "";  
    int a_inv = 0;  
    int flag = 0;  
    for (int i = 0; i < 26; i++)  
    {  
        flag = (a * i) % 26;  
        if (flag == 1)  
        {  
            a_inv = i;  
        }  
    }  
    for (int i = 0; i < cipher.length(); i++)  
    {  
        if(cipher[i]!=' ')  
            msg = msg +  
                (char) (((a_inv * ((cipher[i] +'A' - b)) % 26)) + 'A');
```

```
else

msg += cipher[i];

}

return msg;

}

int main(void)

{

string msg = "I AM TANISHQ";



string cipherText = encryptMessage(msg);

cout << "Encrypted Message is : " << cipherText << endl;

cout << "Decrypted Message is: " << decryptCipher(cipherText);

return 0;

}
```

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

```
C:\Users\tansh\Desktop\New folder (4)\affine.exe
Encrypted Message is : A UQ FUHAOJG
Decrypted Message is: I AM TANISHQ
-----
Process exited after 0.1757 seconds with return value 0
Press any key to continue . . .
```

## Lab Assignment 6

Write a c program to implement encryption and decryption using vigenere cipher.

```
#include <iostream>
#include <string>
using namespace std;
class Vig {
public:
    string k;
    Vig(string k) {
        for (int i = 0; i < k.size(); ++i) {
            if (k[i] >= 'A' && k[i] <= 'Z')
                this->k += k[i];
            else if (k[i] >= 'a' && k[i] <= 'z')
                this->k += k[i] + 'A' - 'a';
        }
    }
    string encryption(string t) {
        string output;
        for (int i = 0, j = 0; i < t.length(); ++i) {
            char c = t[i];
            if (c >= 'a' && c <= 'z')
                c += 'A' - 'a';
            output += c;
        }
        return output;
    }
};
```

```
else if (c < 'A' || c > 'Z')
    continue;

    output += (c + k[j] - 2 * 'A') % 26 + 'A';

    j = (j + 1) % k.length();

}

return output;

}

string decryption(string t) {

    string output;

    for (int i = 0, j = 0; i < t.length(); ++i) {

        char c = t[i];

        if (c >= 'a' && c <= 'z')

            c += 'A' - 'a';

        else if (c < 'A' || c > 'Z')

            continue;

        output += (c - k[j] + 26) % 26 + 'A';

        j = (j + 1) % k.length();

    }

    return output;

};

int main() {
```

```
Vig v("hello");

string ori ="iamtanishq";

string encrypt = v.encryption(ori);

string decrypt = v.decryption(encrypt);

cout << "Original Message: "<<ori<< endl;

cout << "Encrypted Message: " << encrypt << endl;

cout << "Decrypted Message: " << decrypt << endl;

}
```

```
C:\Users\tansh\Desktop\New folder (4)\vignere.exe
Original Message: iamtanishq
Encrypted Message: PEXEOUMDSE
Decrypted Message: IAMTANISHQ

-----
Process exited after 0.2084 seconds with return value 0
Press any key to continue . . .
```

Name : Janisha Singh  
Course : BSc - IT (6<sup>th</sup> Sem)  
Rollno : 1022771(61)

## Assignment

Problem Statement :  
Critical evaluation of 'Gleevac' drug case in India.

Objective :  
To understand the Novartis cancer drug Gleevac case.

Introduction :  
The judgement rendered by the Supreme court in the case of Novartis AG v. Union of India is one of the landmark judgement of the Supreme Court. The decision came as a relief for millions of people around the world to have access to the medicines at low cost, thus preventing the pharmaceutical industries from 'evergreening' their patents. While the judgement is seen as a means to ensure the availability of life-saving drugs at an affordable price to people in India elsewhere, at the same time the decision defined the scope of Section 3(d) of the Indian Patents (Amendment) Act, 2005.

Brief facts of the case :  
In 1997, Novartis, a Swiss based pharmaceutical giant filed an application to grant patent to an anticancer drug Gleevac which is used to treat Chronic Myeloid Leukemia (CML) and Gastrointestinal Stromal Tumours (GIST) on the basis that It invented the beta crystalline salt

(imatinib mesylate) of the free base, imatinib. It is a critical drug which is patented in about 35 countries of the world.

However during those days, India did not grant patent to pharmaceutical products and agrochemical products. It was in the year 2005; the drug became the subject of patent in compliance with the TRIPS agreement. Indian then revised the patent law and started giving patent to pharmaceutical products. Subsequently in 2006, the Madras Patent Office refused the patent application of Novartis for its drug Glivec stating that the drug did not exhibit any major changes in therapeutic effectiveness over its pre-existing form which was already patented outside India. The said decision was based on Section 3(d) of the Indian Patents (Amendment) Act, 2005 which provides a known substance can only be patented if its new forms exhibit "enhanced efficacy".

In May 2006, Novartis filed two writ petitions under Article 226 of the Indian Constitution before the High Court of Madras - one appealing against the order the Madras Patent House/Office rejecting its patent request and the other consenting that Section 3(d) of the Indian Patents Act is not in compliance with TRIPS and is vague, arbitrary, violates ~~the~~ violative of Article 14 of the Constitution.

The Madras High Court refused the Writ petition of Novartis holding that it did not have jurisdiction whether a domestic law is contrary

to the International treaty, so it cannot decide whether Section 3(d) is in compliance with TRIPS. As far as Section 3(d) is concerned, the objective of the Amending Act was to prevent evergreening and to make easy the access of the life-saving drugs to the citizen.

The new phase of litigation started in Intellectual Property Appellate Board, which is an appellate body of patent controller. IPAB considered the beta crystalline form of imatinib mesylate as new and an inventive step but refused to grant a patent to the drug of Novartis since it was hit by Section 3(d) of the Act. Novartis filed the said order by filling special leave petition before the Supreme Court.

#### Observations of Supreme Court

The main issues that came before the Supreme Court was:

- i) Whether the invention is inconsistent with the Section 3(d) of the Patent Act?
- ii) Interpretation of Section 3(d) of Patent Act.
- iii) Whether the invention qualifies for the test of novelty and inventive for alleged products.

The Supreme Court adopted the following approach:

- i) Court observed that the product was one of the new form of the substance and not a whole substance. It has always existed in the original amorphous form. The product thus fails to qualify the test laid by the section 3(d) of Patent Act.

- ii) The Section clearly specifies that a new form of the substance is not patentable under Indian law unless it enhances its "known efficacy".

iii) Novartis contended that the physico-chemical properties of the polymorph form of the imatinib molecule i.e. better flow properties, better thermodynamic stability, resulted in improved efficacy and hence is patentable.

The Apex Court rejected this contention stating that in the case of medicine, improved efficacy means "therapeutic efficacy" and these properties while they may be beneficial do not meet the standard.

### Conclusion

The SC judgement came as a huge relief for those people who cannot afford the lifesaving drugs manufactured by those big pharma giants. These companies who have already made billions of dollar prevent people from purchasing the drug at low price thus endangering the very life of the poor people by acquiring patent over their drug. However, the Supreme Court made it clear in its judgement that India is a developing country and the availability of medicines at low price is necessary. Thus, SC is justified in its decision thereby prohibiting the liberal approach in granting patent to only genuine inventions.

Problem Statement:

'Exception' for grant of patent protection in India

Objective:

To understand the exceptions & limitation to the patent right.

Introduction:

The understanding of Intellectual Property Right (IPR) is crucial to promote innovation and growth of the country. The various form of IPRs are frequently talked about in the debates and general conversation. Despite that, some people still regard IPRs as an impediment in the growth of innovation and technology.

However, after signing of the World Trade Organization's Agreement on Trade-Relatable Aspects of Intellectual Property Rights (TRIPS), which allows Member Countries to provide more extensive protection of intellectual property, the exception and limitation of patent rights in India underwent something of an evolution. The "Exceptions to Rights Conferred" has been incorporated as Article 30 of TRIPS. It provides that Member Countries may provide limited exceptions to the exclusive rights conferred by the patent.

Types of Exception & Limitations

Article 30 of TRIPS allow for limited exception to the exclusive right conferred by a patent.

The exception must not be prejudicial to the legitimate interest of patent owner:

### Private and Non-commercial Use Exception

The exclusive rights conferred by the patent do not allow private use or monopoly over commercial activity. If the patentee is neither using nor vend-ing the invention for profit, the government has the power to grant a license, known as Compulsory Licence, to a third party to use the patented invention so as to restrict the rights of patentee for the purpose of preventing the abuse/misuse of the rights by the property holder. The provision of private and non-commercial use exception has been provided under the Section 84, Section 85 (Revocation of Patent by Controller), Section 92 (Special Provision for compulsory licenses on notification by Central Government) of Patents Act, 1970.

### Experimental/Scientific Use Exception

The experimental use exemption is incorporated under section 47 of the act. Under sub section 3 of the said section, the grant of a patent is subject to the condition that any product, in respect of which the patent is granted, may be made or used by the person for purpose merely of experiment or research including the imparting of instructions to pupils.

This is one of the most widely known exception to patent rights and it grew up to be out of concern that patent right should not hamper the "bona fide" experiments and scientific processes.

### Regulatory use/Prior-use Exemption

The patent rights, on the one hand, provide eco-nomic incentives to innovate, but on the other

hand, the exclusive rights they confer results in monopoly and unaffordable pharmaceutical products. Consequently, Indian Patent (Amendment) Act 2005 incorporated the regulatory-use or prior-use exemption under section 107A to offer a trade-off between incentives to the innovators, and limited access and costs to consumer.

This exemption is also termed as the Polar Provision and is a statutorily created exemption to patent rights that allows the manufacturing of generic drugs for obtaining marketing approval anywhere.

Foreign Vessels, Aircraft and Land Vehicles Exception  
As per Article 5 of Paris Convention, rights conferred by a patent shall not extend to the use of patented invention on board of vessels which such vessels temporarily or accidentally enters the water, provided that invention is used exclusively for need of vessel.

As this exception is not optional for countries party to Paris Convention, the Indian Patent Act, in order to comply, incorporated the said exception under Section 49. According to said section, patent rights are not infringed when the patented invention is used exclusively for the needs of foreign vessels, aircraft, or land vehicles and other accessories thereof, when such foreign vessel, aircraft / land vehicle accidentally enter India.

### Exhaustion of Patent Right

The Doctrine of Exhaustion or First Sale Doctrine refers to the exhaustion of the exclusive right of the patent holder once the patented invention

is sold without any restrictions. As per this Doctrine, the first unrestricted sale of the patented invention is sold without any restriction and exhausts the patentee's further control over the particular item.

The rationale behind the patent holder exhausting their rights once they sold the product is that, the first sale of the patent invention, the patent holder has already used exclusive right to prevent others from making, using, selling, offering for sale in territory of patent grant.

#### Conclusion

A Patent on an invention confers right on the patentee to exclude others from making, using, selling, offering for sale in the territory of patent grant or importing an invention into the territory of patent grant for limited time, in return for public disclosure of invention. This might have lead to monopoly and uncompetitive practices. Therefore, the TRIPs agreement introduce substantive provision on exception under Article 30 for sustainable growth and development of developing countries.

## Problem Statement

For the University you are studying in, identify the key assets and then identify major threat to these assets.

## Objective

Identification of key assets of security and then identifying major threat to these assets.

## Introduction

Basically, first of all let's see what does asset stands for! So, basically asset is any resource, process, product, or system that has some value to an organization, and must therefore be protected. Therefore, important key asset for an organization/universities are document drive, database containing sensitive employee details, or financial system containing tax information. All types of digital files, storage drive, laptop and hard drives containing information such as intellectual property, financial data, employee and student information, and so on. This thus enable the team to identify the most critical assets to put the proper security control in place. Once, as we have identified the organization critical assets, we need to examine (are vulnerable) or threat that an organization/university faces.

Basically, a threat here is any natural or artificial circumstances that can have an adverse affect/impact on the organization/

universities assets. Major threats to an universi-ties are phishing emails and it can be contro-lled by implementing technical control that filter and block suspicious email & strip out malicious links. We also should perform threat analysis on daily intervals. Other thre-ats involved as accessing the database to carry out sensitive data and then use it against the organization/universities. Introduc-tion of ~~as~~ malware such as trojan horse, worm, viruses on the systems is also a great threat to an university. ~~as~~ Introduction of malware through (LAN (Local Area Network) of organization) and to avoid it there there should be a ~~as~~ monthly network security checkup and the firewall must be maintained properly. You could simply make use of guest-access router ~~as~~ or multiple routers to avoid getting attacked or so. Other major threats are DOS and DDOS ~~as~~ attack (Denial of Service) or their even can be ~~as~~ financial frauds in the financial details database is not maintained properly.

## Conclusion

In the end, its just that we should ~~as~~ all be very carefull for what informatio-n we are sharing with the organization and hence follow certain/introduce security trends or policies which help us remain safe. We all should attend a cyber-security awareness camps and all and be constantly aware of our online security .

## Assignment 11

/Write a c program for encryption and decryption using Hill cipher.

```
#include<iostream>

#include<vector>

using namespace std;

int main()

{ int x,y,i,j,k,n;

cout<<"Enter the size of key matrix\n";

cin>>n;

cout<<"Enter the key matrix\n";

int a[n][n];

for(i=0;i>a[i][j]; }

}

cout<<"Enter the message to encrypt\n";

string s;

cin>>s;

int temp = (n-s.size()%n)%n;

for(i=0;i<<ans<<'\n'; return 0;

}
```

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

/\*OUTPUT

Enter the size of key matrix 2

Enter the key matrix

4 1

3 2

Enter the message to encrypt

helloworld

gdddaivyvn

## Assignment 12

//Write a c program for encryption and decryption using DES cipher.

```
#include
```

```
int main() {  
  
int i, cnt=0, p8[8]={6,7,8,9,1,2,3,4};  
  
int p10[10]={6,7,8,9,10,1,2,3,4,5};  
  
char input[11], k1[10], k2[10], temp[11];  
  
char LS1[5], LS2[5]; //k1, k2 are for storing interim keys  
  
//p8 and p10 are for storing permutation key
```

```
//Read 10 bits from user...
```

```
printf("Enter 10 bits input:");  
  
scanf("%s",input);  
  
input[10]='\0';  
  
for(i=0; i<10; i++)  
  
{  
  
cnt = p10[i];
```

```
temp[i] = input[cnt-1];  
}  
  
temp[i]='\0';  
  
printf("\nYour p10 key is :");  
  
for(i=0; i<10; i++)  
{ printf("%d,",p10[i]); }  
  
printf("\nBits after p10 :");  
  
puts(temp);  
  
//Performing LS-1 on first half of temp  
  
for(i=0; i<5; i++)  
{  
    if(i==4)  
        temp[i]=temp[0];  
    else  
        temp[i]=temp[i+1];  
}  
  
//Performing LS-1 on second half of temp  
  
for(i=5; i<10; i++)
```

```
{  
if(i==9)  
temp[i]=temp[5];  
else  
temp[i]=temp[i+1];  
}  
printf("Output after LS-1 :");  
puts(temp);  
printf("\nYour p8 key is :");  
for(i=0; i<8; i++)  
{ printf("%d,",p8[i]); }  
//Applying p8...  
for(i=0; i<8; i++)  
{  
cnt = p8[i];  
k1[i] = temp[cnt-1];  
}  
printf("\nYour key k1 is :");
```

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

puts(k1);

//This program can be extended to generate k2 as per  
DES algorithm.

}

Name:-Tanishq Singh  
Rollno:-1022771(61)

Course:-BSc-IT(6<sup>th</sup> Sem)  
Subject:-INFORMATION SECURITY

/\*Output of program

Enter 10 bits input:1100011100

Your p10 key is :6,7,8,9,10,1,2,3,4,5,

Bits after p10 :1110011000

Output after LS-1 :1100110001

Your p8 key is :6,7,8,9,1,2,3,4,

Your key k1 is :10001100

Applying p10...