SCHEME : K

Name : _____

Roll No. : _____ Year : 20___ 20___

Exam Seat No. : _____

LABORATORY MANUAL FOR

INFORMATION SECURITY-314319

COMPUTER ENGINEERING GROUP

MAHARASHTRA STATE BOARD OF
TECHNICAL EDUCATION, MUMBAI
(Autonomous) (ISO 9001: 2015) (ISO/IEC 27001:2013)

Vision

To ensure that the Diploma level Technical Education constantly matches the latest requirements of Technology and industry and includes the all-round personal development of students including social concerns and to become globally competitive, technology led organization.

Mission

To provide high quality technical and managerial manpower, information and consultancy services to the industry and community to enable the industry and community to face the challenging technological & environmental challenges.

Quality Policy

We, at MSBTE are committed to offer the best in class academic services to the students and institutes to enhance the delight of industry and society. This will be achieved through continual improvement in management practices adopted in the process of curriculum design, development, implementation, evaluation and monitoring system along with adequate faculty development programmes.

Core Values

MSBTE believes in the following:

- Skill development in line with industry requirements
- Industry readiness and improved employability of Diploma holders
- Synergistic relationship with industry
- Collective and Cooperative development of all stake holders
- Technological interventions in societal development
- Access to uniform quality technical education

Information Security

(314319)

Semester-IV

Diploma in Engineering and Technology

(Information Technology/Computer Science & Information Technology)

Maharashtra State Board of Technical Education, Mumbai

(Autonomous) (ISO 9001:2015) (ISO/IEC 27001:2013)

'K' Scheme Curriculum

Maharashtra State Board of Technical Education, Mumbai
(Autonomous) (ISO 9001:2015) (ISO/IEC 27001:2013)
4th Floor, Government Polytechnic Building
49, Kherwadi, Bandra (East), Mumbai – 400051

Maharashtra State Board of Technical Education
Certificate

This is to certify that Mr./Ms. …… Roll No…… of the Fourth Semester of Diploma in ……Engineering/Technology (Program Code - .....4K) of the Institute……(Inst. Code……) has completed the practical work satisfactorily for the course Information Security(Course Code: 314319) for the academic year 20….. – 20……. as prescribed in the curriculum.

Place ……. Enrollment No……

Date:…..... Exam Seat No. …….....

Course Teacher **Head of the Department** **Principal**

Seal of the Institute

Preface

Information Security (314319) laboratory manual is meticulously crafted to equip fourth semester diploma engineering students with valuable practical learning experiences aligned with MSBTE 'K' Scheme Curriculum.

The primary objective of this manual is to learn various techniques to secure user data and information in various formats. Ideally, protecting computer systems from attacks and unauthorized access means anticipating problems and devising strategies to address how people, processes, and technologies interact. The goal, although not always realistic, is to prevent these problems from happening instead of simply reacting to them as so many organizations do today. To achieve this, each practical is mapped with prescribed lab learning outcomes (LLOs) and course outcomes (COs). Course facilitators can adopt suitable pedagogical methods to impart the course with an aim to achieve the prescribed course outcomes effectively.

Lab activities include installation of required security software, authentication of computer system, securing files and folders with various techniques, implementation of various encryption techniques using c programs. It also focuses on firewall setting and gmail security which is widely used now days for communication. It is assured that with each practical of Information Security student will learn different security technique for securing the data and information either on computer on network.

We sincerely hope that this manual proves to be an instrumental resource in your professional journey toward choosing security as one of the career option.

Program Outcomes (POs) to be achieved through Practical:

PO1	Basic and Discipline specific knowledge: Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the engineering problems.
PO2	Problem analysis: Identify and analyses well-defined engineering problems using codified standard methods.
PO3	Design/ development of solutions: Design solutions for well-defined technical problems and assist with the design of systems components or processes to meet specified needs.
PO4	Engineering Tools, Experimentation and Testing: Apply modern engineering tools and appropriate technique to conduct standard tests and measurements.
PO5	Engineering practices for society, sustainability and environment: Apply appropriate technology in context of society, sustainability, environment and ethical practices.
PO6	Project Management: Use engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about well-defined engineering activities.
PO7	Life-long learning: Ability to analyses individual needs and engage in updating in the context of technological changes.

List of Relevant Skills

Technology is constantly evolving and making job roles more challenging and fascinating in Information Technology and Security. As technology enhances, information security threats also increase with the latest techniques and tactics.

- Analytical skills to collect and analyze information
- Strong security framework skills to effectively identify, protect, and respond to cyber threats.
- Working experience with the most common operating systems, such as iOS, Microsoft Windows, and Linux so that vulnerabilities are identified within the operating system resulting in a DoS attack. Good operating system skills help to update and patch the software security gaps to mitigate cyber-attacks.
- Data Privacy skills becoming a crucial part of security and compliance for businesses
- Critical thinking and problem-solving skills are required to determine the issue, develop the solution, and resolve the issue that helps to reduce the impact of security incidents.

Practical Course Outcome Matrix

Course Outcomes (COs)

CO1	Identify types of attacks which causes threat to Information Security
CO2	Apply multi-factor user authentication and access control mechanisms on file, folder, device and applications
CO3	Apply basic encryption / decryption techniques for a given text.
CO4	Apply various encryption algorithms used for information security.
CO5	Implement security techniques to prevent internet threats..

Sr. No.	Title of the Experiment	CO1	CO2	CO3	CO4	CO5
1	*i. Install and configure Antivirus software on system (Licensed copy) ii. Use privacy and security settings on operating system	✓				
2	*i.Set up single level authentication for computer system ii.Recover the password of computer system using any freeware password recovery tool (Example- John the ripper)		✓			
3	*i.Grant security to file, folder or application using access permissions and verify it ii.Grant access permission while sharing file and folder		✓			
4	Write a utility using C/Shell programming to create strong password authentication (Password should be more than 8 characters, and combination of digits, letters and special characters #, %, &, @)		✓			
5	*i.Write a C program to implement caesar cipher technique to perform encryption and decryption of text ii.Apply Caesar cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)			✓		
6	i.ImplementVernam cipher encryption technique to perform encryption of text using C programming language ii.ApplyVernam cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)			✓		
7	* Implement rail fence encryption technique to perform encryption of text using C programming language			✓		
8	Implement simple Columnar Transposition encryption technique to perform encryption of text using C programming language			✓		

9	Create and verify Hash Code for given message using any Open-source tool. (Example-Cryptool)			✓		
10	i.Write a C program to implement Diffie-Hellman key exchange algorithm to perform encryption of text ii. Use Diffie-Hellman key exchange algorithm to perform encryption and decryption of text using any open-source tool (Example - Cryptool)				✓	
11	* Use Steganography to encode and decode the message using any open-source tool (Example-OpenStego)				✓	
12	* Create and verify digital signature using any Opensource tool (Example-Cryptool)				✓	
13	* Configure firewall settings on any operating system					✓
14	Send a test mail securely using any open-source tool (Example- Pretty Good Privacy with GnuPG)					✓
15	Set up security policies for any web browser and Email account (Example: setting filter, spam for email security. Low security apps settings, cookies, synchronization for web browser))	✓				✓

Guidelines to Teachers

1. Teachers should explain prior concepts to students before staring each experiment.
2. Refer to laboratory learning outcome (LLOs) for the execution of the practical to focus on the defined objectives.
3. Promote life-long learning by training the students to equip themselves with essential knowledge, skills and attitudes.
4. If required, provide demonstration for the practical emphasizingon the skills that the student should achieve.
5. Teachers should give opportunity to the students for exhibiting their skills after the demonstration.
6. Provide feedback and/or suggestions and share insights to improve effectiveness.
7. Assess students' skill achievement related to COs of each unit.
8. Teachers may provide additional knowledge and skills to the students even though that may not be covered in manual but expected by students in industries.

Instructions for Students

1. 100% attendance is compulsory for all practical sessions.
2. Students must adhere to ethical practices.
3. Plagiarism is strictly prohibited.
4. Students should feel free to discuss any difficulties faced during the conduct of practical.
5. All the students must follow the schedule of practical sessions, complete the assigned work/activity and submit the assignment in stipulated time as instructed by the course teacher.
6. Follow formal attire and maintain personal appearance.

Content Page

List of Practical and Formative Assessment Sheet

Sr. No	Practical Title	Date of Performance	Date of Submission	Assessment Marks (25)	Teacher's Sign	Remark
1	*i. Install and configure Antivirus software on system (Licensed copy) ii. Use privacy and security settings on operating system					
2	*i.Set up single level authentication for computer system ii.Recover the password of computer system using any freeware password recovery tool (Example- John the ripper)					
3	*i.Grant security to file, folder or application using access permissions and verify it ii.Grant access permission while sharing file and folder					
4	Write a utility using C/Shell programming to create strong password authentication (Password should be more than 8 characters, and combination of digits, letters and special characters #, %, &, @)					
5	*i.Write a C program to implement caesar cipher technique to perform encryption and decryption of text ii.Apply Caesar cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)					
6	i.ImplementVernam cipher encryption technique to perform encryption of text using C programming language ii.ApplyVernam cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)					
7	* Implement rail fence encryption technique to perform encryption of text using C programming language					
8	Implement simple Columnar Transposition encryption technique					

	to perform encryption of text using C programming language					
9	Create and verify Hash Code for given message using any Open-source tool. (Example-Cryptool)					
10	i.Write a C program to implement Diffie-Hellman key exchange algorithm to perform encryption of text ii. Use Diffie-Hellman key exchange algorithm to perform encryption and decryption of text using any open-source tool (Example - Cryptool)					
11	* Use Steganography to encode and decode the message using any open-source tool (Example-OpenStego)					
12	* Create and verify digital signature using any Opensource tool (Example-Cryptool)					
13	* Configure firewall settings on any operating system					
14	Send a test mail securely using any open-source tool (Example- Pretty Good Privacy with GnuPG)					
15	Set up security policies for any web browser and Email account (Example: setting filter, spam for email security. Low security apps settings, cookies, synchronization for web browser))					
				Total		

***Total marks to be transferred to proforma published by MSBTE**

Note:

- '*' Marked Practicals (LLOs) are mandatory.
- Minimum 80% of above list of lab experiment are to be performed.
- Judicial mix of LLOs are to be performed to achieve desired outcomes.

Practical No. 1: *i. Install and configure Antivirus software on system (Licensed Copy)

I. Practical Significance

Antivirus software is a program designed and developed to protect computers formal ware like viruses, computer worms, spyware, botnets, rootkits, key loggers and such. It consists of three basic steps that are scan, detect and remove viruses from your computer.

The purpose of antivirus (AV) software is to detect, neutralize or eradicate malware (malicious software). AV software not only will identify and destroy the computer virus, but it also designed to fight off other kinds of threats such as phishing attacks, worms, Trojan horses,rootkits and more.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO1 - Identify types of attacks which causes threat to Information Security..

IV. Laboratory Learning Outcome(s)

LLO.1.1Install and configure Antivirus software on system

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Antivirus software, or anti-virus software (abbreviated to AV software), also known asantimalware, is a computer program used to prevent, detect, and remove malware.

Antivirus software was originally developed to detect and remove computer viruses, hence thename. However, with the proliferation of other kinds of malware, antivirus software started toprovide protection from other computer threats.In particular, modern antivirus software can protect users from: malicious browser helper objects (BHOs), browser hijackers, ransom ware, keyloggers, backdoors, rootkits, Trojan horses, worms, malicious LSPs, dialers, fraud tools, adwareand spyware. Some products also include protection from other computer threats, such asinfected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), onlinebanking attacks, social engineering techniques, advanced persistent threat (APT) and botnet DdoSattacks.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computerwith basic configuration	01
2	Operating System	Windows	01
3	Software	Antivirus Software	01

VIII. Precautions to be followed

1.Handle Computer System with care

2. Be caution while performing files related operations in computer System.

IX. Procedure

Steps to install antivirus (Steps for installation of Quickhealanti virus)

Once you have purchased the product, the next step is to install and register the product. Those opting to install Quick Heal on Windows 7/10 can use either of the two ways- Quick Heal CD for offline installation or setting up using product keys.

1. Install Quick Heal Total Security Antivirus from CD

- Insert Quick Heal CD in the CD drive of your PC.
- The installer willautorun without any external action.
- Click on Install Quick Heal.

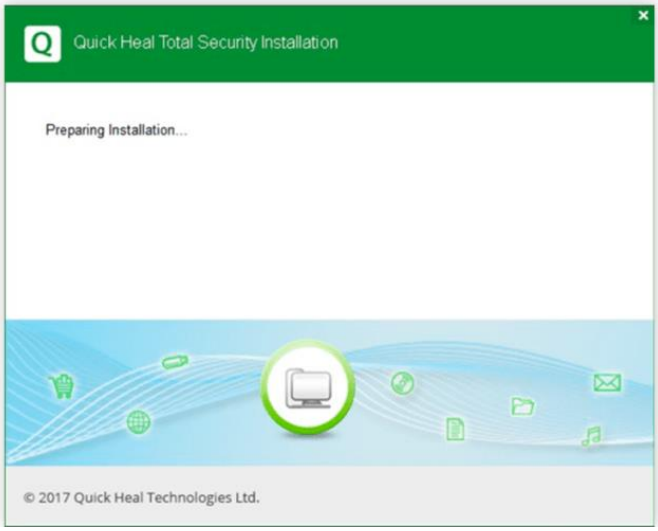


Fig.No.1.1.1

- Follow the steps in the setup wizard.
  - Read the User and License and Agreement carefully and check the box that says 'I Agree'

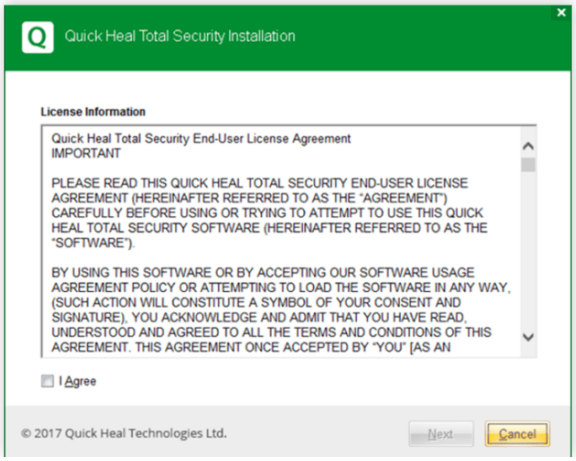


Fig.No.1.1.2

- Select the drive where the software is to be installed.

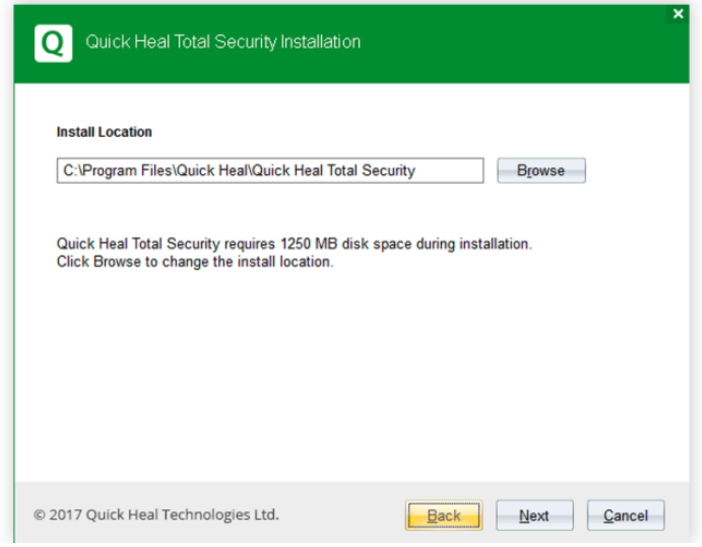


Fig.No.1.1.3

- Let it install files in the selected drive, till it is 100% complete.

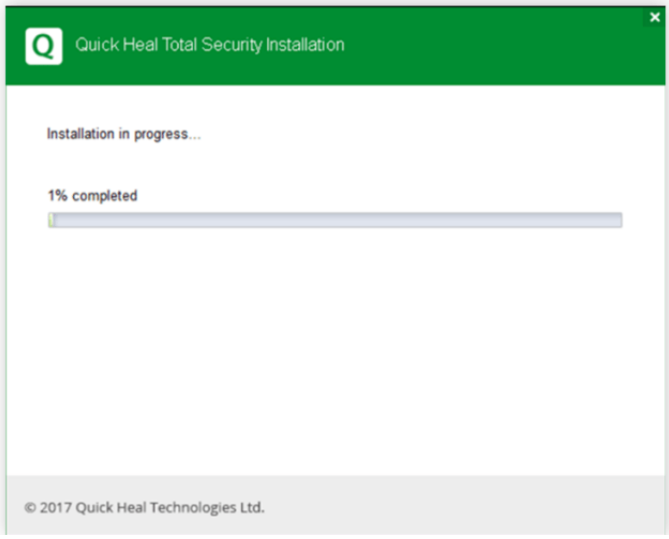


Fig.1.1.4

- Once completed, it will ask you to register the product. Click on 'Register Now'.

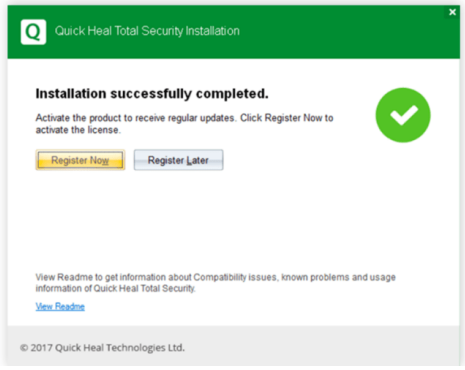


Fig.No. 1.1.5

2. Registering Quick Heal Antivirus License Offline

There are two ways of registering your Quick Heal copy. You can register offline if the system or device isn't connected to the Internet.

- Before visiting the offline activation page, ensure that you have the product key and the installation number with you.
- The product key can be found printed either on or inside the product packaging or will be provided when you purchase Quick Heal AntivirusTotal Security online.
- With the help of a connected device, visit the offline activation page
- Fill the registration form and enter the product key received after buying the product.

3. Installing Quick Heal Antivirus with Product Key Online

Buy Quick Heal Total Security key after installing the free version from the .exe file downloaded from the website. For premium and pro versions, register the product key provided with the product purchase. Here is how to register the Quick Heal Total Security antivirus online:

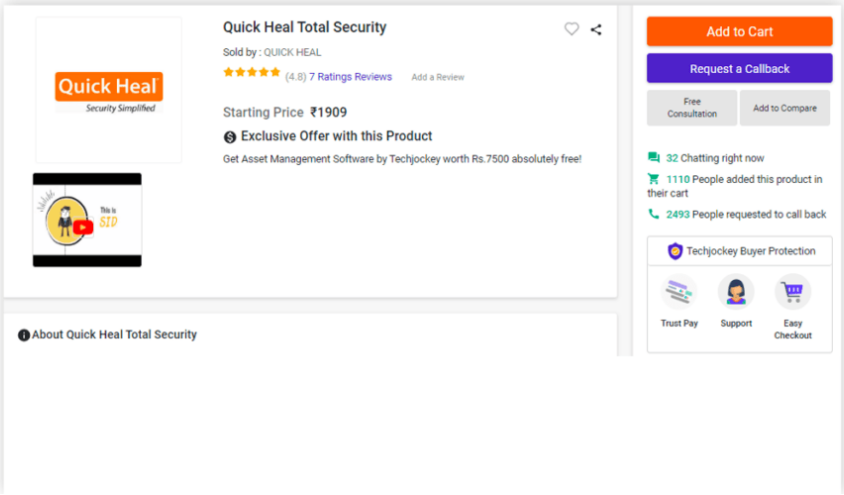


Fig1.1.6

- Sign-in to Quick Heal from your browser.
- Type in your email id and password for Quick Heal and click 'Sign In'.
- You can easily create account using the simple signing-up process in case you do not have an account with Quick Heal.
- Click 'Enter' a new product key to continue.
- Type the product key and click 'Next'.
- Follow the instructions to activate the product.

It is crucial for users to register their copy of Quick Heal Antivirus with the product key after installation. A registered user with a license will be given complete access to all the features of Quick Heal Total Security's features with regular updates and dedicated technical support. They will also receive Quick Heal Total Security antivirus renewal prompt when the renewal is due.

X. Conclusion

……

……

XI. Practical Related Questions

1. Define the term virus?
2. Describe the different phases of virus with suitable example?

Space for answer

XII. References/Suggestions for further reading

1. https://www.w3school.com/antivirus
2. https://www.webroot.com/gb/en/resources/tips-articles/what-is-anti-virus-software

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answerto sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 1: ii. Use privacy and security settings on operating system

I. Practical Significance

The privacy and security setting choose how much information you want to share with Microsoft by changing your privacy settings. Windows Security is an essential tool which helps to protect your computer from malware, viruses, and other security threats. It also includes features such as firewall and device security that can help prevent unauthorized access to your device.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO1 - Identify types of attacks which causes threat to Information Security.

IV. Laboratory Learning Outcome(s)

LLO.1. 2 Apply privacy and security settings to protect operating system.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Microsoft collects data to operate effectively and provide you the best experiences with our services. You provide some of this data directly, such as when you create a Microsoft account, submit a search query to Bing, speak a voice command to Cortana, upload a document to One Drive, complete a survey, or contact us for support. We get some of it by recording how you interact with our services by, for example, using technologies like cookies, and receiving error reports or usage data from software running on your device. Data such as this is usually used for Customer support, Product activation ,Service improvement, Security, safety and dispute resolution, Business operations.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computerwith basic configuration	01
2	Operating System	Windows	01

VIII. Precautions to be followed

1.Handle Computer System with care

2. Be caution while performing files related operations in computer System.

IX. Procedure

Privacy setting in the Windows 10 Operating System

This is the section where you can adjust a myriad of settings to protect your privacy and data from being transmitted to either Microsoft or third parties.

You can find it **Start > Settings > Privacy**.

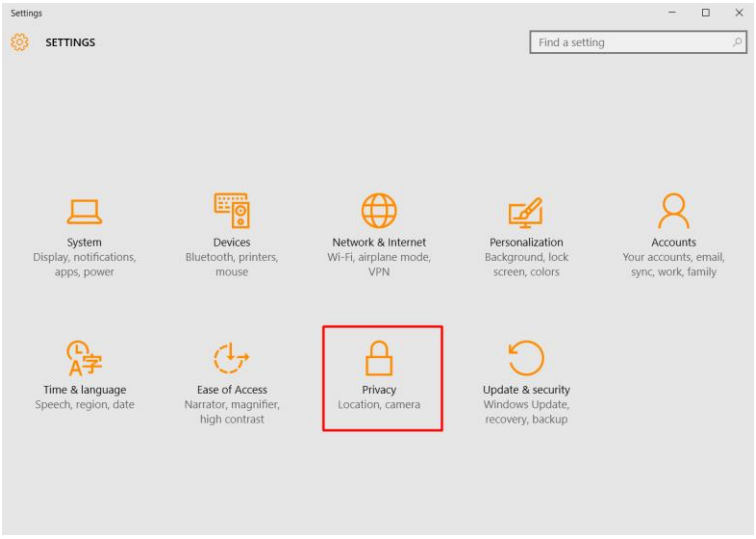


Fig. No. 1.2.1

You will be able to adjust following privacy settings:

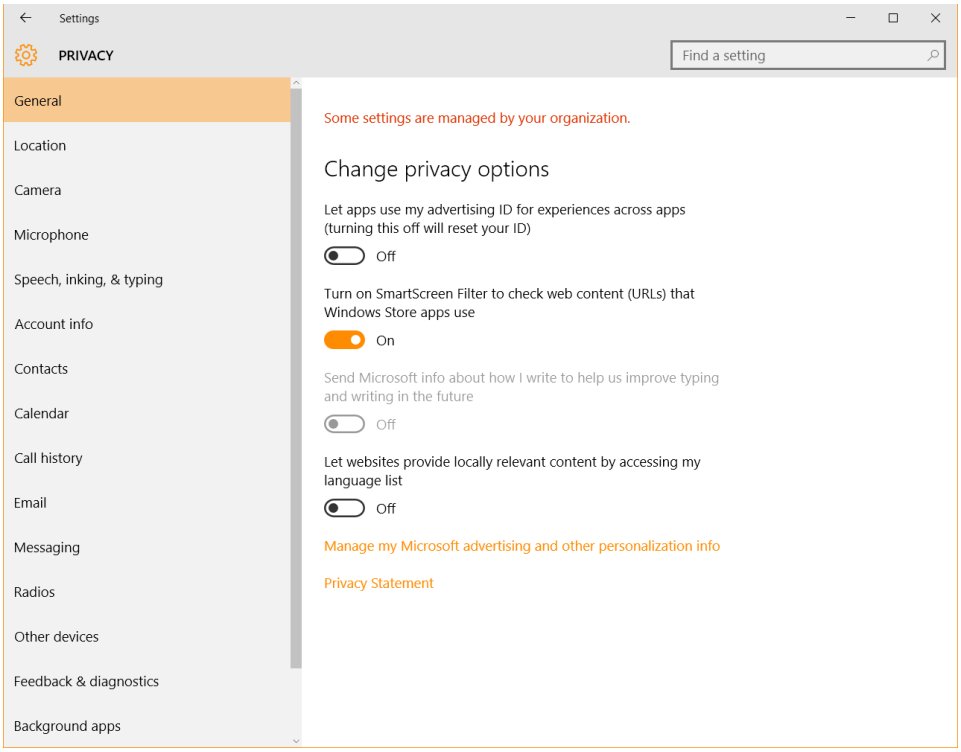


Fig. No1.2.2

1. **GENERAL PRIVACY SETTING**–

Two major types of settings you can adjust:

i. Turn a feature on or off

ii. Keep a feature on, but select which apps it can apply to

2. **LOCATION PRIVACY SETTING**– When it comes to **location data**, you can choose to turn it on or off.**If you choose to turn it on**, you can also control which applications can use your location information to offer tailored services and suggestions.

3. **CAMERA PRIVACY SETTING**– Here's where you decide if any apps can use your camera or if only some of them can.
4. **MICROPHONE PRIVACY SETTINGS**– When adjusting microphone settings, remember to keep the feature on for any apps that may actually require voice interaction, such as Skype or your voice recorder.
5. **SPEECH, INKING AND TYPING PRIVACY SETTINGS –**
   If you want to use Cortana, the personal assistant built into Windows 10, you can help her get to know you by letting her collect information about your speech and writing patterns.
6. **ACCOUNT INFO SECURITY SETTINGS –**
   If you want your apps to use your account information like name, birthdate, credit card details and so on.
7. **CONTACTS PRIVACY SETTINGS –**
   These setting allow your application to have access to your contacts
8. **CALENDAR PRIVACY SETTINGS -**

   These setting allow your application to use your calendar data.
9. **CALL HISTORY PRIVACY SETTINGS –** This setting share your call history data
10. **EMAIL PRIVACY SETTINGS -**
11. **MESSAGING PRIVACY SETTINGS -** Decide which apps, if any, should be able to read or send messages to your family, friends, coworkers and so on.
12. **RADIOS PRIVACY SETTINGS –** All setting of radio based technology is done here**.**
13. **OTHER DEVICES PRIVACY SETTINGS -** This is the place where you choose how your devices can connect to one another to share data.
14. **FEEDBACK AND DIAGNOSTICS PRIVACY SETTINGS**- Select how often Windows should ask for feedback.

You will be able to following Security Setting –

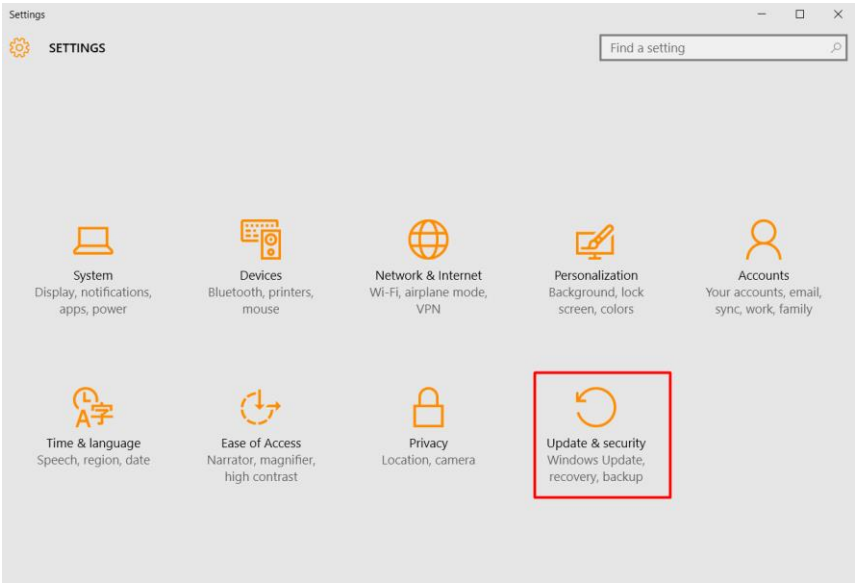


Fig. No.1.2.3

1. ACCOUNTS - When installing Windows 10, you'll be prompted to either log into your Microsoft account, if you have one, or you can choose to use a local account.

You can find the Account settings: Start > Settings > Accounts.

Here, you'll find 3 options:

- Change account settings
- Lock
- And Sign out.

Click on Change account settings to **adjust detailed settings** such as:

- Billing info, family settings, subscriptions, security settings and more for your Microsoft account (if you chose to log in with it) - this setting will take you to **https://account.microsoft.com/about**, where you can manage all these details;
- Sign in with a local account;
- Choose a picture for your account or create one using your computer's camera;
- Add other accounts to access email, calendar and contacts from;
- You can also add another Microsoft account or a work or school account to your device:

  From here you can also customize your sign-in options, such as:
  - Pick when Windows 10 should require you to sign in again;
  - Choose or change a password for your account;
  - Set up a PIN to use instead of passwords;
  - Set up Windows Hello to use biometric-based authentication, such as your fingerprint, instead of passwords;
- Set up a picture password.
- In the "Work access" section you'll be able to connect to your workplace or school account to get access to the data you have stored there.
- In the "Family & other users" section, you can set up dedicated accounts for your kids or other family members, with settings of their own. Here, you can also create guest accounts with limited access, to keep your system and data safe from intrusion.
- In the "Sync your settings" section, you'll be able to... sync your settings across devices (obviously). You can see, at a glance, what options you have and decide if and what data you want to make available on other devices you own that run Windows 10.

2. **UPDATES & SECURITY –**

i. **WINDOWS UPDATE** -

Follow this path to find it: Start > Settings > Update & Security > Windows Update. You get all windows update at once and they can actually be installed automatically or you can choose to be notified to schedule a restart.

ii. **WINDOWS DEFENDER** - Windows Defender is a software that attempts to detect and remove malware from your Windows-based computer. Microsoft released Windows Defender as an antispyware program initially, but improved it and embedded it into the operating system starting with Vista.

iii. **BACKUP -** Windows Backup provides a simple way to create a copy of your data on a connected disk drive (external storage device), so you can make sure that your data is safe if something happens to your computer**.**

iv. **RECOVERY -** You may find yourself in need to do a system recovery at some point.

v. **FIND MY DEVICE -** You can use "Find my device" to find your laptop if you misplaced it or if it was stolen

3. BITLOCKER ENCRYPTION - BitLocker is a full disk encryption feature integrated into Windows 10 that you can use to protect your data by encrypting it. Using BitLocker is easy, because it's built into the operating system, so there's no need to use additional software to encrypt and decrypt your data.

To find your encryption options, search for "control panel" , Choose "System and Security" And then go to BitLocker Drive Encryption:

4. TRUSTED APPS - This is a new feature integrated into the Windows Store. Long story short: every application distributed through the Windows Store has to be signed by either Microsoft or by a trusted vendor. This helps reduce the number of dangerous applications that can harm your data's safety or privacy from being sold or distributed through the store.

5.SMARTSCREEN FILTER - According to Microsoft, SmartScreen Filter is a technology embedded into the Windows Store and in Microsoft Edge that helps protect you against phishing attempts.

You can turn the SmartScreen Filter on and off by going to **Start > Settings > Privacy > General**. There, you can "Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use."

6. **MICROSOFT EDGE -** Microsoft Edge is the default browser in Windows 10, and its role is to replace Internet Explorer on all devices in the Windows ecosystem.

Edge claims to be a rather safe browser, because of the various integrated security settings and because it limits add-ons and plugins that can have a potential harmful impact.

7. **CYBER THREATS TARGETING WINDOWS 10 -** The new operating system brought some improvements in terms of security and some changes, but the most vulnerable applications continued to exist.

8. **RECOMMENDED SECURITY APPS FOR WINDOWS 10 -** Even if it claims to be "the most secure Windows" to date, Windows 10 is surely not impenetrable against cyber attacks. That's why you need additional applications to keep your data and confidential information safe.

There are 5 categories of security-related products recommend to install:

a. Antivirus
b. Antimalware
c. Password manager
d. Encryption tools
e. Backup solutions

X. Conclusion

……..…

……..…

……..…

XI. Practical Related Questions

1. Write steps to change password of your local account.
2. Control which apps and services have access to your location.

Space for answer

XII. References/Suggestions for further reading

1. https://heimdalsecurity.com/windows-10-security-guide/privacy
2. https://heimdalsecurity.com/windows-10-security-guide/security
3.https://www.practicalmoneyskills.com/en/resources/data_privacy/device-privacy-tips/How-Protect-Privacy-Windows10.html

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answerto sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 2: *i. Set up single level authentication for computer system

I. Practical Significance

Just as you want a lock on your front door, or a combination on your safe, digital assets should be protected against unwanted access from possibly malicious actors. Identity validation through authentication is the way that we protect critical assets in the digital world.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO2–Apply multi-factor user authentication and access control mechanisms on file, folder, device and applications

IV. Laboratory Learning Outcome(s)

LLO.2. 1 Setup and recover password of computer system.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Authentication is to prove that you are who claim to be. There are many different types of authentication which contribute to the network of digital security, including password-based, adaptive, SAML, SSO, out of band, biometric, token, and more.

Different types of authentication methods are there. The number of factors required for each authentication method is reflected in its name:

- **Single-factor Authentication (SFA)**: Requires users to provide one verifiable credential to access online resources.
- **Two-factor Authentication (2FA)**: Requires users to provide two verifiable credentials to access online resources.
- **Multi-factor authentication (MFA)**: Requires users to provide at least two verifiable credentials to access online resources.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computerwith basic configuration	01
2	Operating System	Windows 10	01

VIII. Precautions to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System.

IX. Procedure

Setting single level authentication

Click on the Windows icon in the bottom-left corner. Go to the top of the window and click on the username or you can find the Account settings: Start > Settings > Accounts.

Here, you'll find 3 options:

- Change account settings
- Lock
- And Sign out.

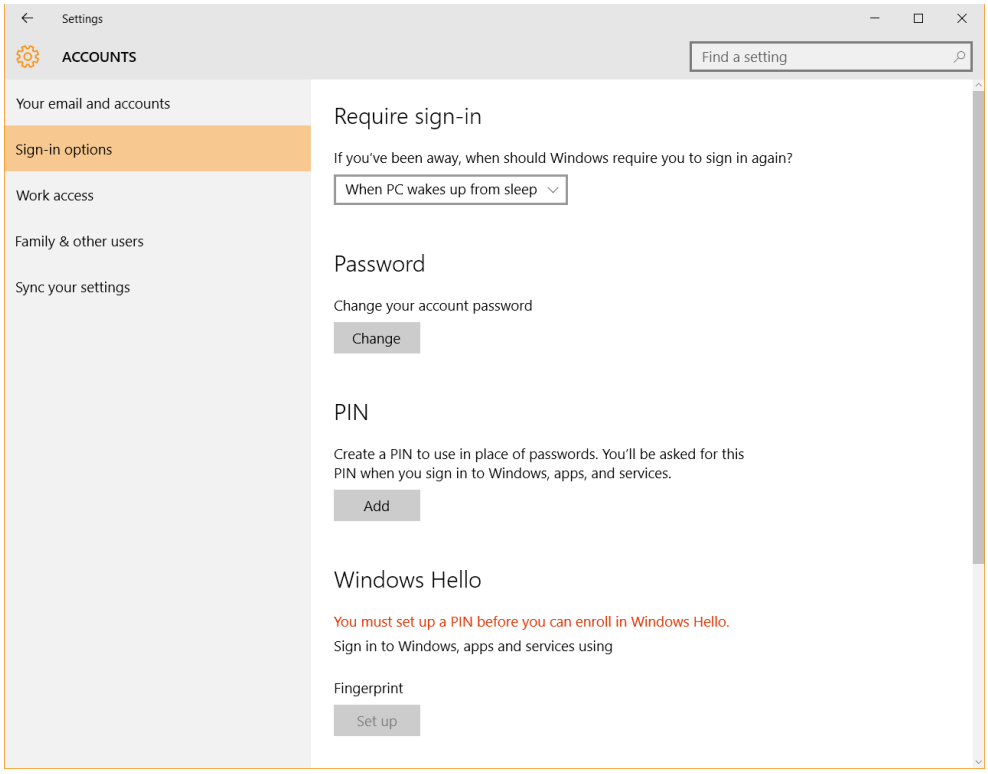


Fig. No. 2.1.1

From here you can also customize your sign-in options, such as:

- Pick when Windows 10 should require you to sign in again;
- **Choose or change a password for your account**
- Set up a PIN to use instead of passwords

X. Conclusion

……

……

XI. Practical Related Questions

1. List and explain different techniques used to improve the password security.
2. List and explain different password attacks.

Space for answer

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://www.wikihow.com/Password-Protect-Your-Windows-Computer
2. https://heimdalsecurity.com/windows-10-security-guide/security

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 2: ii. Recover the password of computer system using any freeware password recovery tool (Example- John the ripper)

I. Practical Significance

Valid credentials (username and password) enable a typical user to authenticate against a resource. If a username is known to threat actors, obtaining the account's password becomes a hacking exercise. Often, a threat actor will first target a systems administrator since their credentials may have privileges to directly access sensitive data and systems.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO2–Apply multi-factor user authentication and access control mechanisms on file, folder, device and applications

IV. Laboratory Learning Outcome(s)

LLO.2. 1 Setup and recover password of computer system.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Password cracking (also called password hacking) is an attack vector that involves hackers attempting to crack or determine a password for unauthorized authentication. Password hacking uses a variety of programmatic techniques, manual steps, and automation using specialized tools to compromise a password. These password cracking tools are referred to as 'password crackers'. Increasingly, these tools are leveraging AI to improve password cracking speed and efficiency. Passwords can also be stolen via other tactics, such as by memory-scraping malware, shoulder surfing, third party breaches, and tools like Redline password stealer.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computerwith basic configuration	01
2	Operating System	Windows / Linux Kali	01

VIII. Precautions to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System.

IX. Procedure

John Ripper Software

John the Ripper is a free password cracking software tool developed by Openwall. Originally developed for Unix Operating Systems but later on developed for other platforms as well. It is one of the most popular password testings and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types commonly found in Linux or Windows. It can also be to crack passwords of Compressed files like ZIP and also Documents files like PDF.

John the Ripper can be downloaded from Openwall's Website https://www.openwall.com/john/

John the Ripper comes pre-installed in Linux Kali and can be run from the terminal as shown below:

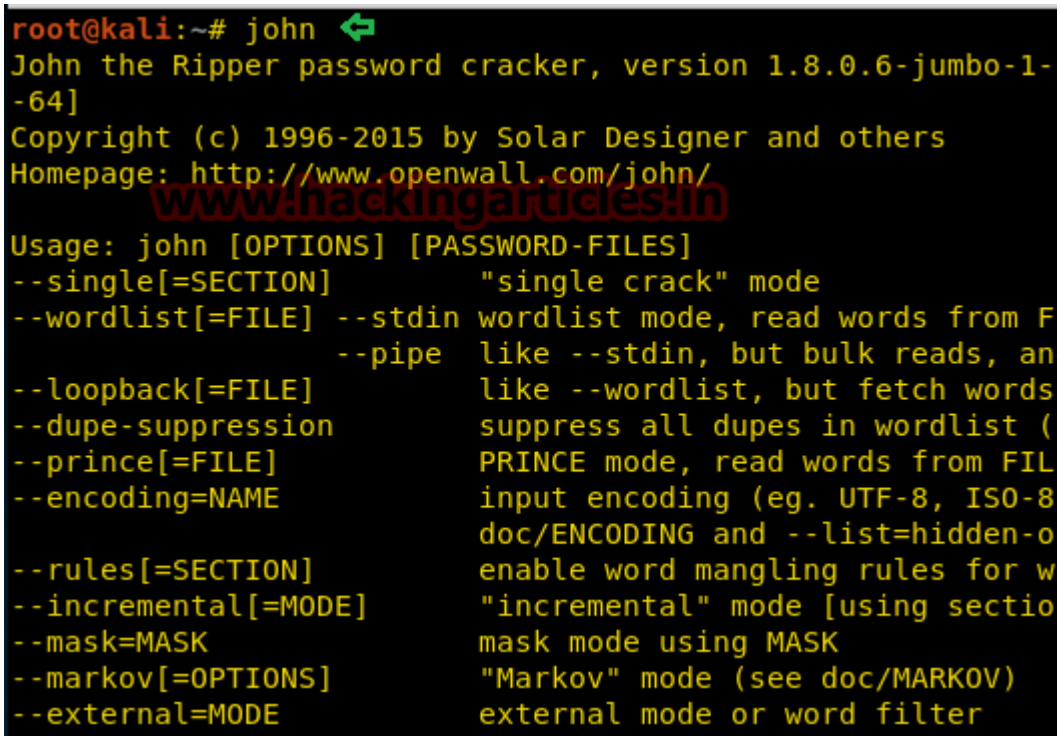


Fig. No. 2.2.1

John the Ripper works in 3 distinct modes to crack the passwords:

1. Single Crack Mode
2. Wordlist Crack Mode
3. Incremental Mode

1. John the Ripper Single Crack Mode

In this mode John the ripper makes use of the information available to it in the form of a username and other information. This can be used to crack the password files with the format of

Username: Password

For Example: If the username is "Hacker" it would try the following passwords:

hacker
HACKER
hacker1
h-acker
hacker=

We can use john the ripper in Single Crack Mode as follows:
Here we have a text file named crack.txt containing the username and pas sword, where the password is encrypted in SHA1 encryption so to crack this password we will use:

Syntax: john [mode/option] [password file]

```
john --single --format=raw-sha1 crack.txt
```

As you can see in the screenshot that we have successfully cracked the password.

Username: ignite

Password: IgNiTe

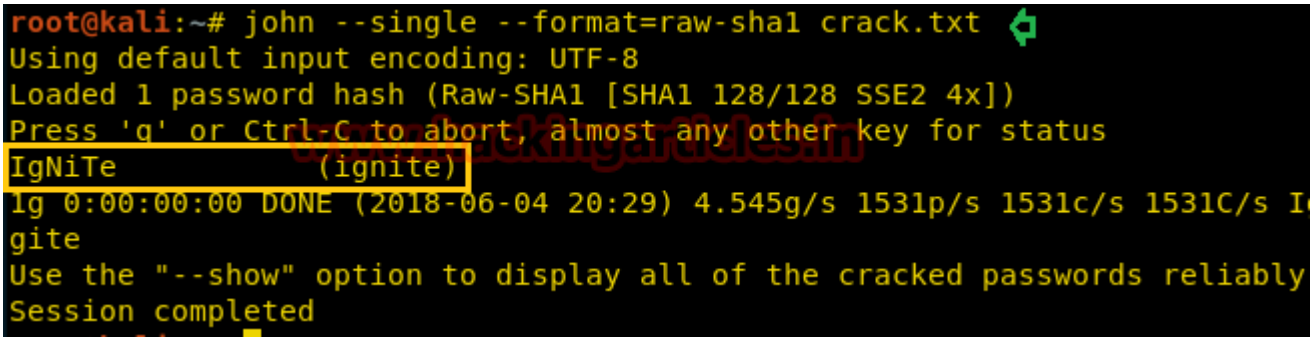


Fig. No. 2.2.2

2. John the Ripper Wordlist Crack Mode

In this mode John the ripper uses a wordlist that can also be called a Dictionary and it compares the hashes of the words present in the Dictionary with the password hash. We can use any desired wordlist. John also comes in build with a password.lst which contains most of the common passwords.

Let's see how John the Ripper cracks passwords in Wordlist Crack Mode:

Here we have a text file named crack.txt containing the username and password, where the password is encrypted in SHA1 encryption so to crack this password we will use:

Syntax: john [wordlist] [options] [password file]

```
john --wordlist=/usr/share/john/password.lst --format=raw-sha1 crack.txt
```

As you can see in the screenshot, john the Ripper have cracked our password to be asdfasdf

```
root@kali:~# john --wordlist=/usr/share/john/password.lst
--format=raw-sha1 crack.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])
Press 'q' or Ctrl-C to abort, almost any other key for sta
tus
asdfasdf         (pavan)
1g 0:00:00:00 DONE (2018-06-04 21:07) 1.562g/s 1175p/s 117
5c/s 1175C/s arizona..asdfasdf
Use the "--show" option to display all of the cracked pass
words reliably
Session completed
```

Fig. No. 2.2.3

3. Cracking the User Credentials

We are going to demonstrate two ways in which we will crack the user credentials of a Linux user.

Before that we will have to understand, what is a shadow file?

In the Linux operating system, a shadow password file is a system file in which encrypted user password is stored so that they are not available to the people who try to break into the system. It is located at /etc/shadow.

we will crack the credentials of a particular user "pavan".

Now to do this First we will open the shadow file as shown in the image.

```
root@kali:~# cat /etc/shadow
root:$6$QizMF3Ej$W7m6QbPmvRb4eyjt.Ic6KiwjCy/FU86vUucgdc/Z
.THObbp2VvMCEDJXAEt0ibpL0sV6Fxps.8k9FpmKKY1FJ.:17569:0:99
999:7:::
daemon:*:17557:0:99999:7:::
bin:*:17557:0:99999:7:::
sys:*:17557:0:99999:7:::
sync:*:17557:0:99999:7:::
games:*:17557:0:99999:7:::
man:*:17557:0:99999:7:::
lp:*:17557:0:99999:7:::
mail:*:17557:0:99999:7:::
news:*:17557:0:99999:7:::
uucp:*:17557:0:99999:7:::
proxy:*:17557:0:99999:7:::
www-data:*:17557:0:99999:7:::
backup:*:17557:0:99999:7:::
list:*:17557:0:99999:7:::
irc:*:17557:0:99999:7:::
```

Fig. No. 2.2.4

And we will find the credentials of the user pavan and copy it from here and paste it into a text file. Here we have the file named crack.txt.

Fig. No. 2.2.5

Now we will use john the ripper to crack it.

```
john crack.txt
```

As you can see in the image below that john the ripper has successfully cracked the password for the user pavan.

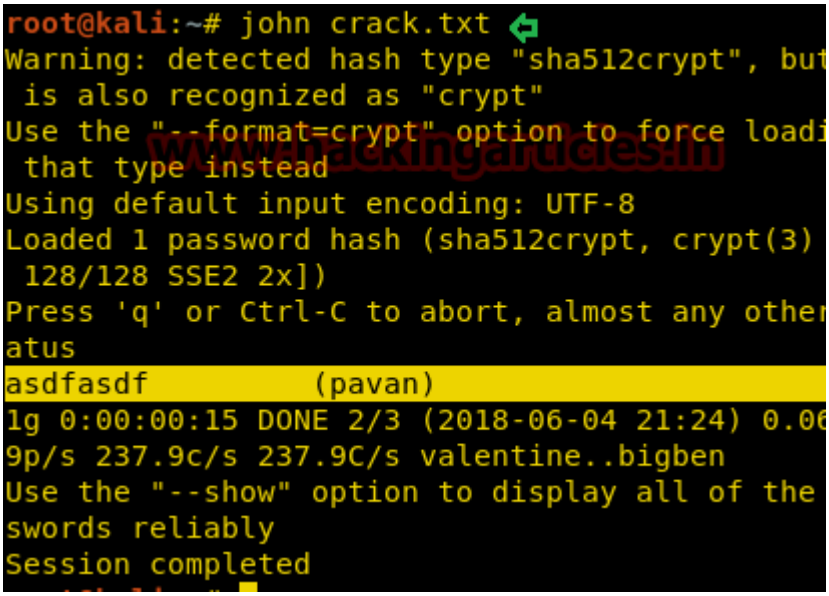


Fig. No. 2.2.6

X. Conclusion

……

……

XI. Practical Related Questions

1. List Password recovery tools available today.
2. Explain brute-force and dictionary attacks.

Space for answer

……

……

XII. References/Suggestions for further reading

1. https://www.beyondtrust.com/blog/entry/password-cracking-101-attacks-defenses-explained
2. https://www.hackingarticles.in/beginner-guide-john-the-ripper-part-1/

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 3: *i. Grant security to file, folder or application using access permissions and verify it

I. Practical Significance

Setting permissions is one of the most basic elements of web security. Assigning the correct permissions to the files and directories helps prevent data theft and malicious intrusions. Permissions specify who and what can read, write, modify, and access content on your site.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO2 – Apply multi-factor user authentication and access control mechanisms on file, folder, device and applications

IV. Laboratory Learning Outcome(s)

LLO 3.1 Grant read ,writeand execute permission onfile and folder.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

There are six standard permission types which apply to files and folders in Windows:

- Full Control
- Modify
- Read & Execute
- List Folder Contents
- Read
- Write
- Each level represents a different set of actions users can perform.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computerwith basic configuration	01
2	Operating System	Windows 10	01

VIII. Precautions to be followed

1.1. Handle Computer System with care

2. Be caution while performing files related operations in computer System.

IX. Procedure

Understanding and assigning File and Folder Permissions in Windows

Windows provides two sets of permissions to restrict access to files and folders: NTFS permissions and share permissions.

NTFS permissions are applied to every file and folder stored on a volume formatted with the NTFS file system. By default, permissions are inherited from a root folder to the files and subfolders beneath it. NTFS permissions take effect regardless of whether a file or folder is accessed locally or remotely. NTFS permissions, at the basic level, offer access levels of Read, Read and Execute, Write, Modify, List Folder Contents, and Full Control, as shown below:

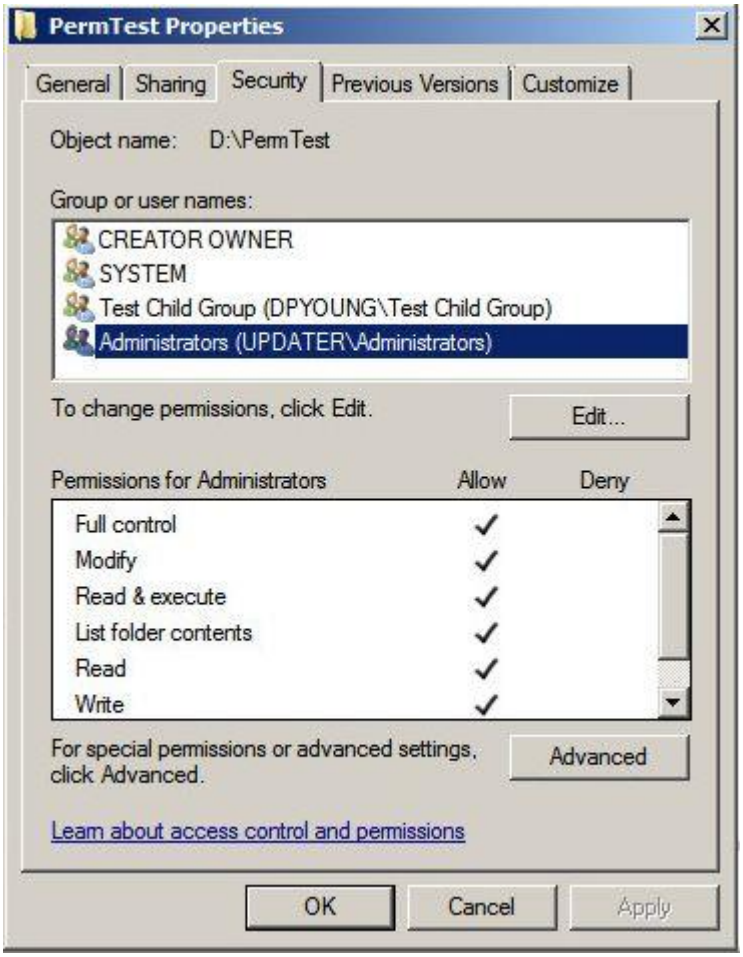


Fig. No. 3.1.1

Create a New Folder

In many cases you will need to create a new folder. If you are using an existing folder and do not wish to create a new folder, continue with *Accessing the Properties Dialog Box*.

1. Click on the Start menu.
2. Click Computer.
3. From the *Computer* window, select the shared drive for your area or department
4. Navigate to the location you want the new folder to appear (e.g., within one of your existing folders).

5. On the menu bar, select New Folder.
   OR
   Right click » select New » select Folder.
   A new folder is created which inherits the security permissions of its "parent."
6. In the newly created folder, type the desired folder name.
7. Press [Enter] or click off of the folder.

Accessing the Properties Dialog Box

When working with permissions in Windows 7, you are required to work from the *Properties* dialog box. This dialog box for the file or folder you are working with can be accessed in a few steps.

1. Click on the Start menu.
2. Click Computer.
3. Select the folder or file you wish to adjust/view permissions for.
4. Right-click the folder or file.
5. Select Properties.
   The *Properties* dialog box appears.

Granting Access to a File or Folder

After creating a new folder, or even if you will use an existing folder, you will need to determine who will have access to it. Also, keep in mind that by default the same persons who have access to the "parent" (original) folder also have access to the new folder, and vice versa. This may not be ideal. It is a simple process to grant access to specific users for any folder you have created.

1. Access the *Properties* dialog box.
2. Select the *Security* tab.

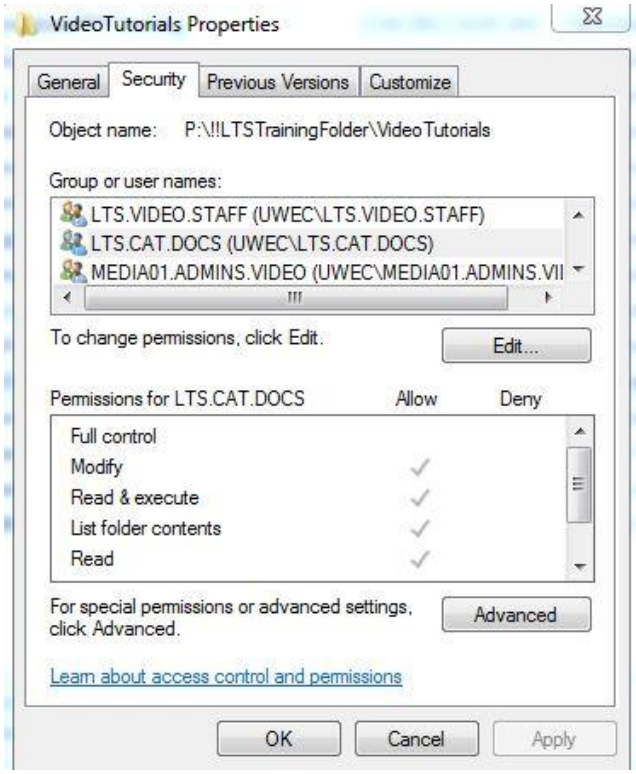


Fig. No. 3.1.2

3. Click Edit.
   The *security* tab opens in a new window.

4. Click Add...
   The *Select Users, Computers, or Groups* dialog box appears.

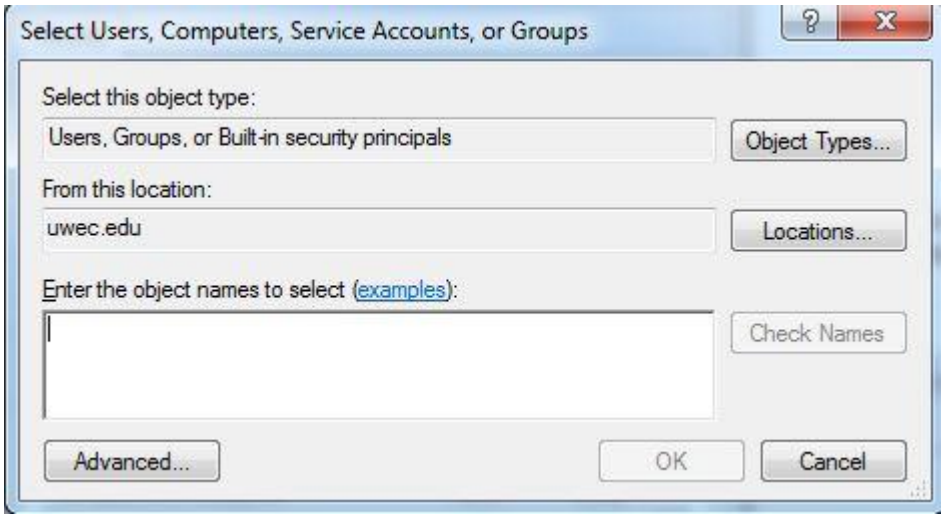


Fig. No. 3.1.3

5. In the *Enter the object names to select* text box, type the name of the user or group that will have access to the folder (e.g., 2125.engl.498.001 or username@uwec.edu).
   HINT: You may type the beginning of the name and then click Check Names. *The name will either be resolved or a list of users beginning with those characters will display for you to select from.*
6. Click OK.
   The *Properties* dialog box reappears.
7. Click OK on the *Security* window.
8. Continue with *Setting Permissions* below.

Setting Permissions

Once you have granted a group or individual user access to a folder, you will need to set permissions for the new user(s). When you set permissions, you are specifying what level of access a user(s) has to the folder and the files within it. Be careful about checking *Deny* for any permissions, as the *Deny* permission overrides any other related to *Allow* permissions.

Folder permissions can be changed only by the owner of the folder (i.e., the creator) or by someone who has been granted permission by the owner. If you are not the owner of the folder or have not been granted permission by the owner, all checkboxes will be gray. Therefore, you will not be able to make any changes until the owner grants you permission.

1. Access the *Properties* dialog box.
2. Select the Security tab.
   The top portion of the dialog box lists the users and/or groups that have access to the file or folder.

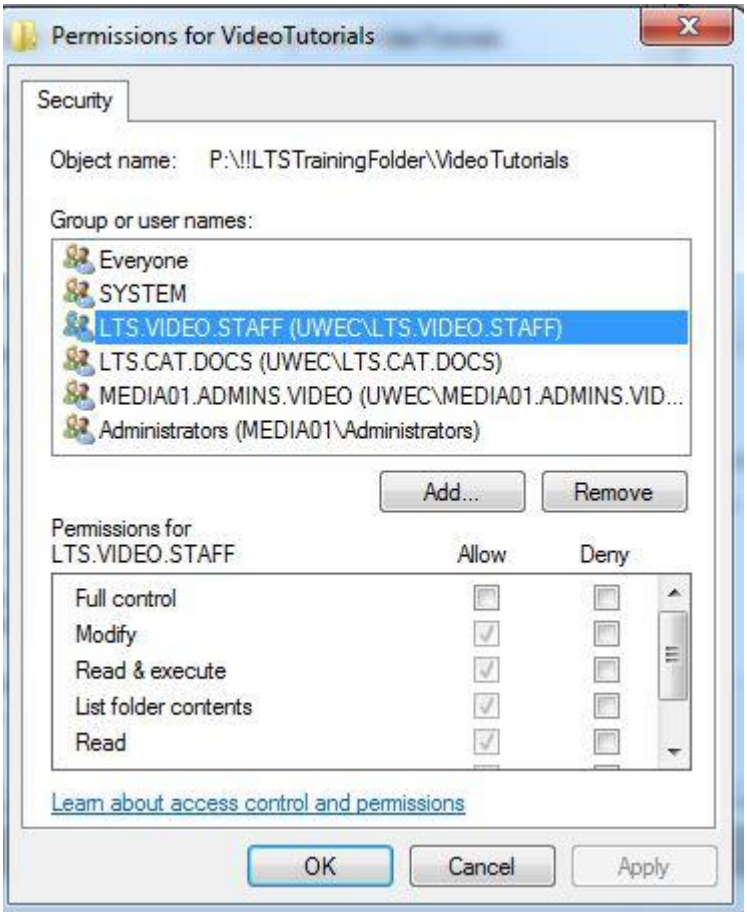


Fig. No. 3.1.4

3. Click Edit
4. In the *Group or user name* section, select the user(s) you wish to set permissions for
5. In the *Permissions* section, use the checkboxes to select the appropriate permission level
6. Click Apply
7. Click Okay

   The new permissions are added to the file or folder.

X. Conclusion

……

……

XI. Practical Related Questions

1. List and explain different ways to implement the access controls computer systems and networks
2. List and explain Different Access Control Policies.

Space for answer

……

……

……

XII. References/Suggestions for further reading

1. https://kb.uwec.edu/articles/drives-establishing-windows-file-and-folder-level-permissions#Create
2. https://www.dell.com/support/kbdoc/en-in/000137238/understanding-file-and-folder-permissions-in-windows
3. https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/access-control

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 3: ii. Grant access permission while sharing file and folder

I. Practical Significance

Setting permissions is one of the most basic elements of web security. Assigning the correct permissions to the files and directories helps prevent data theft and malicious intrusions. Permissions specify who and what can read, write, modify, and access content on your site.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO2 – Apply multi-factor user authentication and access control mechanisms on file, folder, device and applications

IV. Laboratory Learning Outcome(s)

LLO 3.1 Grant read, write and execute permission on file and folder.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

The file server permissions must be carefully implemented to provide appropriate access to content. This involves locking down permissions on the share and physical folders

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows 10	01

VIII. Precautions to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System.

IX. Procedure

Configuring Share Permission to File and Folder

1. In Windows Explorer, right-click the folder you want to share, and then click **Properties**.

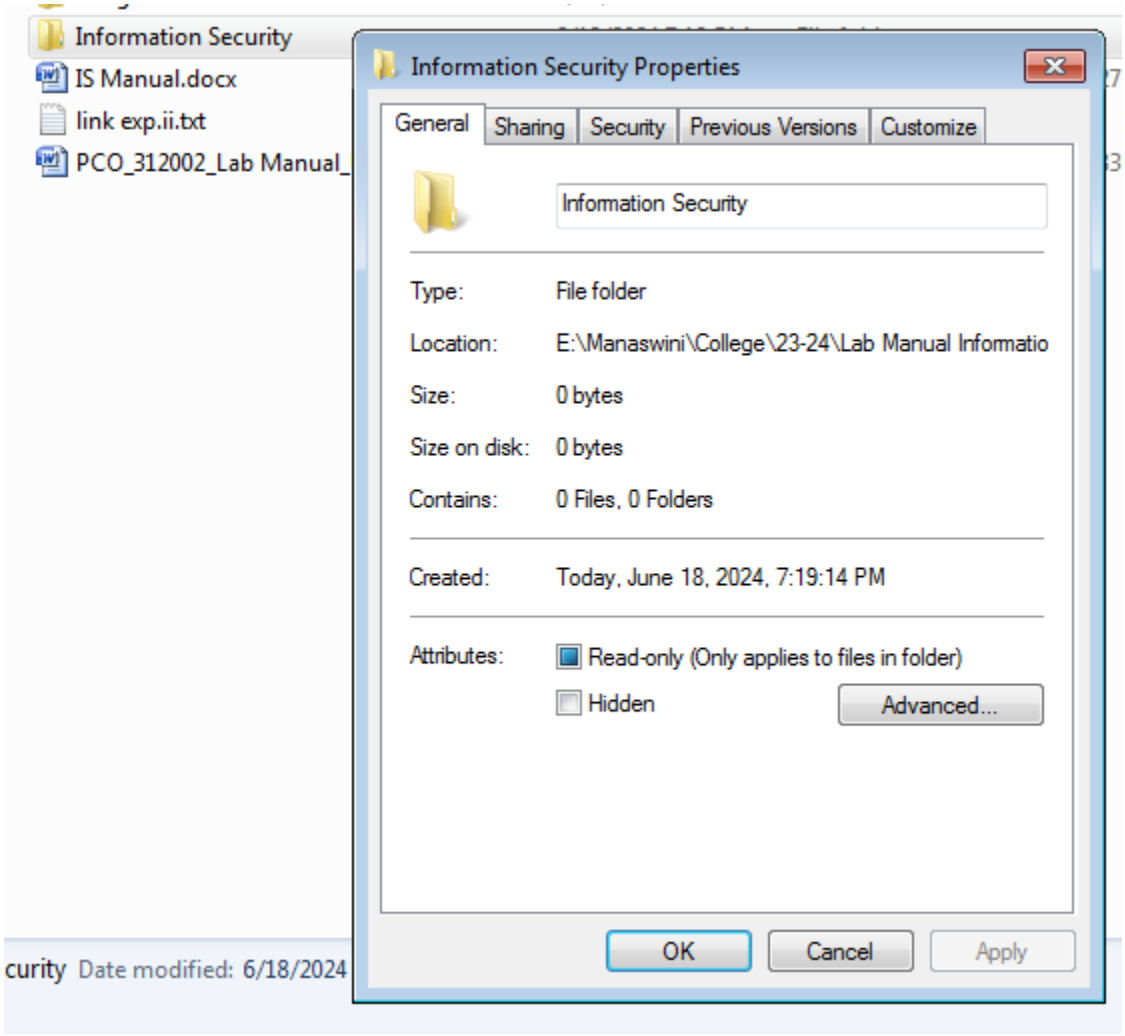


Fig. No.3.2.1

2. On the **Sharing** tab, click **Advanced Sharing**.
3. In User Account Control, click **Continue** to accept the prompt that Windows needs your permission to perform the action.
4. In the **Advanced Sharing** dialog box, check **Share this folder**.
5. Set the **Share name** and **Comments** as appropriate. To make the share hidden, add a $ to the end of the share name.

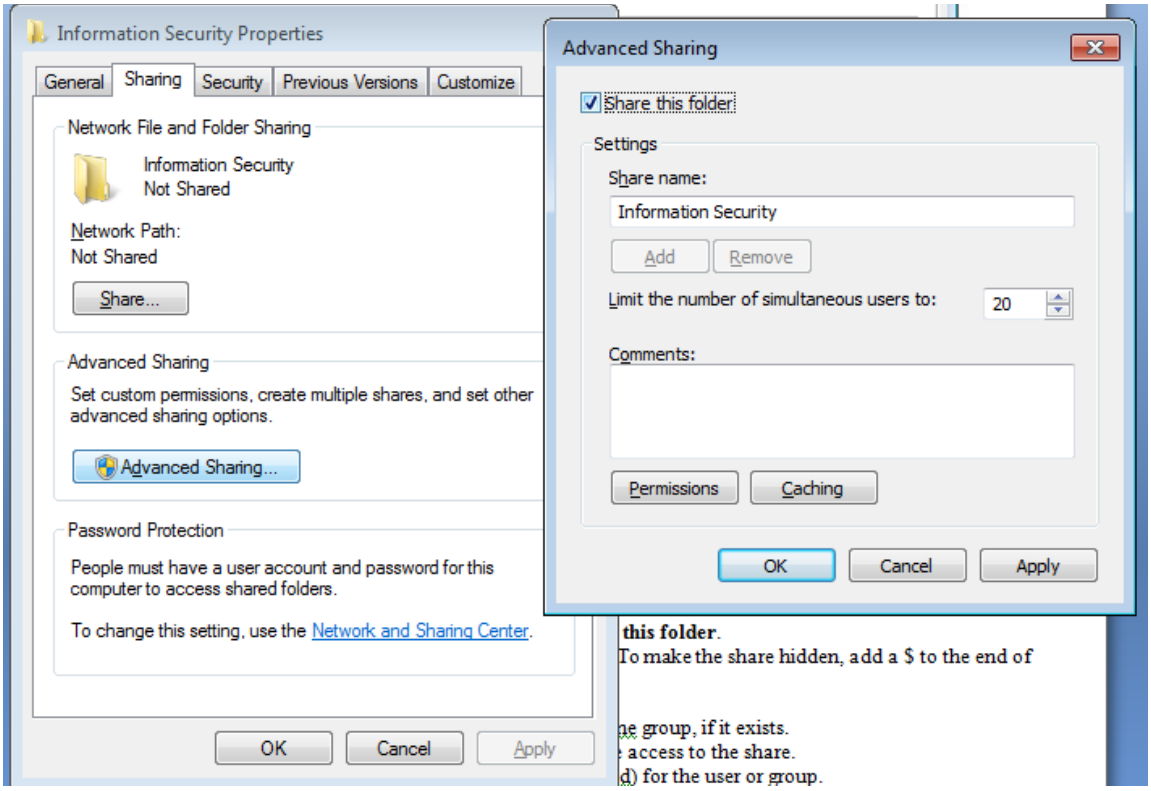


Fig. No. 3.2.2

6. Click **Permissions**.
7. Add the appropriate user or group that should have access to the share.
8. Specify the permissions (Full Control, Change, Read) for the user or group.

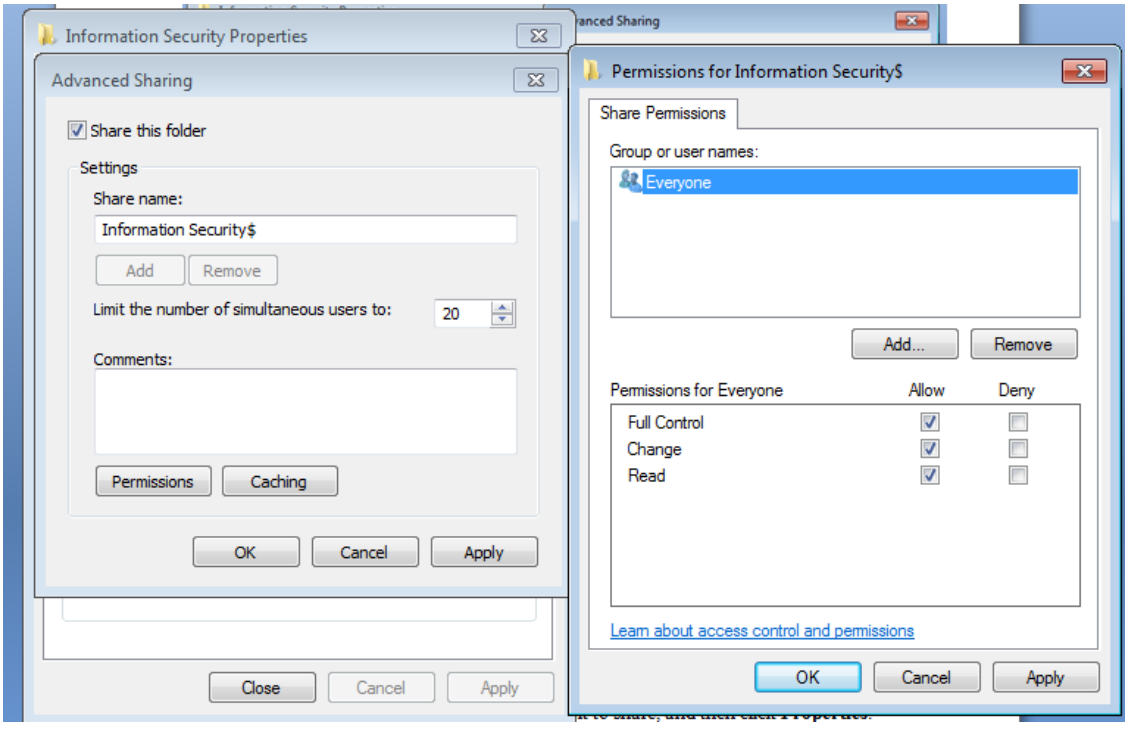


Fig. No. 3.2.3

9. Click **OK** twice and then click **Close** to close the dialog boxes.

X. Conclusion

……

……

XI. Practical Related Questions

1. Which of the following methods enable you to create shared network folders? [Check all correct answers]

a. Right-click a folder in either My Computer or Windows Explorer, select Sharing And Security, click the option button Share This Folder, and click OK.

b. Right-click a folder in either My Computer or Windows Explorer, select Properties, click the Sharing tab, click the option button Share This Folder, and click OK.

c. Open the Computer Management Console, expand Shared Folders, right-click the Shares node, and click New File Share. Follow the on-screen instructions for the Create Shared Folder Wizard.

d. Open a command prompt window. Type "Net Share share_name=x:\folder_name", where share_name represents the name you want to assign to the shared folder, x: represents the drive letter where the folder resides, and folder_name represents the actual name of the folder.

2. Explain Access Control Matrix(ACM).

Space for answer

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://learn.microsoft.com/en-us/iis/web-hosting/configuring-servers-in-the-windows-web-platform/configuring-share-and-ntfs-permissions
2. https://learn.microsoft.com/en-us/answers/questions/491526/sharing-folders-with-specific-computers-on-a-workg
3.https://answers.microsoft.com/en-us/windows/forum/all/access-to-shared-folder-on-windows-10/10756447-09d6-4655-ac4f-9d7a55f654c5

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 4: Write a utility using C/Shell programming to create strong password authentication (Password should be more than 8 characters, and combination of digits, letters and special characters #, %, &, @)

I. Practical Significance

A strong password is one that is difficult to guess or crack through brute-force attacks.Weak passwords are a significant security risk and can lead to data breaches. Strong passwords are important because they help prevent unauthorized access to personal information and accounts. This is especially important for accounts containing sensitive information, such as financial email and social media accounts.

II. Industry / Employer Expected Outcome(s)

Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO2 – Apply multi-factor user authentication and access control mechanisms on file, folder, device and applications

IV. Laboratory Learning Outcome(s)

LLO 4 .1 Implement Password Authentication.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Weak passwords can expose your accounts to hacking attempts, including brute-force attacks, dictionary attacks, and other malicious techniques. Robust passwords possess the following characteristics:

1. **Complexity:** Incorporating a mix of uppercase letters, lowercase letters, digits, and special characters.
2. **Length:** Longer passwords inherently offer greater security.
3. **Unpredictability:** Avoiding easily guessable patterns and common words.
4. Understanding the probability of password generation is a fundamental concept. It reveals the level of security your password provides. The probability of generating any specific password can be calculated as:

   $P(\text{Specifipassword}) = (1\text{noofpossiblecharacters})$

5. Let's calculate the probability for a basic 12-character password using only lowercase letters, which amounts to 26 possible characters:

   $P(\text{Specifipassword}) = (261)12 \approx 1.7665 \times 10-17$

6. This extremely low probability makes it challenging for an attacker to guess the password.

Following table shows the probabilities for passwords of varying lengths and character type selections.

Password Length	Uppercase	Lowercase	Digits	Special Characters	Probability
8	Yes	Yes	Yes	No	2.183 × 10^-15
10	Yes	Yes	Yes	Yes	3.656 × 10^-22
12	No	Yes	Yes	Yes	1.225 × 10^-27
14	Yes	Yes	No	No	2.833 × 10^-34

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computerwith basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Turbo C Compiler(optional)	

VIII. Precautions to be followed

1.Handle Computer System with care

2.Be caution while performing files related operations in computer System.

IX. Procedure

- **Step 1** − Start
- **Step 2** − The length of an ideal password should be at least eight characters.
- **Step 3** − Must contain at least a digit character.
- **Step 4** − There should be at least one lowercase character. [Example: a,b,c.....,z]
- **Step 5** − There should be at least one uppercase character. [Example: A,B,C.....,Z]
- **Step 6** − It should contain at least one special character. [Example: !@#$ %^&*()-+]
- **Step 7** − End

X. Conclusion

……

……

XI. Practical Related Questions

1. Write a utility using C/Shell programming to create strong password authentication follow the instructions while writing utility
   a. Minimum Length of password - 8 characters,
   b. Password should include digits,
   c. Password should include lower case and upper case letters
   d. Password should include special characters #, %, &, @
2. Explain Brute Force Attack
3. List various Password Attacks and explain any one.

Space for answer

……

……

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1.https://esymith.hashnode.dev/creating-strong-and-versatile-passwords-with-c-programming
2. https://www.geeksforgeeks.org/create-a-password-generator-using-shell-scripting/

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 5 *i.Write a C program to implement caesar cipher technique to perform encryption and decryption of text

I. Practical Significance

Data encryption is important because it helps protect people's privacy, and secures data from attackers and other cyber security threats. The Caesar cipher is a simple encryption technique used to send secret messages.

II. Industry / Employer Expected Outcome(s)

Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO3 – Apply basic encryption / decryption techniques for given text.

IV. Laboratory Learning Outcome(s)

LLO 5.1 Implement Caesar cipher encryption technique.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Cipher text is encrypted text transformed from plaintext using an encryption algorithm. Cipher text can't be read until it has been converted into plaintext (decrypted) with a key. The decryption cipher is an algorithm that transforms the cipher text back into plaintext.

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computerwith basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Turbo C Compiler(optional)	

VIII. Precautions to be followed

1.Handle Computer System with care

2.Be caution while performing files related operations in computer System.

IX. Procedure

Algorithm for Caesar Cipher:

1. Choose a shift value between 1 and 25.
2. Write down the alphabet in order from A to Z.
3. Create a new alphabet by shifting each letter of the original alphabet by the shift value. For example, if the shift value is 3, the new alphabet would be:
4. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
   D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
5. Replace each letter of the message with the corresponding letter from the new alphabet. For example, if the shift value is 3, the word "hello" would become "khoor".
6. To decrypt the message, shift each letter back by the same amount. For example, if the shift value is 3, the encrypted message "khoor" would become "hello".

X. Conclusion

……

……

XI. Practical Related Questions

1. Write a C program to implement caesar cipher technique to perform encryption and decryption of text
2. Differentiate between Substitution Cipher and Transposition Cipher.
3. Consider plain text "computer security" and convert given plain into cipher text?
4. Consider plain text "Network information security" encrypt it help of Caesar cipher?

Space for answer

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://www.javatpoint.com/caesar-cipher-technique
2. https://codedamn.com/news/cryptography/caesar-cipher-introduction

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 5 ii. Apply Caesar cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)

I. Practical Significance

Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.

II. Industry / Employer Expected Outcome(s)

Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO3 – Apply basic encryption / decryption techniques for given text.

IV. Laboratory Learning Outcome(s)

LLO 5.1 Implement Caesar cipher encryption technique.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

The process of transforming information into nonhuman readable form is called encryption. The process of reversing encryption is called **decryption**. Decryption is done using a **secret key** which is only known to the legitimate recipients of the information. The key is used to decrypt the hidden messages. This makes the communication secure because even if the attacker manages to get the information, it will not make sense to them. The encrypted information is known as a **cipher.**

Cryptool-

- A freeware program with graphical user interface (GUI).
- A tool for applying and analyzing cryptographic algorithms.
- With extensive online help, it's understandable without deep crypto knowledge.
- Contains nearly all state-of-the-art crypto algorithms.
- "Playful" introduction to modern and classical cryptography.
- Not a "hacker" tool.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Open source-crytool 1	

VIII. Precautions to be followed

1.Handle Computer System with care

2.Be caution while performing files related operations in computer System.

IX. Procedure

Open-source tool Cryptool 1–

CrypTool aims at making people understand network security threats and working of cryptology. It includes asymmetric ciphers like RSA, elliptic curve cryptography. CrypTool1 (CT1) experiments with different algorithms and runs on Windows. It was developed in C++ language.

Download cryptool 1 from https://www.cryptool.org/en/ct1/downloads/

Follow the following steps for **Encryption and Decryption of Caesar Cipher**

Demonstration of Caesar Encryption using CrypTool

In this CrypTool demonstration, we will use Caesar, one of the oldest encryption algorithms.

Encryption

1. Open the Cryptool UI and the document that needs to be encrypted.

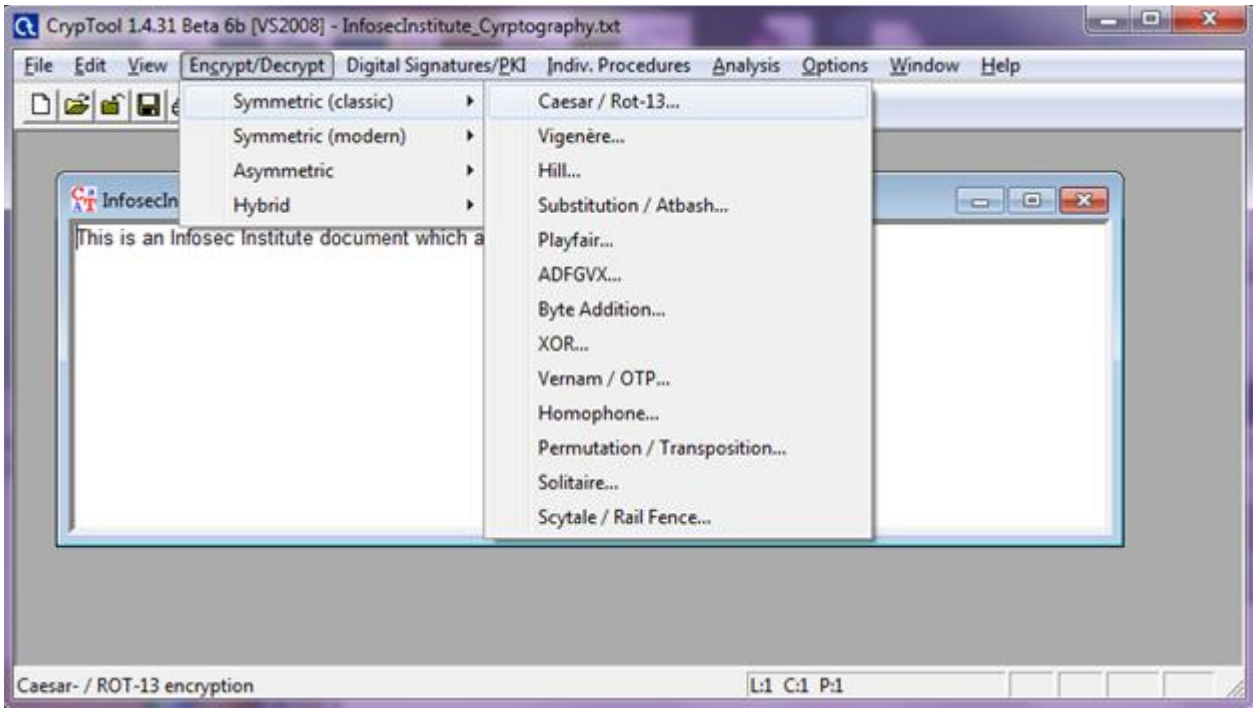


Fig. No.5.2.1

2. Click Encrypt/Decrypt > Symmetric (classic) > Caesar

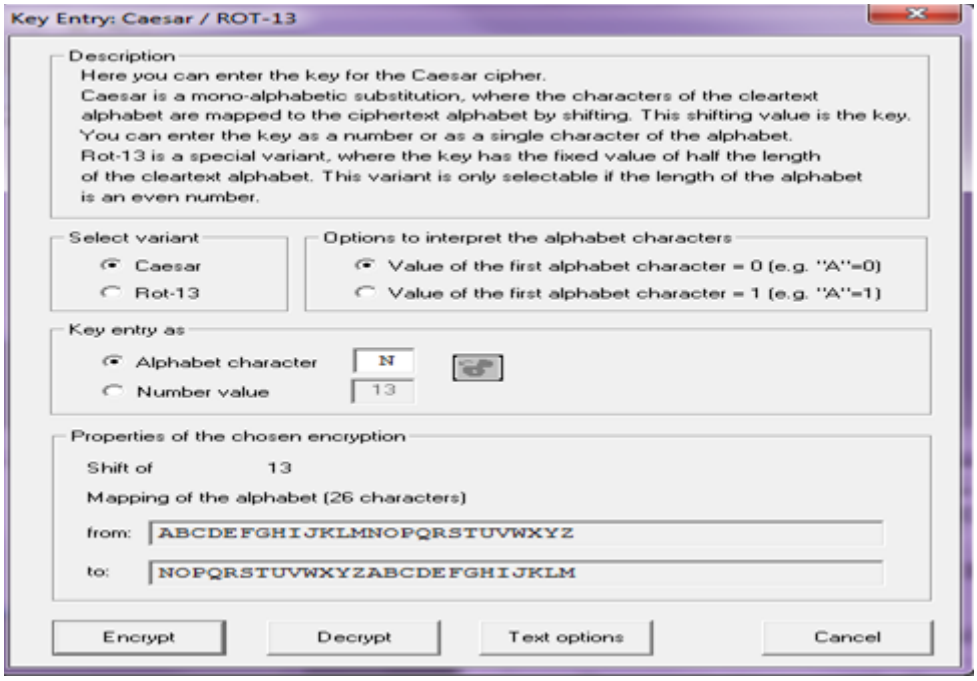


Fig. No. 5.2.2

3. Select Caesar mode and the "alphabet character" is "N." That means that the text will have characters replaced starting with N. So A >N, B>M, and so on. Click on "encrypt."

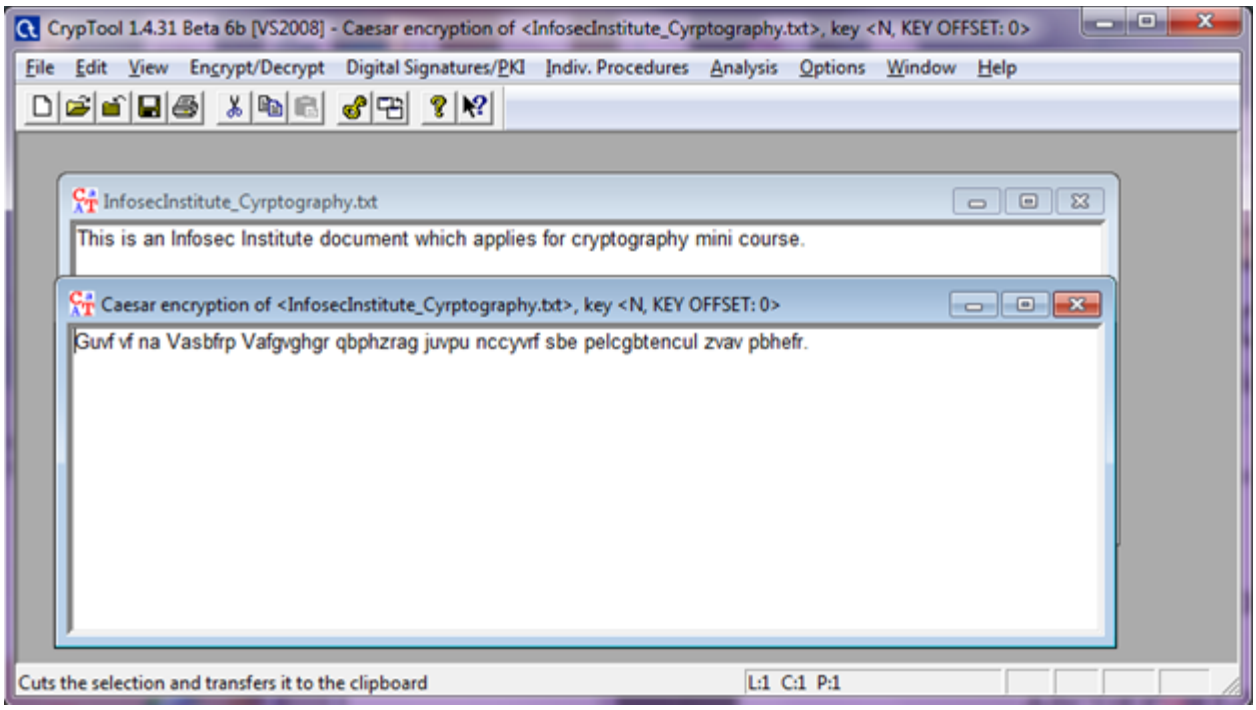


Fig. No. 5.2.3

The document is encrypted as per the configured policy. This is a very basic example of how symmetric encryption works.

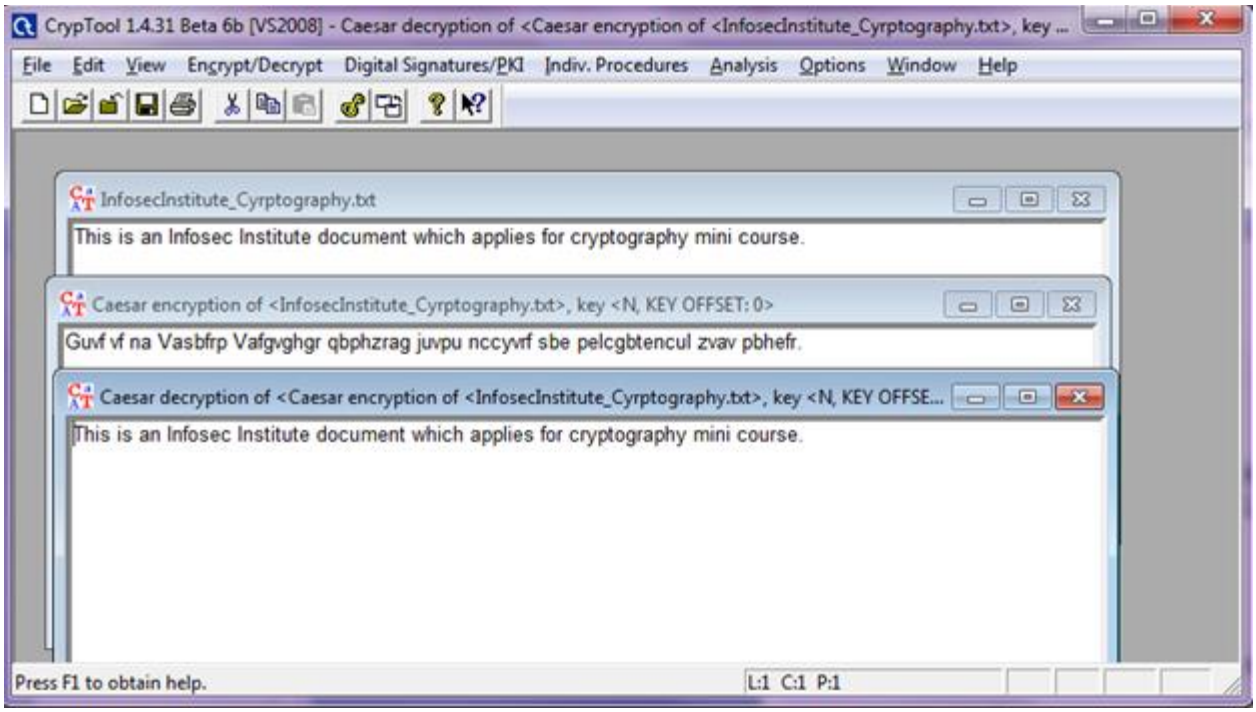


Fig. No. 5.2.4

Decryption process

Perform the following steps to decrypt the encrypted document.

1. Open the encrypted document, and click on "Encrypt.Decrypt" >Symmetric >Caesar.
2. Enter "N" as the alphabet character. This is the shared secret that both parties must know in order to encrypt and decrypt.
3. Click on decrypt.

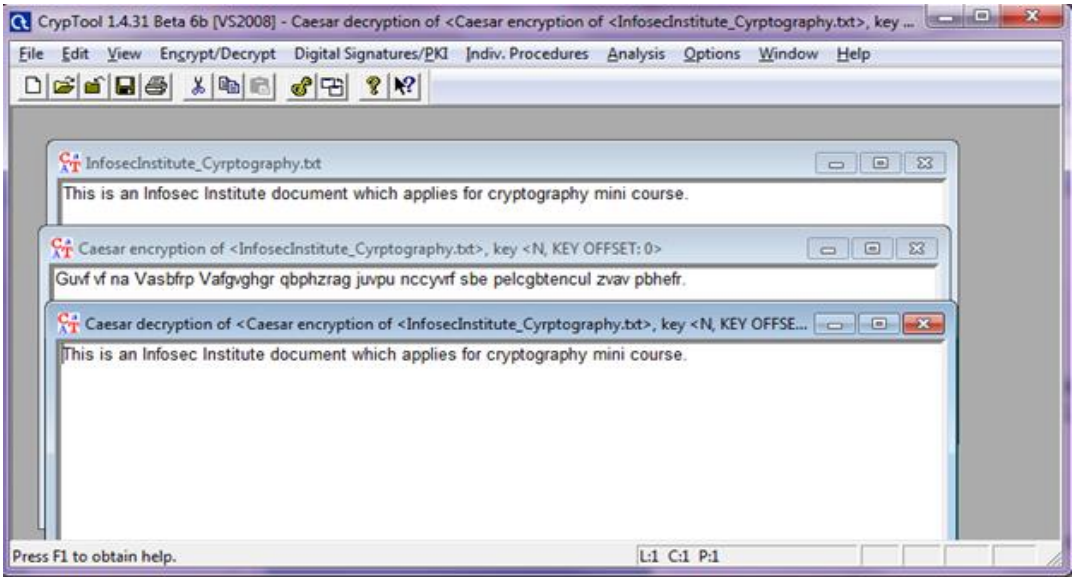


Fig. No. 5.2.5

X. Conclusion

……

……

XI. Practical Related Questions

1. Enlist any 5 Web-based cryptanalysis tools.
2. A plaintext was encrypted with a Caesar cipher with a shift of 7 (A maps to H). The resulting cipher text is:
   Kvu'aqbknl h ivvr if pazjvcly
3. What was the original plaintext?
4. Write your name and encrypt using crptool and attach screenshot of encrypted file.

Space for answer

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://www.c-sharpcorner.com/article/encryption-decryption-using-cryptool/
2. https://www.infosecinstitute.com/resources/cryptography/cryptanalysis-tools/

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 6 i.Implement Vernam cipher encryption technique to perform encryption of text using C programming language

I. Practical Significance

Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.Vernam Cipher is a cryptographic algorithm to encrypt and decrypt an alphabetic text.

II. Industry / Employer Expected Outcome(s)

Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO3 – Apply basic encryption / decryption techniques for given text.

IV. Laboratory Learning Outcome(s)

LLO 6.1 Implement Vernamcipher encryption technique.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitution techniques for converting plain text into cipher text. Instead of a single key, each plain text character is encrypted using its own key. This means that there is no way that the cipher text can be deciphered without the key.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computerwith basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Turbo C Compiler	

VIII. Precautions to be followed

1.Handle Computer System with care

2.Be caution while performing files related operations in computer System.

IX. Procedure

Vernam Cipher –

The **Vernam cipher** is a substitution cipher where each plain text character is encrypted using its own key. To encrypt the message, each character of the plain text and the key will need to be converted to a numeric code. We can use standard ASCII codes as numeric code for character.

For example, the letter 'H' is 72. This number has a binary representation of 01001000 (using 8 bits).

To use the Vernam cipher, you will need to use an XOR operation. The operation's truth table is shown below:

INPUTA	INPUTB	OUTPUTQ
0	0	0
0	1	1
1	0	1
1	1	0

To apply the Vernam cipher, each bit of the binary character code for each letter of the plain text undergoes a XOR operation with the corresponding bit of each letter of the binary character code for the corresponding character from the key stream — this creates the **cipher text**.

Encryption –

1. Obtain the 8-bit ASCII code for each letter of the plain text:
2. Obtain the 8-bit ASCII code for each letter of the key:
3. Carry out the XOR operation, applying it to each corresponding pair of bits:

In the below example, the message 'HELLO' will be encrypted using the key 'PLUTO'. The letters will be converted into 8-bit ASCII codes.

Plain text

H	01001000
E	01000101
L	01001100
L	01001100
O	01001111

Key

P	01010000
L	01001100
U	01010101
T	01010100
O	01001111

Plain text	01001000	01000101	01001100	01001100	01001111
Key	01010000	01001100	01010101	01010100	01001111
Cipher text in binary	00011000	00001001	00011001	00011000	00000000

Cipher text:
00011000, 00001001, 00011001, 00011000, 00000000
the cipher text could be displayed in denary as:
24, 9, 25, 24, 0
or in hexadecimal (hex) as:
18, 9, 19, 18, 0

Decryption-

1. Obtain the binary code for each character of the cipher text
2. Obtain the 8-bit ASCII code for each letter of the key:
3. Carry out the XOR operation, applying it to each corresponding pair of bits:

Cipher text

24	00011000
9	00001001
25	00011001
24	00011000
0	00000000

Key

P	01010000
L	01001100
U	01010101
T	01010100
O	01001111

Cipher text	00011000	00001001	00011001	00011000	00000000
Key	01010000	01001100	01010101	01010100	01001111
Plain text	01001000	01000101	01001100	01001100	01001111
Plain text converted back into characters	H	E	L	L	O

X. Conclusion

……

……

XI. Practical Related Questions

1. Write a C program to implement Vernam cipher encryption and decryption technique.
2. Given Plain text: 'IF' ,Key: 10100. Convert the given plain text into cipher text using Vernam Cipher.
3. Using the Vernam cipher, encrypt and decrypt the word "HELLO" using the Key value "DGHBC"

4. List Advantages and disadvantages of Vernam CipherTechnique.

Space for answer

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://japp.io/cryptography/vernam-cipher-algorithm-program-in-c-c/
2https://www.geeksforgeeks.org/vernam-cipher-in-cryptography/

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 6 ii.ApplyVernam cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)

I. Practical Significance

Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.Vernam Cipher is a cryptographic algorithm to encrypt and decrypt an alphabetic text.

II. Industry / Employer Expected Outcome(s)

Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO3 – Apply basic encryption / decryption techniques for given text.

IV. Laboratory Learning Outcome(s)

LLO 6.1 Implement Vernam cipher encryption technique.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitution techniques for converting plain text into cipher text. Instead of a single key, each plain text character is encrypted using its own key. This means that there is no way that the cipher text can be deciphered without the key.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computerwith basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Cryptool 1	

VIII. Precautions to be followed

1.Handle Computer System with care

2.Be caution while performing files related operations in computer System.

IX. Procedure

Vernam Cipher –

Demonstration of **Vernam Cipher**Encryption using CrypTool

In this CrypTool demonstration, we will use Caesar, one of the oldest encryption algorithms.

Encryption

1. Open the Cryptool UI and the document that needs to be encrypted.

2. Click Encrypt/Decrypt > Symmetric (classic) >XOR

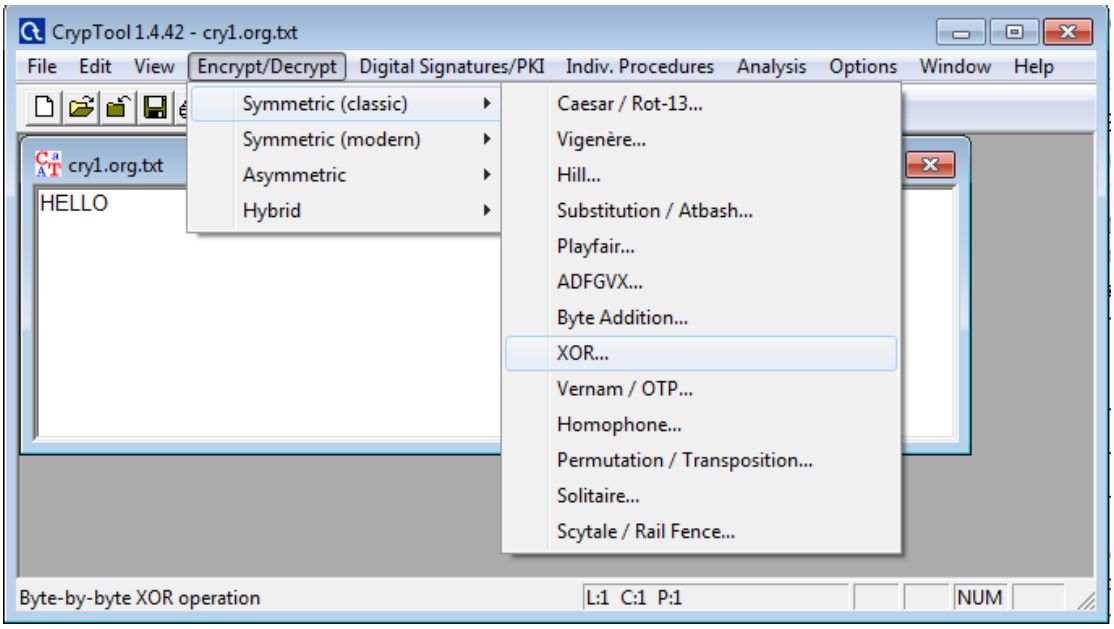


Fig. No. 6.2.1

3. Enter key value in Hex format which of same length as original text.

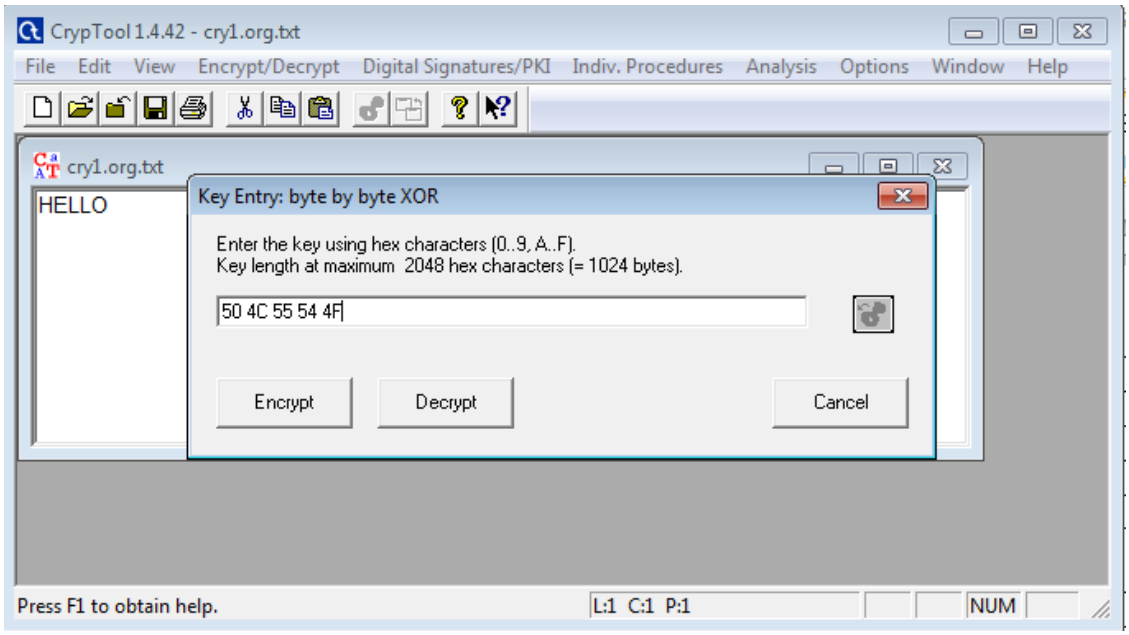


Fig. No. 6.2.2

5. Click on "encrypt."

Decryption process

Perform the following steps to decrypt the encrypted document.

1. Open the encrypted document, and click on "Encrypt.Decrypt" >Symmetric(classic)> XOR.
2. Enter Key value in Hexadecimal form
3. Click on decrypt.

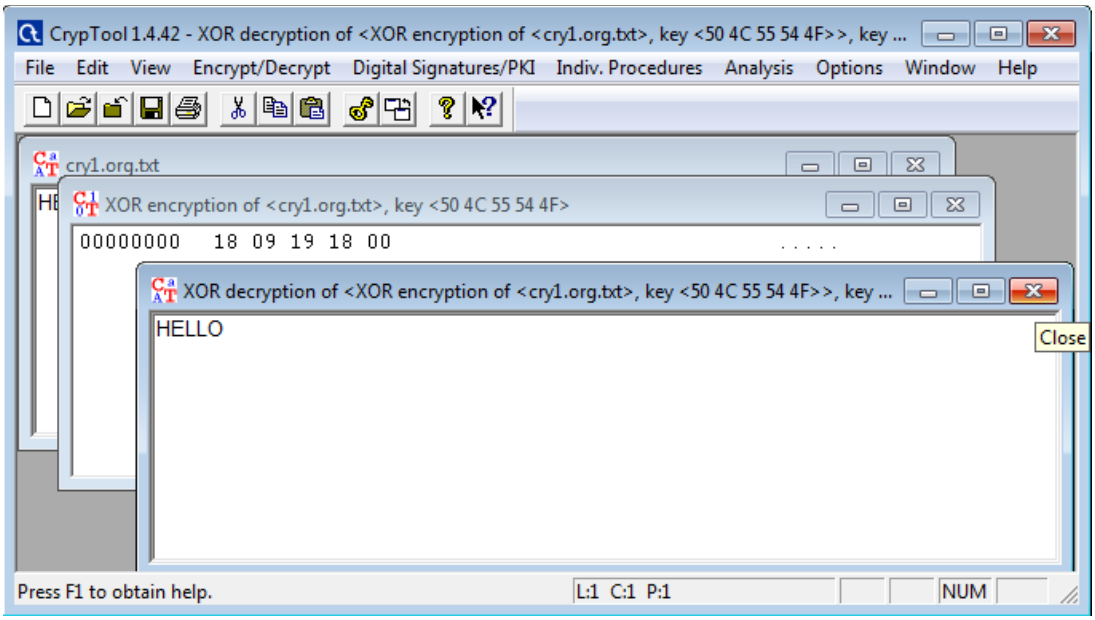


Fig. No. 6.2.3

X. Conclusion

.....

.....

XI. Practical Related Questions

1. Use online Cryptool from https://legacy.cryptool.org/de/cto/vernam. Try to encrypt Text HELLO using key PLUTO. Write Encrypted Text.
2. Encrypt the Message = HELLO with Key = MONEY. Write Encrypted text.

Space for answer

.....

.....

.....

.....

.....

XII. References/Suggestions for further reading

1. https://japp.io/cryptography/vernam-cipher-algorithm-program-in-c-c/
2. https://www.geeksforgeeks.org/vernam-cipher-in-cryptography/

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 7 * Implement rail fence encryption technique to perform encryption of text using C programming language

I. Practical Significance

Since the importance of privacy and security has grown, several cryptographic methods and techniques have been developed to protect our sensitive data.

II. Industry / Employer Expected Outcome(s)

Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO3 – Apply basic encryption / decryption techniques for given text.

IV. Laboratory Learning Outcome(s)

LLO 7.1 Implement rail fence encryption technique.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

In classical cryptography techniques, namely substitution technique, the original message's characters are replaced with different characters, numbers, or symbols. The Caesar cipher is an example of the substitution technique. Conversely, the transposition technique involves rearranging the plaintext through permutation.

Rail fence cipher falls into the category of transposition techniques where we change the position of each plaintext letter. The term "Rail-Fence" is attributed to the resemblance of this technique to a cluster of zigzagging rails.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Turbo C Compiler	

VIII. Precautions to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System.

IX. Procedure

Rail fence cipher technique:

Encryption Process–

The rail fence cipher's encryption process requires choosing the number of rails, writing the message diagonally in a zigzag pattern determined by the selected number of rails, and then combining the characters along each rail from left to right to obtain the encrypted message.

First, consider "RAILFENCE" as a plain text. Next, let's take the number of rails or fences as three, which can also be referred to as a key. The key will determine the height of the zigzag pattern. Subsequently, we can write the message diagonally in a zigzag pattern from left to right:

R				F				E
	A		L		E		C	
		I				N		

Fig. No. 7.1

Lastly, we'll combine individual rows to generate the cipher text, which in this case will be "RFEALECIN".

The encryption algorithm involves two broad steps:

1. Writing the message on a 2D grid where each row is called a "rail". The message "zig-zags" between the top and bottom rails, one message character per column. The height (number of rows) is the "key".
2. The cipher text is created by reading the characters of the grid in a top-to-bottom-left-to-right sequence. Where the classical rail fence cipher has a \key" which is a single integer, A, your algorithm will use two integers A, and B with A > B and B > 1; alternating between them when writing out the message on the fence rails. This algorithm reduces down to the classical rail fence cipher if A = B.

X. Conclusion

……..…

……..…

XI. Practical Related Questions

1. Write a C Program to implement Rail Fence Encryption and Decryption.
2. The encoded message is "CYTGAHITEROWIIGROVNCDSRPORPYSHATFRTNOSLIGOE" Using key =3 decode the message.
3. What is the alternative name given to Rail fence cipher?
   a) random cipher b) matrix cipher c) zigzag cipher d) columnar cipher
4. Rail fence cipher is an example of _____

a) mono-alphabetic cipher b) poly-alphabetic cipher c) transposition cipher
d) additive cipher

5. Encryption in Rail fence cipher is done using _____
a) by arranging the letters in a zigzag fashion in a table b) by randomly arranging letters
c) by arranging letters in vigenere table d) by swapping adjacent letters

Space for answer

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://www.baeldung.com/cs/cryptography-rail-fence-cipher
2. https://www.geeksforgeeks.org/rail-fence-cipher-encryption-decryption/
3.https://medium.com/@amanpalrayat/implementation-of-rail-fence-algorithm-in-c-language-2640ffcda4b
4.https://www.cprograms4future.com/p/encryption-rail-fence-cipher.html#google_vignette

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No.8: Implement simple Columnar Transposition encryption technique to perform encryption of text using C programming language

I. Practical Significance

Columnar Transposition involves writing the plaintext out in rows, and then reading the cipher text off in columns. In its simplest form, it is the Route **Cipher** where the route is to read down each **column** in order.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO3 - Apply basic encryption / decryption techniques for a given text.

IV. Laboratory Learning Outcome(s)

LLO 8.1 Implement simple columnar transposition technique

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

The columnar transposition cipher is a fairly simple, easy to implement cipher. It is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the cipher text.

Although weak on its own, it can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on its own. **Example:**

The key for the columnar transposition cipher is a keyword e.g. GERMAN. The row length that is used is the same as the length of the keyword. To encrypt a piece of text e.g. Defend the east wall of the castle

We write it out in a special way in a number of rows (the keyword here is GERMAN):

G E R M A N
d e f e n d
t h e e a s
t w a l l o
f t h e c a
s t l e x x

In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.

A E G M N R
n e d e d f
a h t e s e
l w t l o a
c t f e a h
x t s e x l

The ciphertext is read off along the columns:

nalcxehwttdttfseeleedsoaxfeahl

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Turbo C Compiler	

VIII. Precaution to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System

IX. Procedure

Algorithm for simple columnar encryption technique

The simple columnar transposition technique is a classical encryption method that rearranges the characters of the plaintext according to a specified keyword. Here's a step-by-step outline of the algorithm:

1. **Choose a keyword:** The length of the keyword determines the number of columns in the transposition grid.
2. **Create the grid**: Write the plaintext message in rows under the columns labeled by the keyword's letters. If the plaintext does not fill the grid completely, pad the remaining cells with null characters or spaces.
3. **Sort the keyword alphabetically:** This will determine the order in which the columns are read.
4. **Read columns in the new order:** Read the columns in the order determined by the alphabetical positions of the keyword's letters to create the cipher text.

X. Conclusion

……..…

……

……..

XI. Practical Related Questions

1. Write a C Program to implement simple columnar encryption technique.
2. List types of cryptographic algorithm?
3. Comparison of substitution cipher and transposition cipher?

Space for answer

……..…

……

……..

……..

……

……

……

XII. References/Suggestions for further reading

1. https://www.w3school.com/columnar-transposition-cipher
2. https://www.reasearch .ijcaonline.org

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No.9: Create and verify Hash Code for given message using any Open-source tool. (Example- Cryptool)

I. Practical Significance

The contents of a **file** are processed through a cryptographic algorithm, and a unique numerical **value** – the **hash value** - is produced that identifies the contents of the **file**. If the contents are modified in any way, the **value** of the **hash** will also change significantly.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO3 - Apply basic encryption / decryption techniques for a given text.

IV. Laboratory Learning Outcome(s)

LLO 9.1 Generate Hash Code

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

A **cryptographic hash function** (**CHF**) is a hash function that is suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size (often called the "message") to a bit string of a fixed size (the "hash value", "hash", or "message digest") and is a one-way function, that is, a function which is practically infeasible to invert Ideally, the only way to find a message that produces a given hash is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes. Cryptographic hash functions are a basic tool of modern cryptography. The ideal cryptographic hash function has the following main properties:

- it is deterministic, meaning that the same message always results in the same hash
- it is quick to compute the hash value for any given message
- it is infeasible to generate a message that yields a given hash value
- it is infeasible to find two different messages with the same hash value
- a small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value (avalanche effect).

Cryptographic hash functions have many information-security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information-security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for more general functions with rather different properties and purposes.

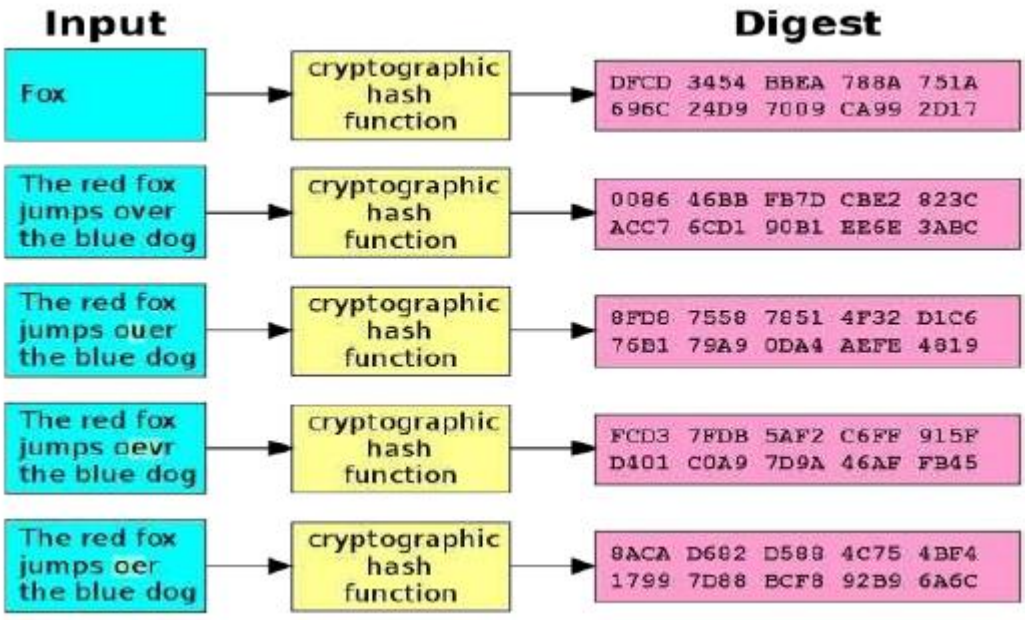


Fig. No. 9.1

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Cryptool 1	01

VIII. Precaution to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System

IX. Procedure

Here is a step-by-step guide to generate a hash code:

1. **Open Cryptool 1:** Launch the Cryptool 1 application on your computer.
2. **Load or Enter Data:** Either type in the data you want to hash directly into Cryptool or load a file containing the data.

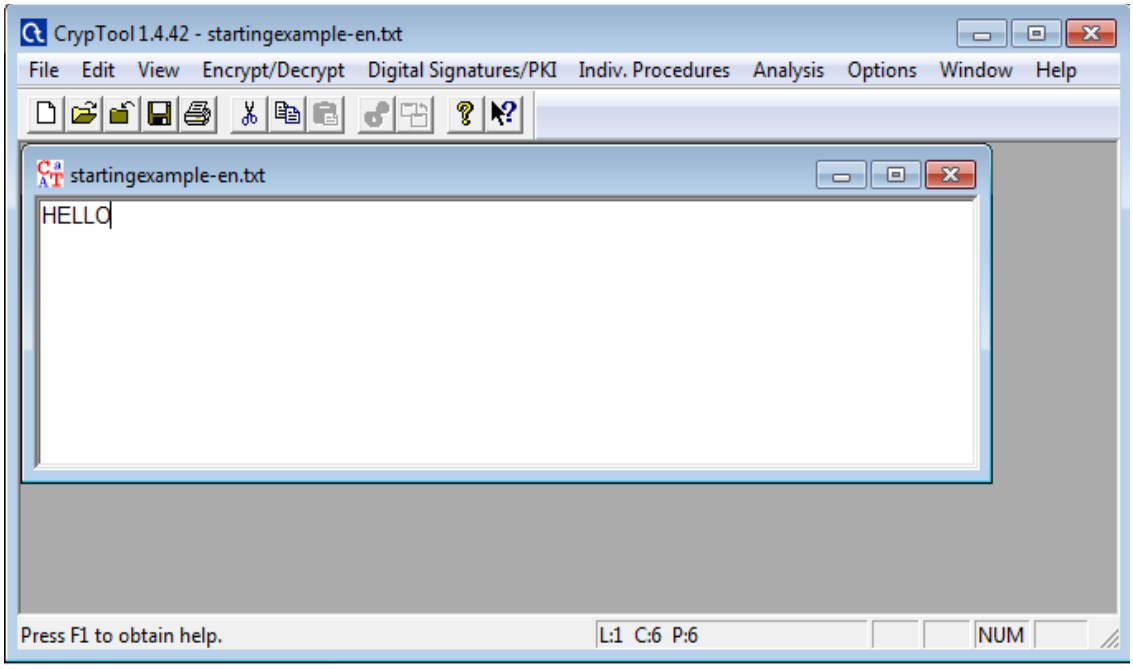


Fig. No. 9.2

3. **Select Hash Function:**
   - Go to the "Individual Procedures" menu.
   - Select "Hash Values".
   - Choose the desired hash function (e.g., MD5, SHA-1, SHA-256).

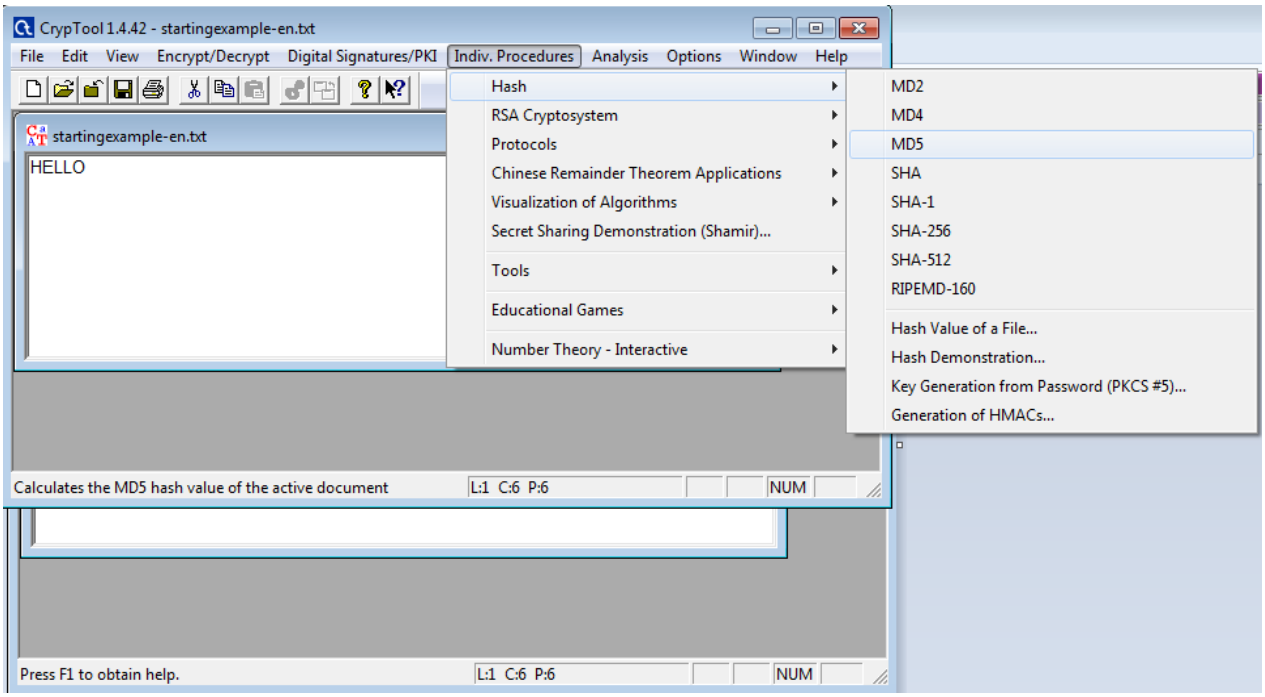


Fig. No. 9.3

4. **Generate Hash:**
   - After selecting the hash function, Cryptool will compute the hash value for your data.
   - The resulting hash code will be displayed in a new window or pane within the Cryptool interface.

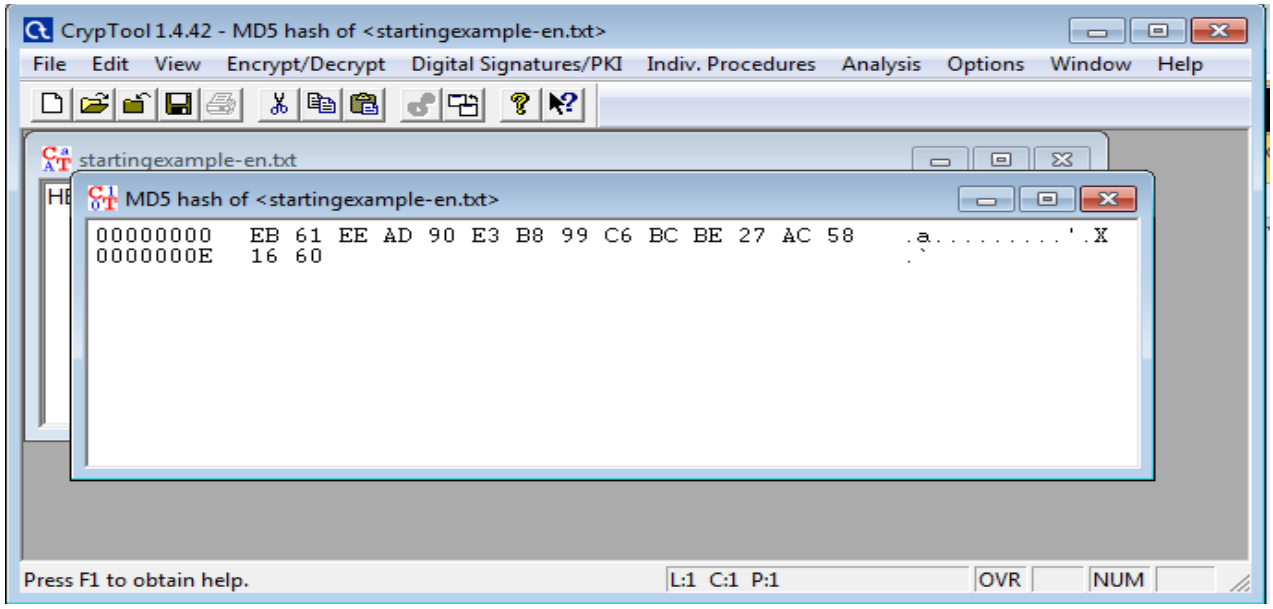


Fig. No. 9.4

5. **Copy or Save Hash:** You can copy the hash code directly from the window or save it to a file if needed.

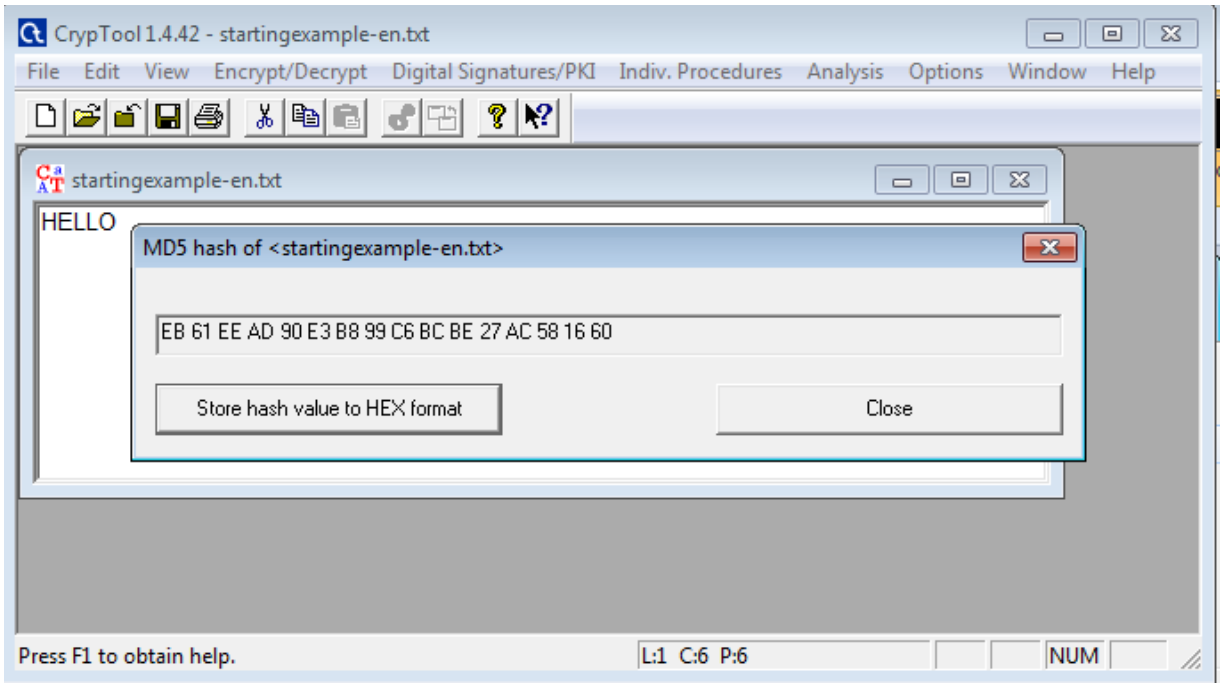


Fig. No. 9.5

X. Conclusion

……

……

……

XI. Practical Related Questions

1. What is digital signature?
2. Diagram of digital signature?

Space for answer

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://www.w3school.com/hashcode
2. https://www.simplilearn.com/tutorials/cyber-security-tutorial/md5-algorithm

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time	
	Total 25	
	Dated Signature of Course Teacher	

Practical No.10: i. Write a C program to implement Diffie-Hellman key exchange algorithm to perform encryption of text

I. Practical Significance

Diffie-hellman key exchange is a method of digital encryption that securely exchanges cryptographic keys between two parties over a public channel without their conversation being transmitted over the internet, the two parties use symmetric cryptography to encrypt ad decrypt their messages.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO4 - Apply various encryption algorithms used for information security.

IV. Laboratory Learning Outcome(s)

LLO 10.1 Implement Diffie-Hellman key exchange encryption technique

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Diffie-Hellman key exchange raises numbers to a selected power to produce decryption keys. The components of the keys are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming. The method doesn't share information during the key exchange. The two parties have no prior knowledge of each other, but the two parties create a key together.

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

- For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.
- P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

Step-by-Step explanation is as follows:

Alice	**Bob**
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated =	Key generated =
Exchange of generated keys takes place	

Key received = y	Key received = x
Generated Secret Key =	Generated Secret Key =
Algebraically, it can be shown that	
Users now have a symmetric secret key to encrypt	

Example:

Step 1: Alice and Bob get public numbers P = 23, G = 9

Step 2: Alice selected a private key a = 4 and Bob selected a private key b = 3

Step 3: Alice and Bob compute public values :

Alice: x =(9^4 mod 23) = (6561 mod 23) = 6

Bob: y = (9^3 mod 23) = (729 mod 23) = 16

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key y =16 and

Bob receives public key x = 6

Step 6: Alice and Bob compute symmetric keys :

Alice: ka = y^a mod p = 65536 mod 23 = 9

Bob: kb = x^b mod p = 216 mod 23 = 9

Step 7: 9 is the shared secret.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Turbo C Compiler	

VIII. Precaution to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System

IX. Conclusion

……..…

……

…….

X. Practical Related Questions

1. Write a C Program to implement Diffie-Hellman key exchange algorithm to perform encryption of text.
2. Write the applications and limitations of Diffie-hellman algorithm.
3. Comparison of Diffie-hellman and RSA.

Space for answer

……

……

……

……

XI. References/Suggestions for further reading

1. https://www.geeksforgeeks.org/implement-diffie-hellman-key-exchange
2. https://www.programmnigoss.com/2015/11/diffie-hellman-key-exchange-algorithm.html

XII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No.10: ii. Use Diffie-Hellman key exchange algorithm to perform encryption and decryption of text using any open-source tool (Example - Cryptool)

I. Practical Significance

Diffie-hellman key exchange is a method of digital encryption that securely exchanges cryptographic keys between two parties over a public channel without their conversation being transmitted over the internet, the two parties use symmetric cryptography to encrypt ad decrypt their messages.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO4 - Apply various encryption algorithms used for information security.

IV. Laboratory Learning Outcome(s)

LLO 10.1 Implement Diffie-Hellman key exchange encryption technique

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

CrypTool is a popular educational software for learning about and experimenting with cryptographic algorithms. Here's how you can use CrypTool to work with the Diffie-Hellman key exchange algorithm:

Steps to Use CrypTool for Diffie-Hellman

1. Download and Install CrypTool:

- Visit the [CrypTool website](https://www.cryptool.org/en/).
- Download the version suitable for your operating system (CrypTool 1, CrypTool 2, or CrypTool Online).
- Install the software by following the installation instructions.

2. Open CrypTool:

- Launch CrypTool after installation.

3. Navigate to the Diffie-Hellman Algorithm:

- In CrypTool 1:
  - Go to the menu bar and select "Indiv. Procedures" > "Key Exchange Protocols" > "Diffie-Hellman".
- In CrypTool 2:
  - Go to the "Workspace Manager" and create a new project.
  - Drag and drop the "Diffie-Hellman Key Exchange" component from the component list into your workspace.

4. Set Up Parameters:

- You will be prompted to input the parameters for the Diffie-Hellman key exchange. These typically include:
  - Prime number (p)
  - Base (g)
- You can either use the default values provided or input your own.

5. Generate Private and Public Keys:
- Each participant (often referred to as Alice and Bob) generates their private key.
- The software will compute the corresponding public keys using the base (g) and prime (p).

6. Exchange Public Keys:
- Alice and Bob exchange their public keys. In CrypTool, this step is simulated automatically.

7. Compute the Shared Secret:
- Both Alice and Bob use the received public key and their private key to compute the shared secret.
- CrypTool will show you the steps and the final shared secret.

8. Visualization and Analysis:
- CrypTool provides a detailed visualization of the process, including intermediate steps and mathematical calculations.
- You can analyze the key exchange process and understand how the shared secret is derived.

9. Experiment and Learn:
- Change parameters, generate new keys, and repeat the process to see how different values affect the key exchange.
- Use the educational resources and explanations provided by CrypTool to deepen your understanding of the Diffie-Hellman algorithm.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Open source-crytool 1	01

VIII. Precaution to be followed

1. Handle Computer System with care.
2. Be caution while performing files related operations in computer System.

IX. Procedure

1. Go to Indiv. Procedure -> Protocols – Diffie-Hellman Demonstration.

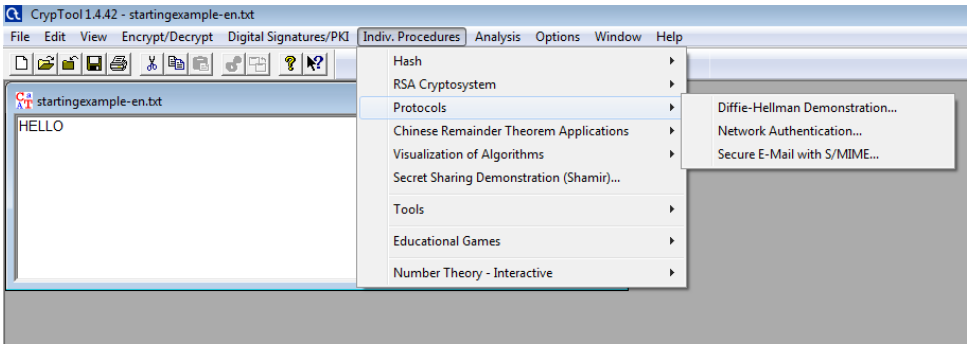


Fig. No. 10.2.1

2. Click Set public Parameters -> Set Public Parameter Dialog box will Appear -> click Ok to proceed for to generate public parameters.

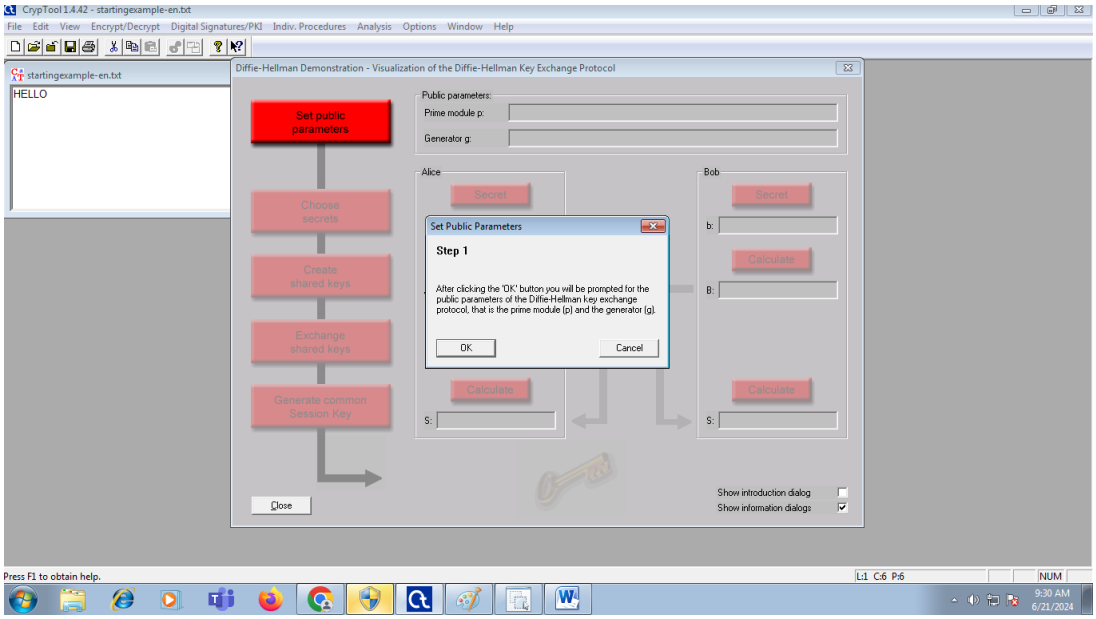


Fig. No. 10.2.2

3. Next dialog box of Generate public parameter will appear -> click on Generate Prime button.

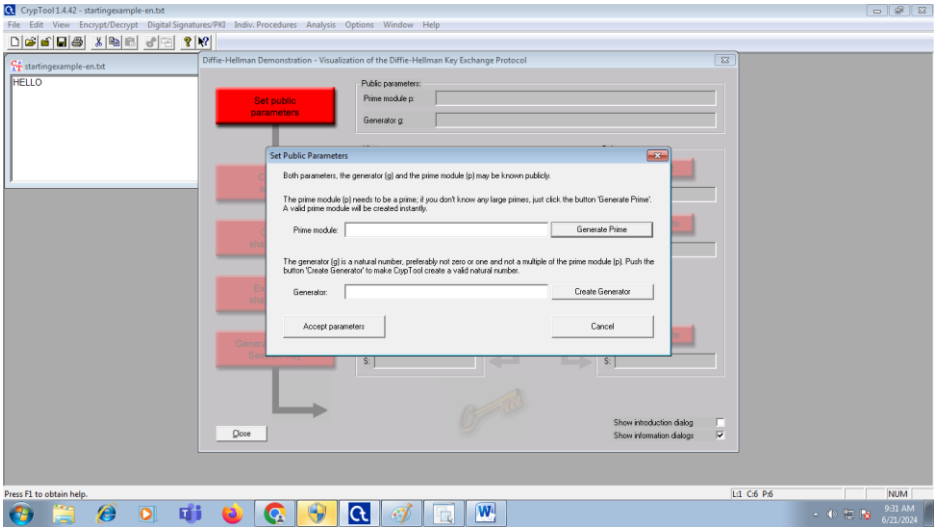


Fig. No. 10.2.3

4. Set bit length. No will be displayed in Prime -> Click on Accept Prime button.

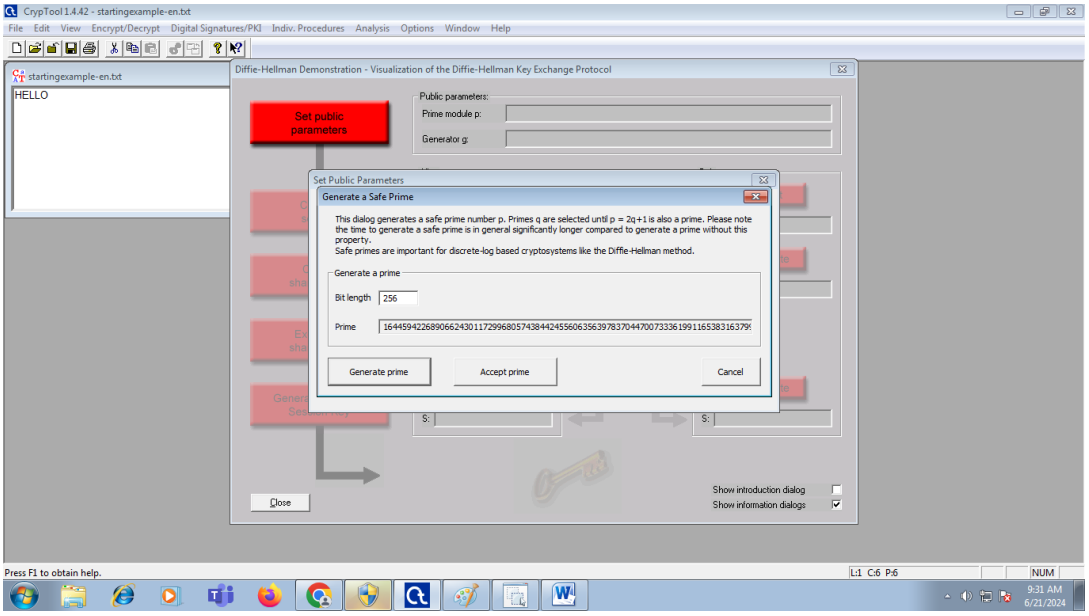


Fig. No. 10.2.4

5. Click on Create Generator. No will be displayed in Generator Field. -> Click on Accept Parameters.

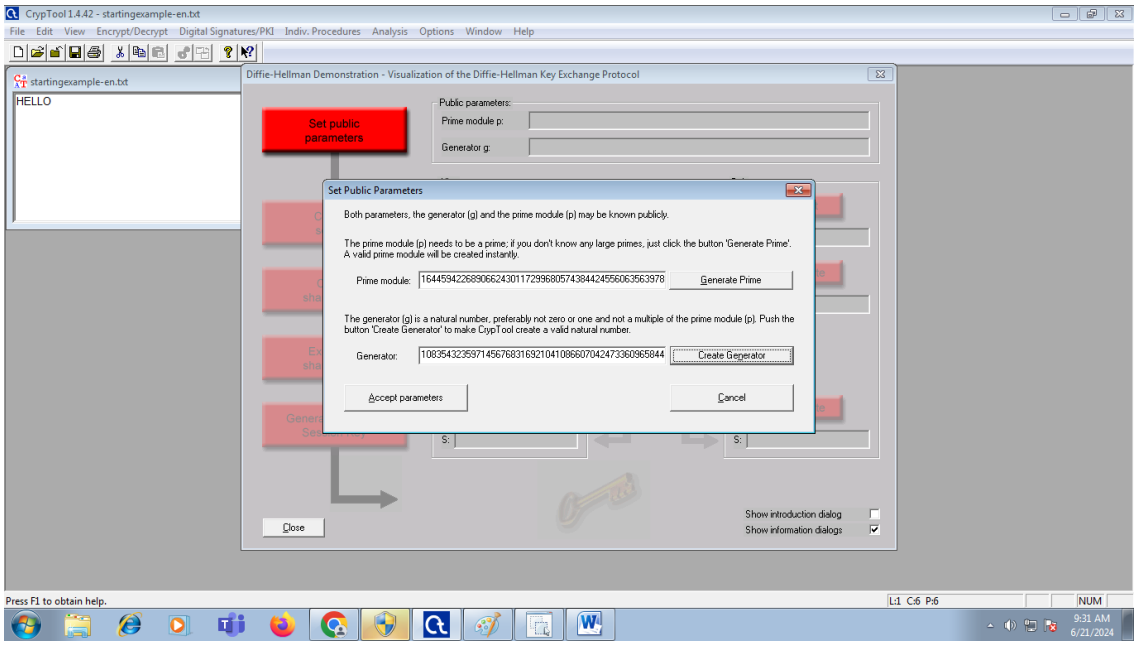


Fig. No. 10.2.5

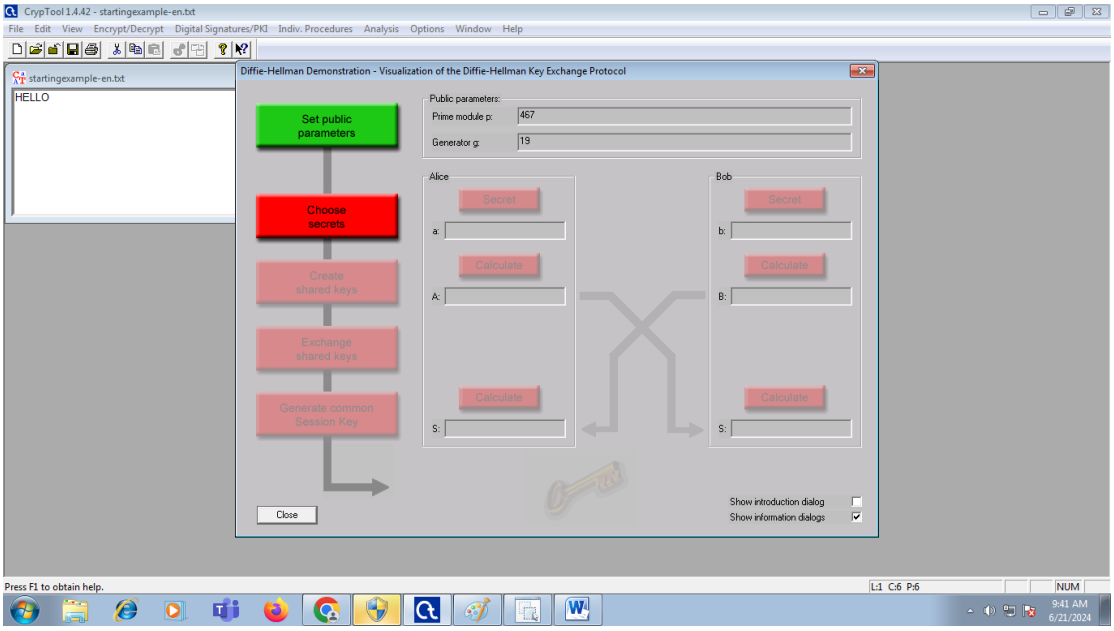


Fig. No. 10.2.6

6. On the flowchart window click on choose secretes button. Choose secrete dialog box appears Stating to choose separate secrete no for Alice and Bob -> Click OK.

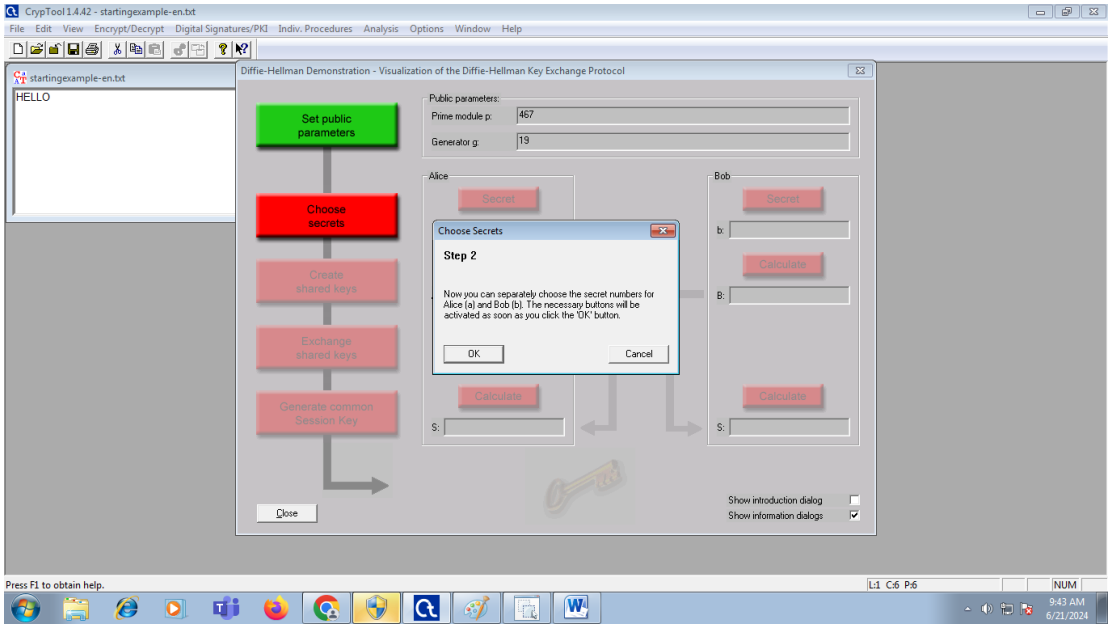


Fig. No. 10.2.7

7. Click on Secrete button of Alice -> Choose Alice's Secrete dialog box appears asking you to Generate Secrete. Click Generate Secrete and Accept Secrete.

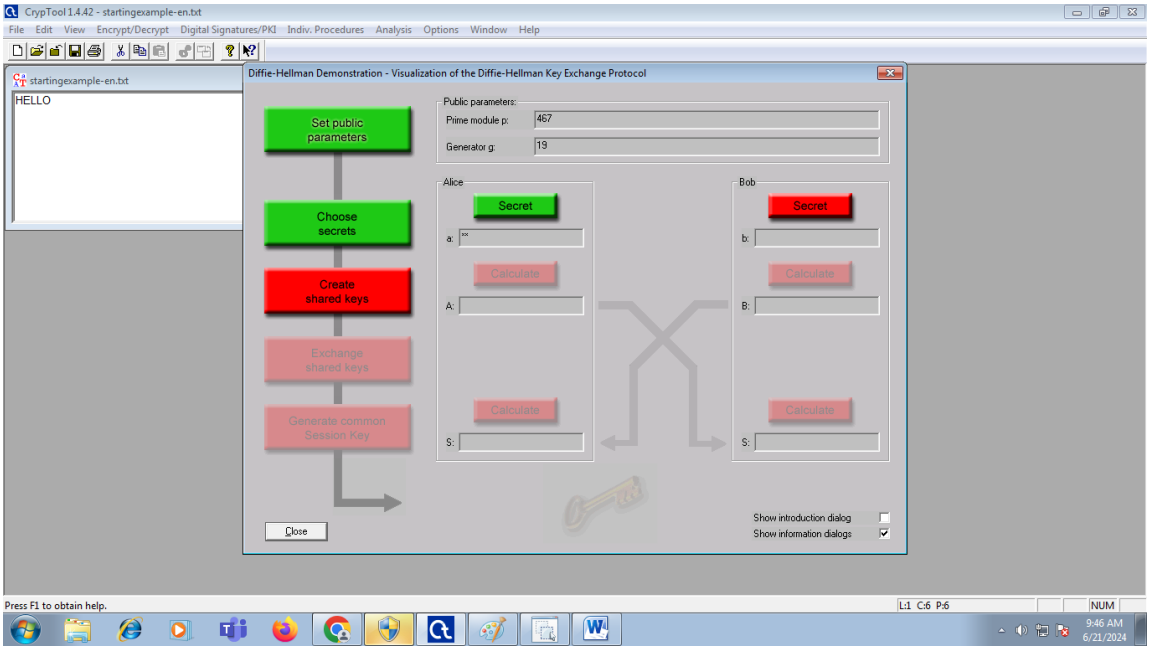


Fig. No. 10.2.8

8. Follow the same procedure for Bob's Secret Key Generation.

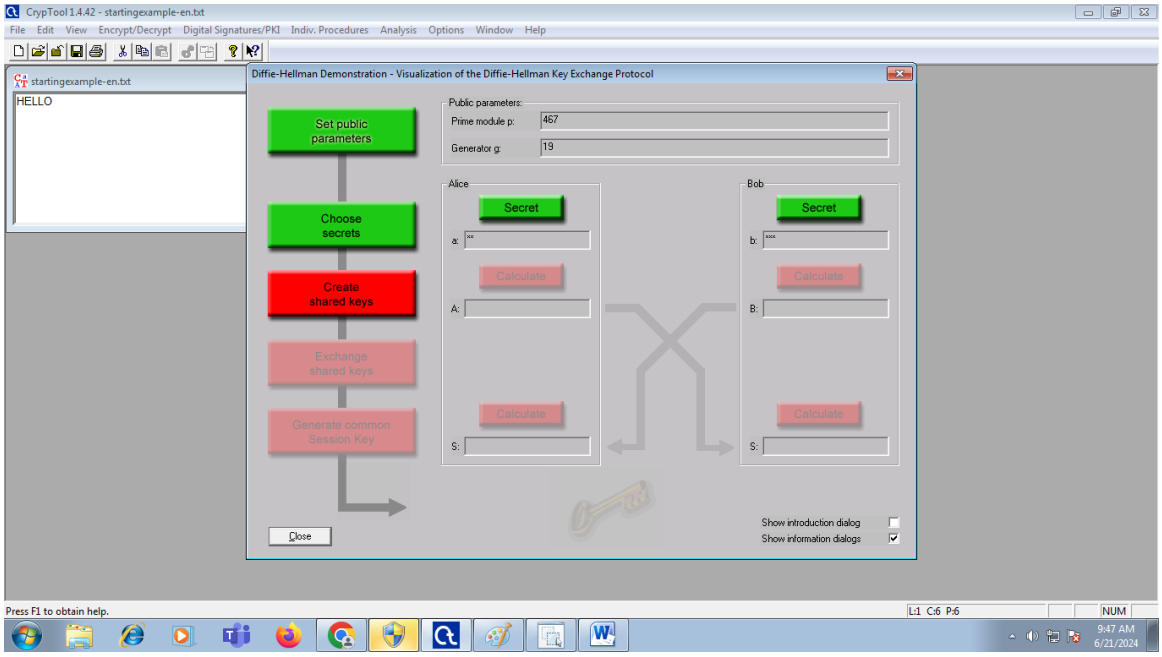


Fig. No. 10.2.9

9. Next Click on Create Shared Key. Create Shared Key dialog box appears. Click Ok.

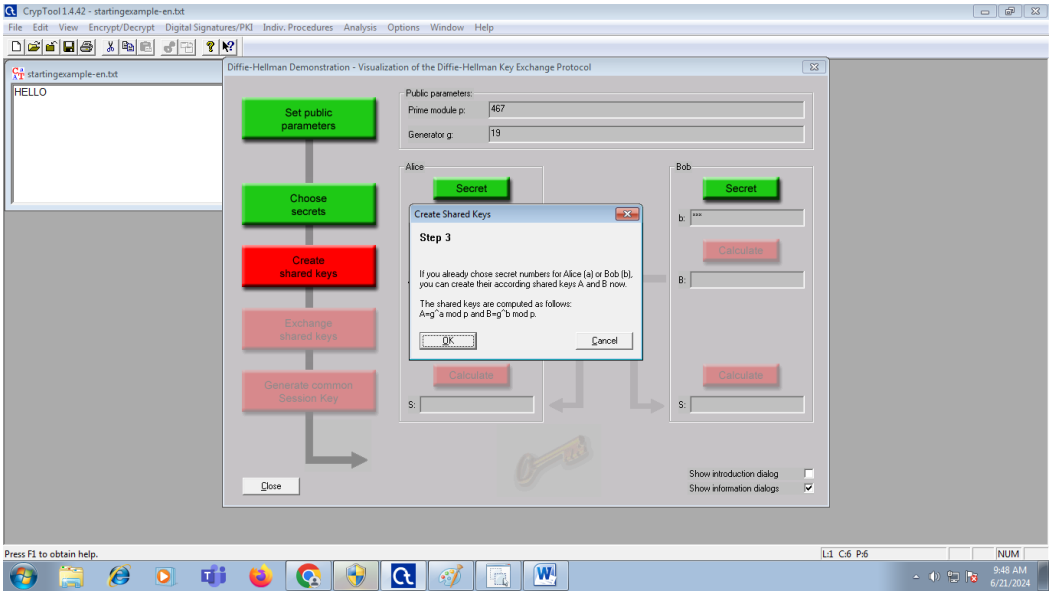


Fig. No. 10.2.10

10. Click Calculate button of Alice and Bob.

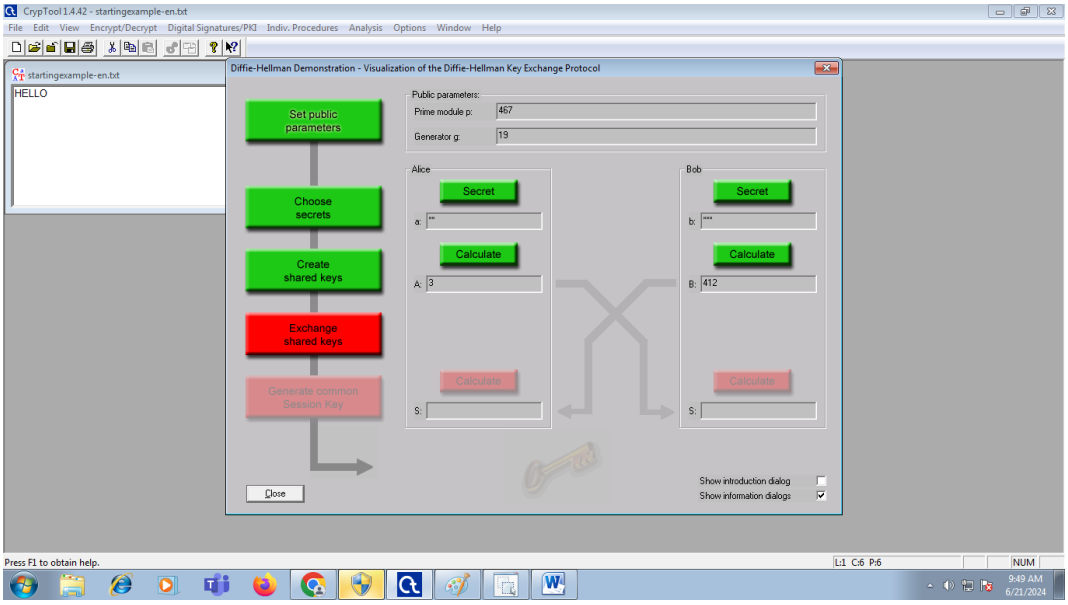


Fig. No. 10.2.11

11. Next Click Exchange shared Key Button on Flow chart window. This will prompt a dialog box stating Alice and Bob will exchange their Keys.

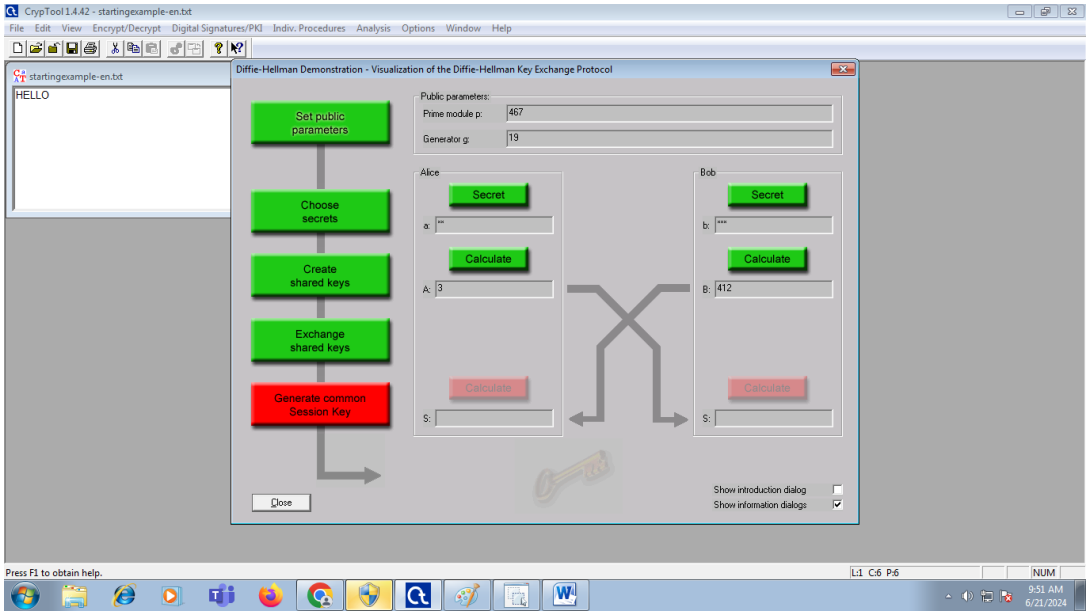


Fig. No. 10.2.12

12. Click on Generate Common Session Key Button on Flowchart window. A dialog box appears stating a common session key will be generated for Alice and Bob.

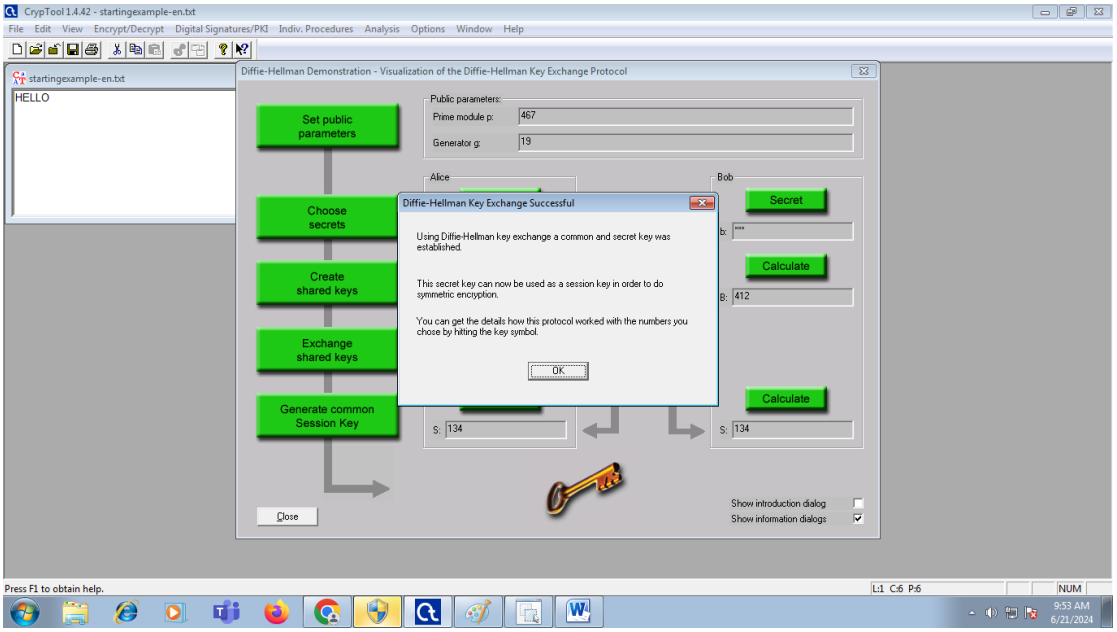


Fig. No. 10.2.13

13. Click Ok on the dialog box. -> Click on Key symbol displayed on the flowchart window.-> Summary of flow process will be displayed.

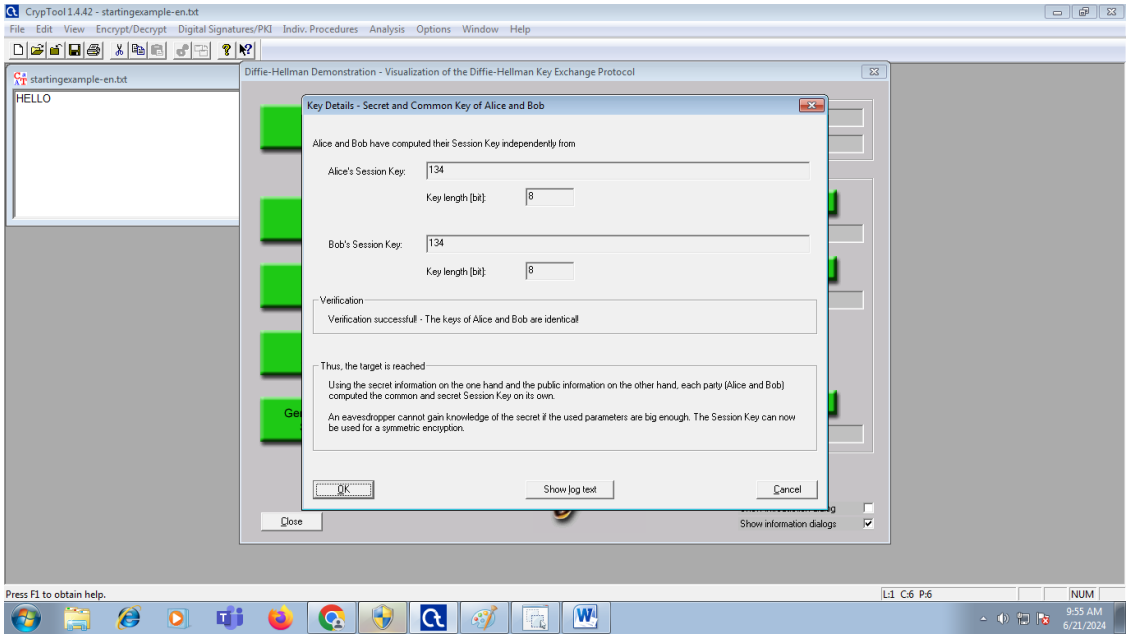


Fig. No. 10.2.14

14. If you want to see log text click on Show Log Text. A new file will be created showings stepwise procedure. Then Click Ok.

X. Conclusion

……

……

……

XI. Practical Related Questions

1. What is Man in the Middle (MIM) attack?
2. What is Asymmetric and Symmetric Encryption.?
3. Differentiate between private and public key.

Space for answer

……

……

……

……

……

……

……

……

……

……

……

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

XII. References/Suggestions for further reading

1. https://www.geeksforgeeks.org/implement-diffie-hellman-key-exchange
2. https://www.programmnigoss.com/2015/11/diffie-hellman-key-exchange-algorithm.html

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

*Practical No.11: Use Steganography to encode and decode the message using any open-source tool (Example-OpenStego)

I. Practical Significance

Steganography is a technique that allows one to hide binary data within an image while adding few noticeable changes. Steganography is the dark cousin of cryptography, the use of codes. While cryptography provides privacy, steganography is intended to provide secrecy. Privacy is what you need when you use your credit card on the Internet -- you don't want your number revealed to the public. For this, you use cryptography, and send a coded pile of gibberish that only the web site can decipher. Though your code may be unbreakable, any hacker can look and see you've sent a message. For true secrecy, you don't want anyone to know you're sending a message at all.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO4 - Apply various encryption algorithms used for information security.

IV. Laboratory Learning Outcome(s)

LLO 11.1 Implement stenography

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which stenographic techniques are more suitable for which applications.

LSB algorithm: The algorithm used for Encryption and Decryption in this application provides using several layers lieu of using only LSB layer of image. Writing data starts from last layer (8st or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So every step we go to upper layer image quality decreases and image retouching transpires. The encryption is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination. The decryption is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden in that. LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a

simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover. LSB substitution is also possible for GIF formats, but the problem with the GIF image is whenever the least significant bit is changed the whole colour palette will be changed. The problem can be avoided by only using the gray scale GIF images since the gray scale image contains 256 shades and the changes will be done gradually so that it will be very hard to detect.JPEG, the direct substitution of steganographic techniques is not possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images. There are many approaches available for hiding the data within an image: one of the simple least significant bit submission approaches is 'Optimum Pixel Adjustment Procedure'.

The simple steps for OPA explain the procedure of hiding the sample text in an image.

Step1: A few least significant bits (LSB) are substituted with in data to be hidden.

Step2: The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize the errors.

Step3: Let n LSBs be substituted in each pixel.

Step4: Let d= decimal value of the pixel after the substitution.d1 = decimal value of last n bits of the pixel.d2 = decimal value of n bits hidden in that pixel.

Step5: If (d1~d2)<=(2^n)/2then no adjustment is made in that pixel. Else

Step6: If(d1d2)d = d + 2^n.T h i s ' d ' is converted to binary and written back Ravinder Reddy Ch et al IJCSET |November 2012 | Vol 2, Issue 11, 1488-1492 www.ijcset.net | ISSN:2231- 0711 1489 t o p i x e l . T h i s me t h o d o f substitution is simple and easy to retrieve the data and the image quality better so that it provides good security. The encoder algorithm is as given below: 1: for i = 1,…., len (msg) do 2: p = LSB(pixel of the image) 3: if p != message bit then 4: pixel of the image = message bit 5: end if 6: end for The encoding process shows that the entire algorithm can be implemented by writing just a few lines of code. The algorithm works by taking the first pixel of the image and obtaining its LSB value (as per line 2 of the Algorithm). This is typically achieved by calculating the modulus 2 of the pixel value. This will return a 0 if then number is even, and a 1 if the number is odd, which effectively tells us the LSB value. We then compare this value with the message bit that we are trying to embed. If they are already the same, then we do nothing, but if they are different then were place the pixel value with the message bit. This process continues whilst there are still values in the message that need to be encoded The decoder algorithm is:1: for i = 1, ..., len(image string) do2:message string = LSB (pixel string of the image)3: end for The decoding phase is even simpler. As the encoder replaced the LSBs of the pixel values in c in sequence, we already know the order that should be used to retrieve the data. Therefore all we need to do is calculate the modulus 2 of all the pixel values in the stegogramme, and we are able to reconstruct m as m0 .The above Algorithms how the pseudo code of the decoding process. Note that this time we run the loop for length of message instead of length of string. This is because the decoding process is completely separate from the encoding process and therefore has no means of knowing the length of the message. If a key were used, it would

probably reveal this information, but instead we simply retrieve the LSB value of every pixel. When we convert this to ASCII, the message will be readable up to the point that the message was encoded, and will then appear as gibberish when we are reading the LSBs of the image data.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Open source tool-OpenStego	01

VIII. Precaution to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System

IX. Procedure

Download and install OpenStego: OpenStego is available for multiple operating systems, including Windows, Linux, and macOS. Download the compatible version with your operating system and install it on your computer.

1. Launch OpenStego: Once OpenStego is installed, launch the software.
2. Select the file to embed data: To embed data within a file, click on the "Embed" button and select the file ed data within.

Hide data

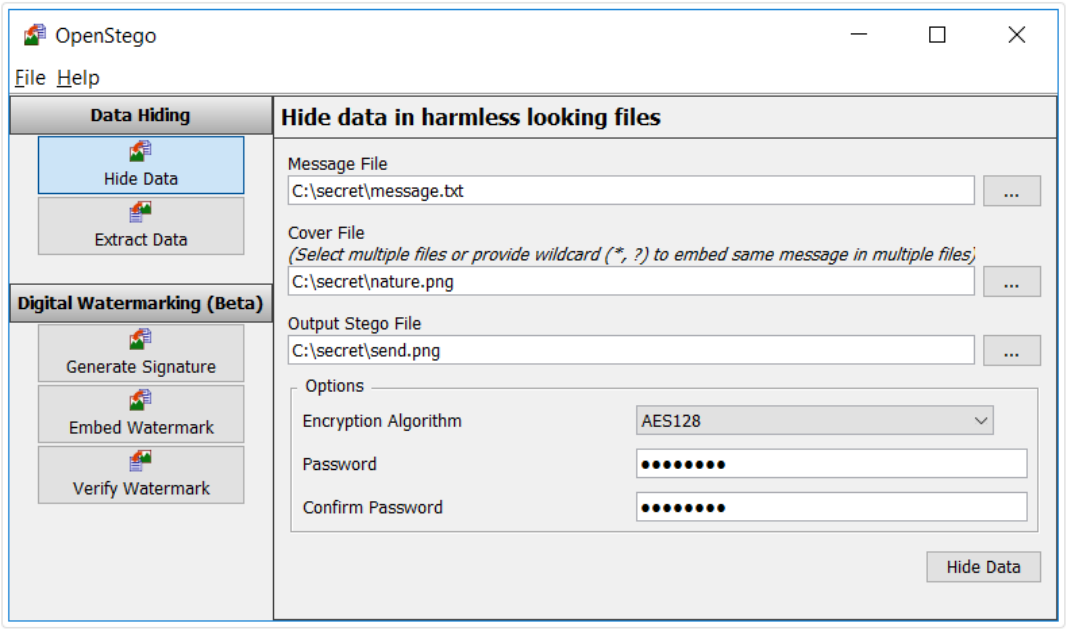


Fig. No. 11.1

3. Select the data to embed: Select the data you want in the file. OpenStego supports various data types, data types, images, and files.

4. Configure the encryption settings: OpenStego provides various encryption settings that can be customized according to your needs. Configure the settings according to your preferences.
5. Embed the data: Once you have configured the encryption settings, click on the "Embed" bun to embed the data within the file

Extract data

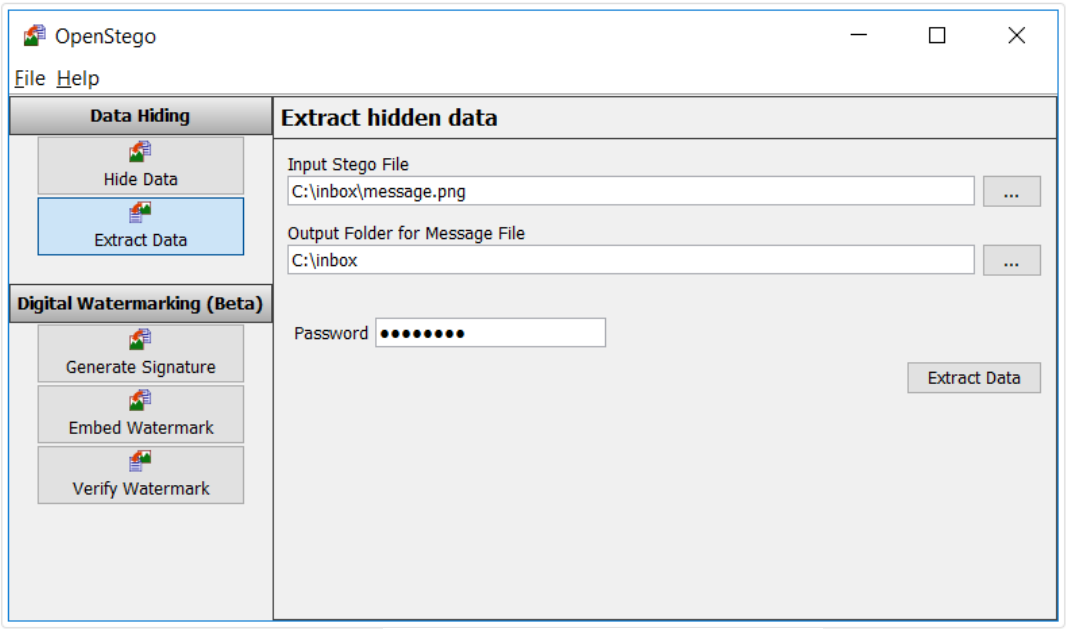


Fig. No. 11.2

6. Extract the data: To extract the hidden data from the file, click the "Extract" but he “Extract” button and select the file data. Remove will extract the hidden removed and display it on the screen.

Generate signature

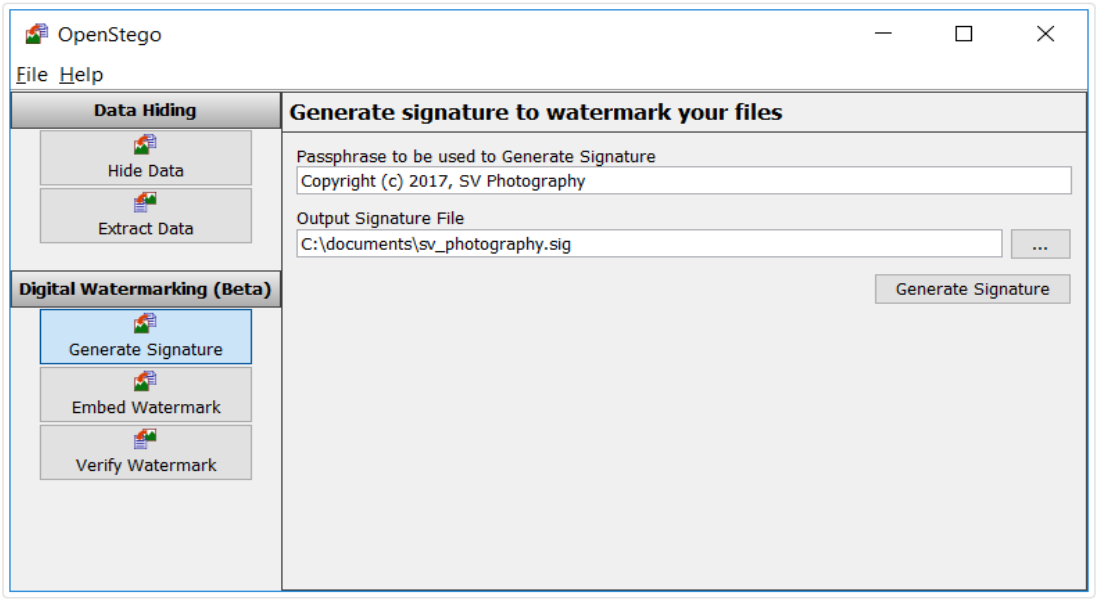


Fig. No. 11.3

Embed watermark

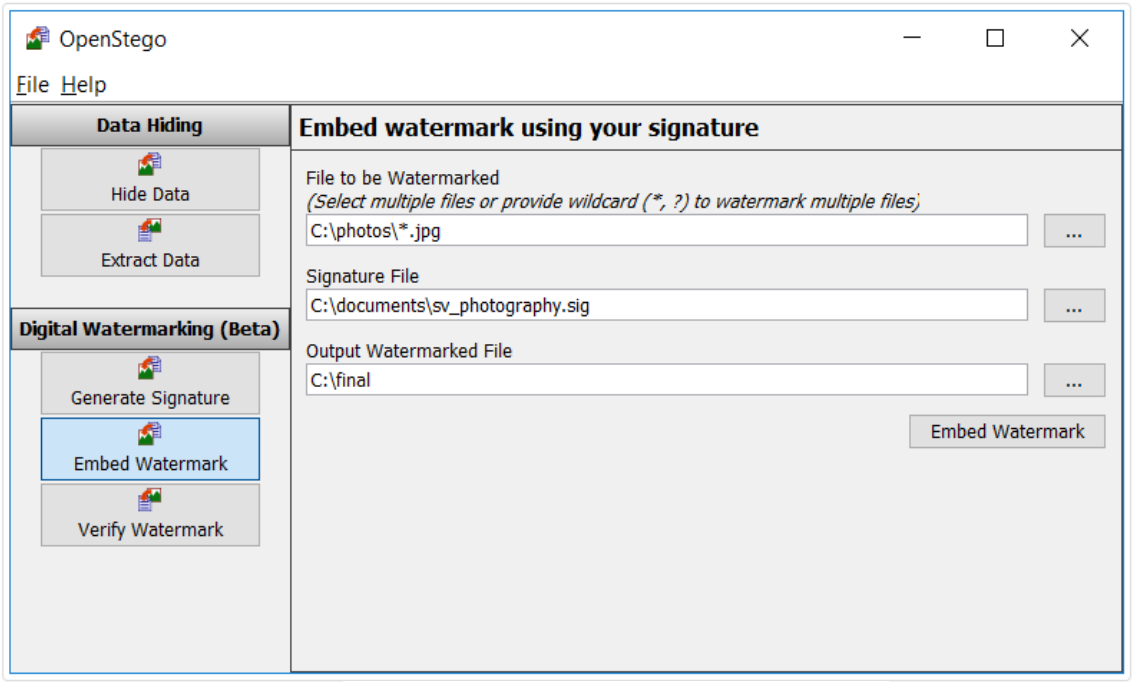


Fig. No. 11.4

Verify watermark

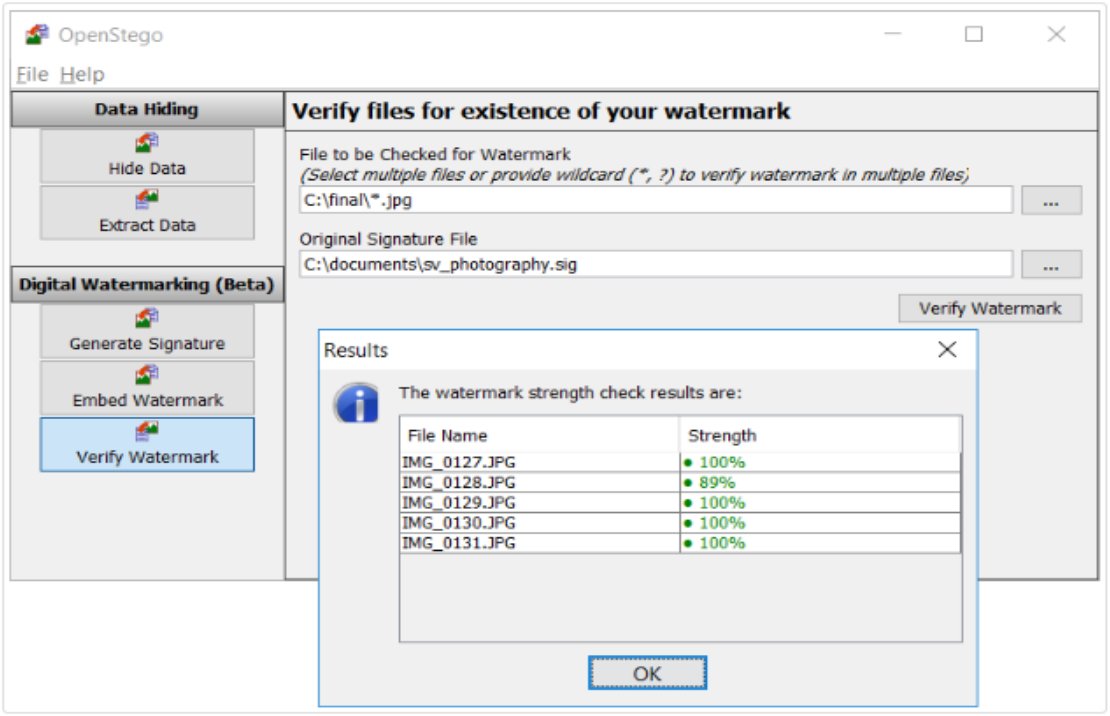


Fig. No. 11.5

X. Conclusion

……

……

……

XI. Practical Related Questions

1. What is steganography?
2. List terminologies used in steganography?

Space for answer

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://www.openstego.com
2. https://www.simplilearn.com/what-is-stegnography-article

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1	Correctness of flow of procedure	
2	Debugging ability	
3	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4	Answer to sample questions	
5	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

*Practical No.12: Create and verify digital signature using any Open source tool (Example- Cryptool)

I. Practical Significance

A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity).

Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO4 - Apply various encryption algorithms used for information security.

IV. Laboratory Learning Outcome(s)

LLO 12.1 Generate digital signature

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature. The Digital Signature Algorithm (DSA), developed by the National Institute of Standards and Technology, is one of many examples of a signing algorithm.

In the following discussion, 1n refers to a unary number.

Formally, a **digital signature scheme** is a triple of probabilistic polynomial time algorithms, (*G, S, V), satisfying:*

- *G* (key-generator) generates a public key (*pk*), and a corresponding private key (*sk*), on input 1*n*, where *n* is the security parameter.
- *S* (signing) returns a tag, *t*, on the inputs: the private key (*sk*), and a string (*x*).

• *V* (verifying) outputs *accepted* or *rejected* on the inputs: the public key (*pk*), a string (*x*), and a tag (*t*).

For correctness, *S* and *V* must satisfy
Pr [(*pk*, *sk*) ← *G*(1*n*), *V*(*pk*, *x*, *S*(*sk*, *x*)) = *accepted*] = 1.[14]
A digital signature scheme is **secure** if for every non-uniform probabilistic polynomial time adversary, A
Pr [(*pk*, *sk*) ← *G*(1^n), (*x*, *t*) ← $A^{S(sk, \cdot)}$(*pk*, 1^n), $x \notin Q$, *V*(*pk*, *x*, *t*) = *accepted*] < negl(*n*), where $A^{S(sk, \cdot)}$ denotes that *A* has access to the oracle, *S*(*sk*, ·), *Q* denotes the set of the queries on *S* made by *A*, which knows the public key, *pk*, and the security parameter, *n*, and $x \notin Q$ denotes that the adversary may not directly query the string, *x*, on *S*.

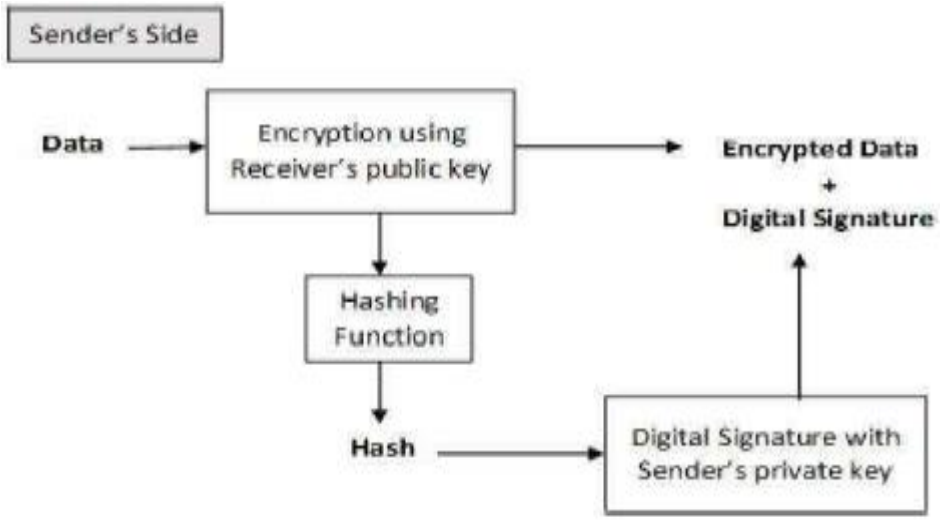


Fig. No. 12.1

Digital signatures versus ink on paper signatures
An ink signature could be replicated from one document to another by copying the image manually or digitally, but to have credible signature copies that can resist some scrutiny is a significant manual or technical skill, and to produce ink signature copies that resist professional scrutiny is very difficult.
Digital signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Paper contracts sometimes have the ink signature block on the last page, and the previous pages may be replaced after a signature is applied. Digital signatures can be applied to an entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered, but this can also be achieved by signing with ink and numbering all pages of the contract.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Crytool 1	01

VIII. Precaution to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System

IX. Procedure

1. Create new file or open existing file

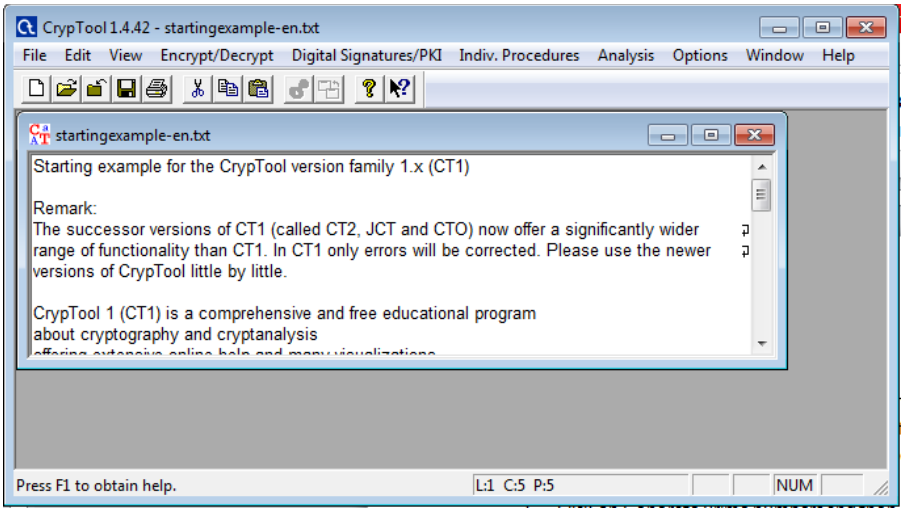


Fig. No. 12.2

2. Select Digital signature/PKI - >Signature Demonstration. Flow chart will be displayed.

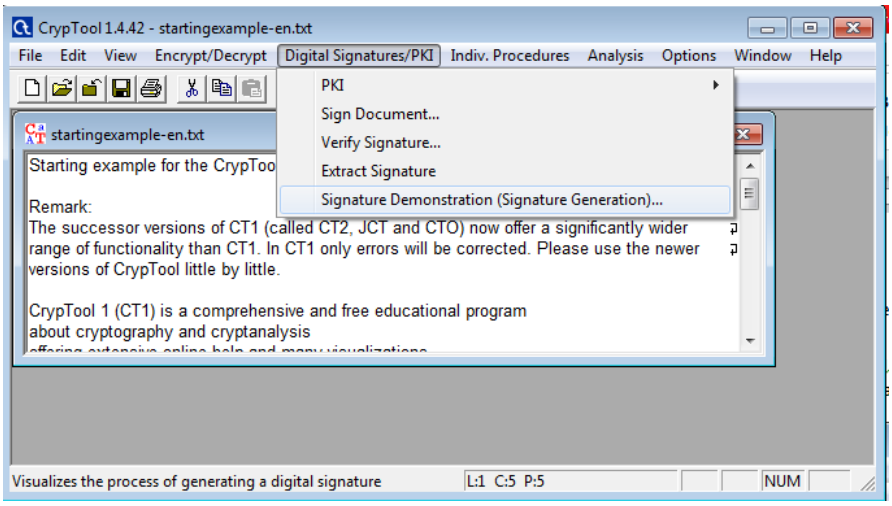


Fig. No. 12.3

3. Click on select has function and select hash function (e.g. MD5) as per your choice. Click Ok.

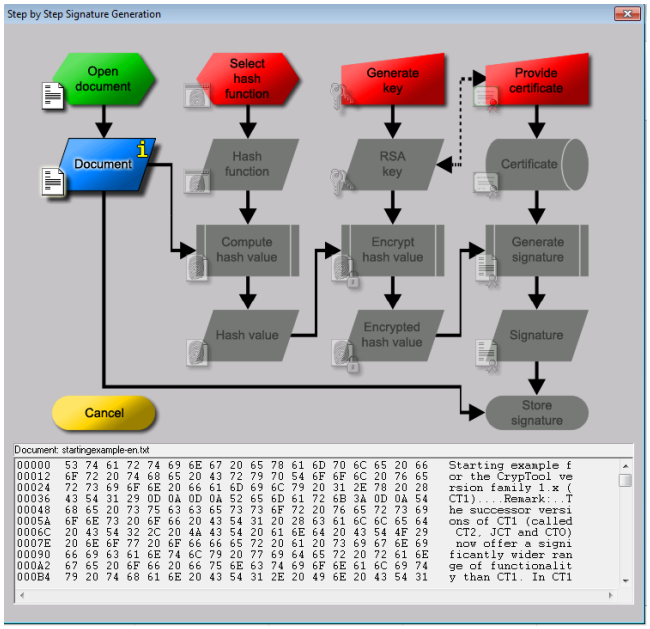


Fig. No. 12.4

4. Next click on Generate Key. Generate RSA key window will popup. Click on Generate Prime.

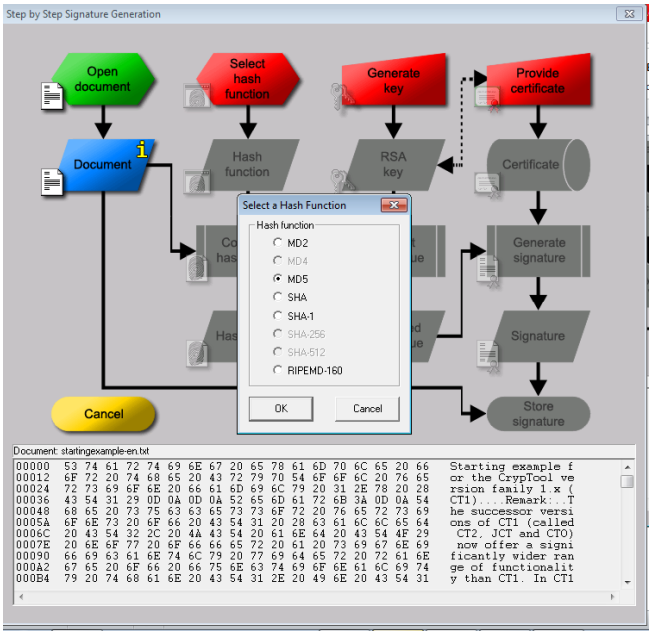


Fig. No. 12.5

5. No. Select as options as per shown in Fig. No. 12.6

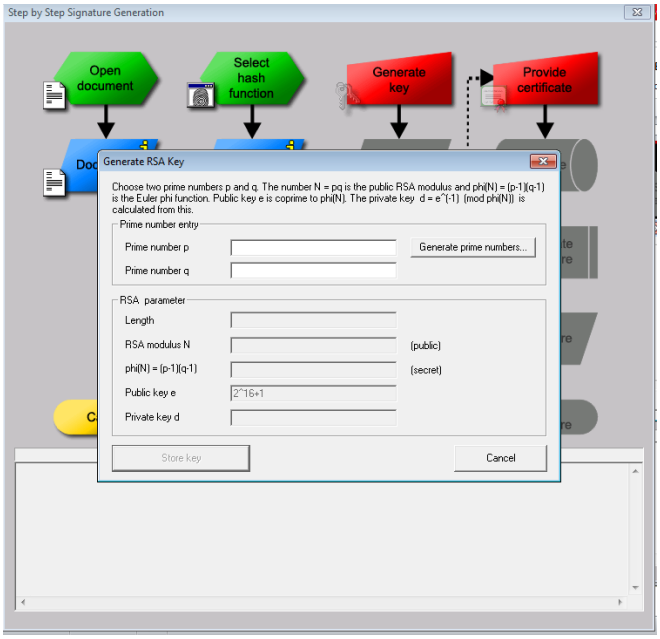


Fig. No. 12.6

6. Click on Generate Prime numbers and then Apply primes button. Then Click on Store Key.

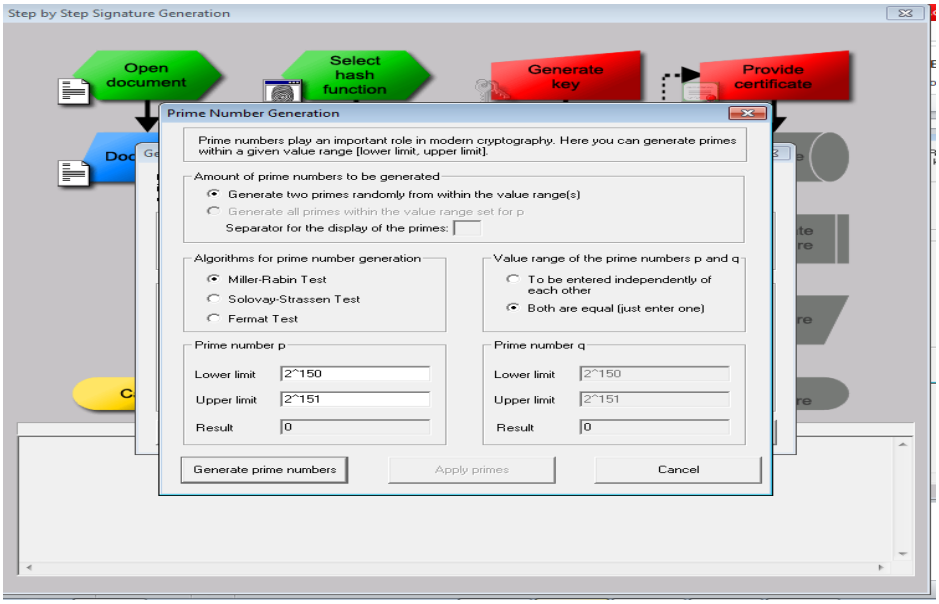


Fig. No. 12.7

7. After this in flow chart click on Provide certificate. Create certificate and PSE window will appear.

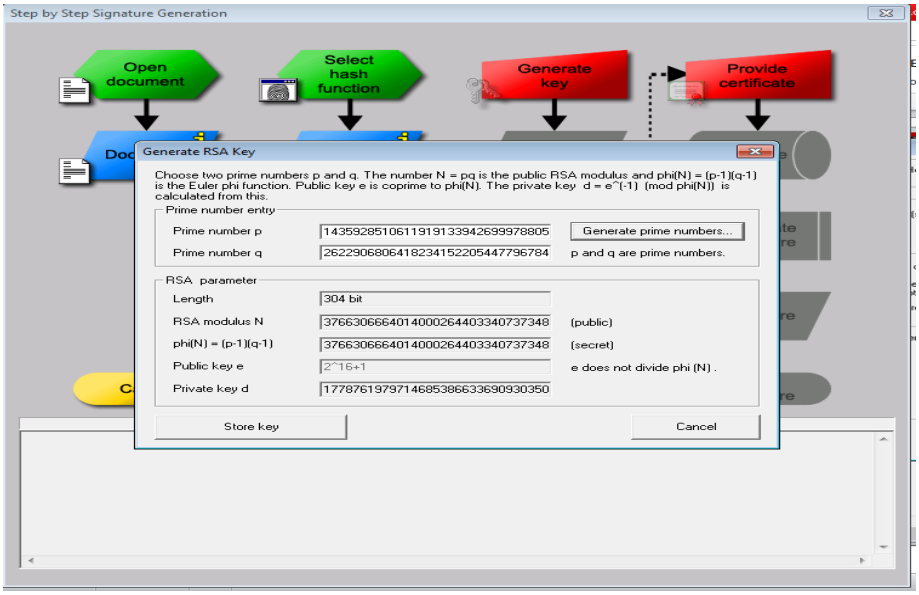


Fig. No. 12.8

8. Enter personal data for certificate. And click on create certificate and PSE button.

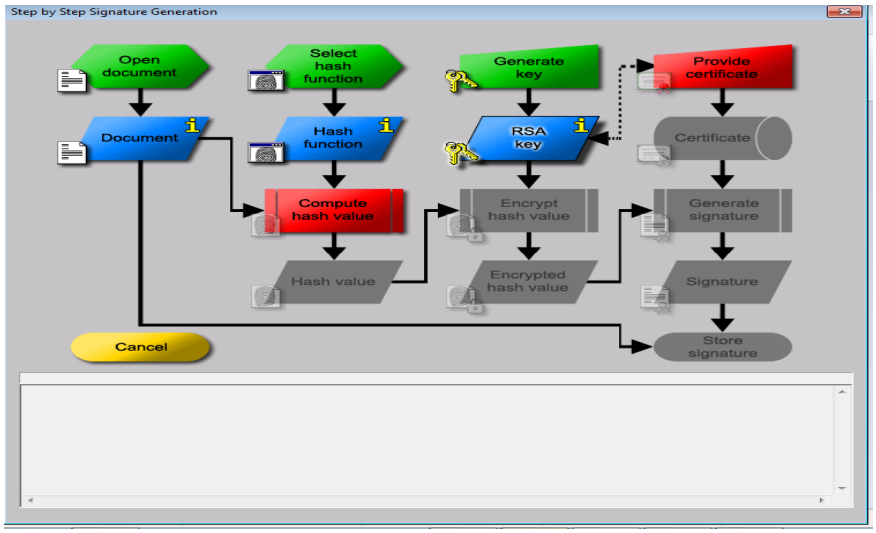


Fig. No. 12.9

9. On flow chart click on has value.

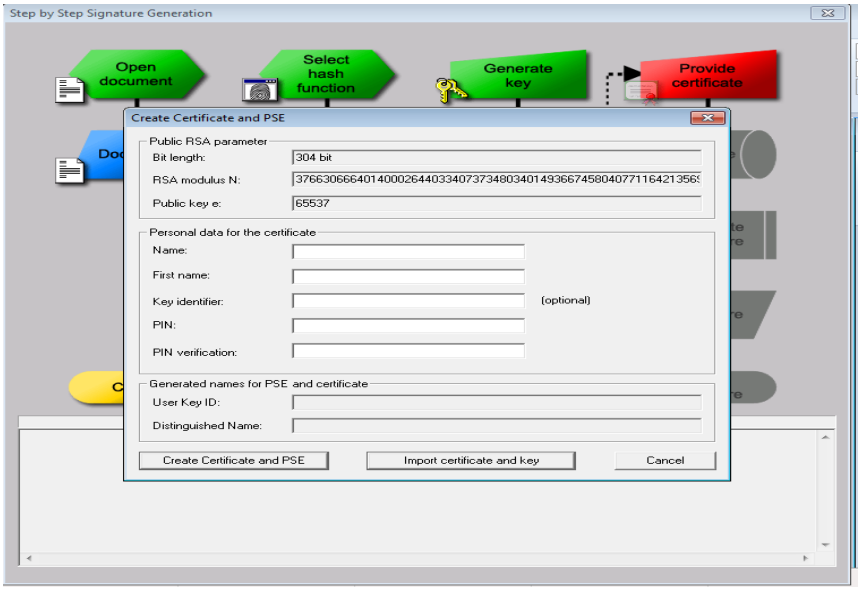


Fig. No. 12.10

10. Then Click on encrypt has value.

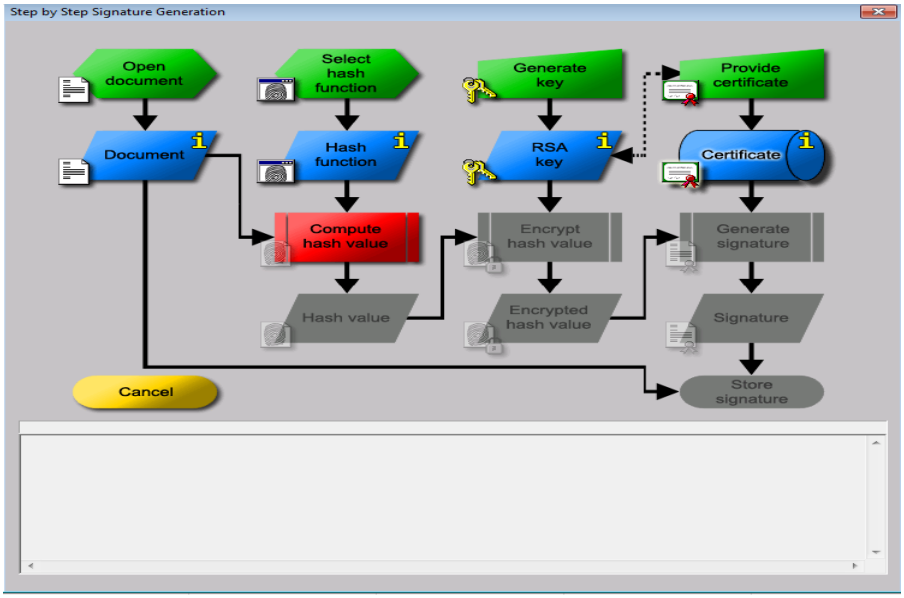


Fig. No. 12.11

11. Then click on Generate Signature. Signature will be generated.

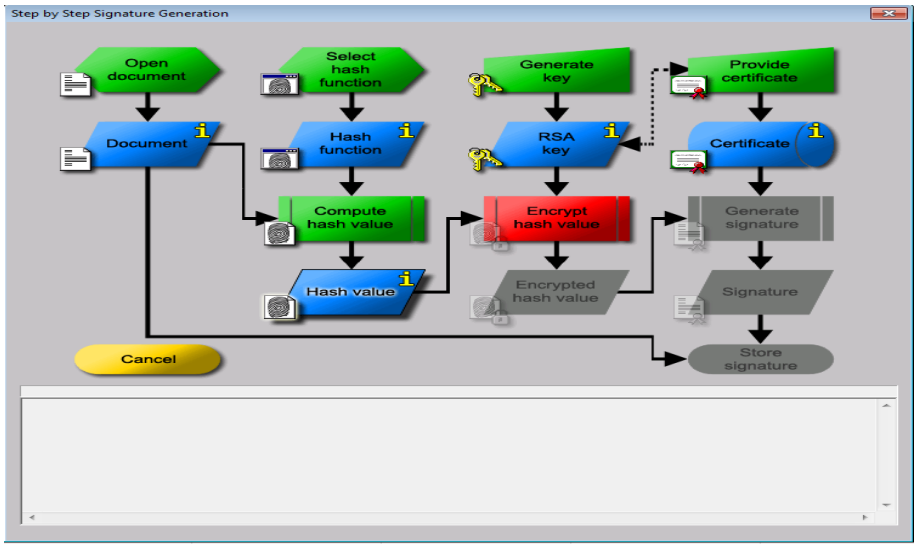


Fig. No. 12.12

12. Then click on store signature.

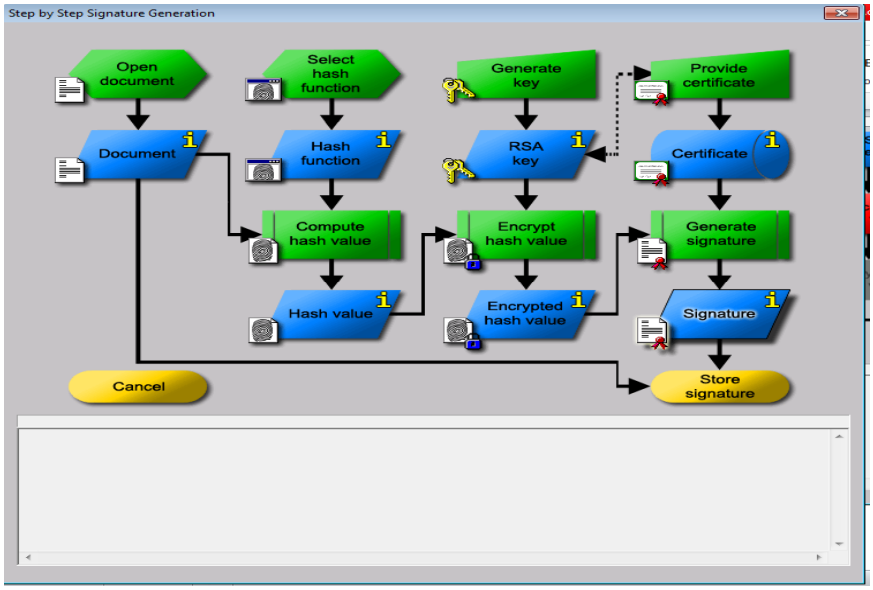


Fig. No. 12.13

13. Window will pop saying congratulation, you have successfully created RSA signature. Click Ok.

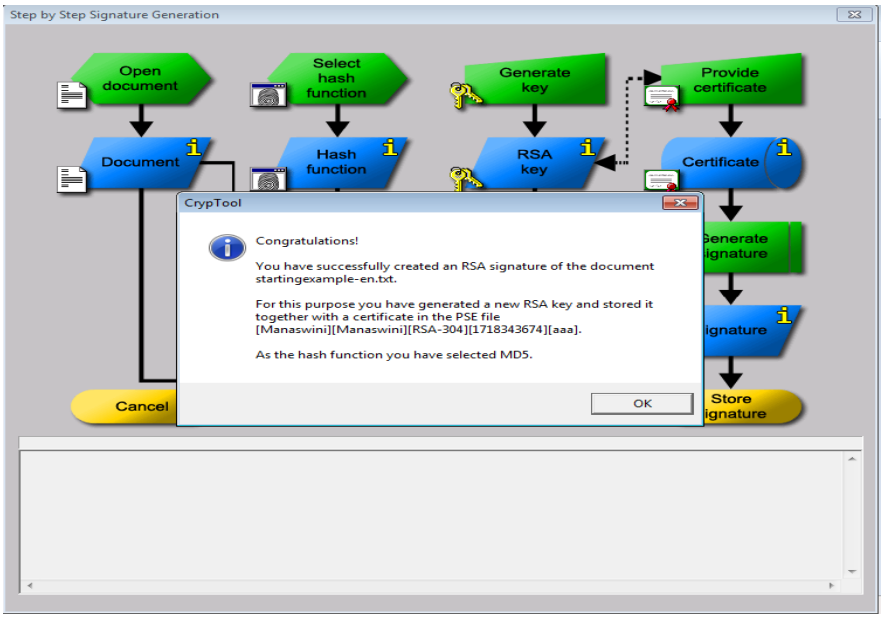


Fig. No. 12.14

14. You will get window which is document created with unique digital signature.

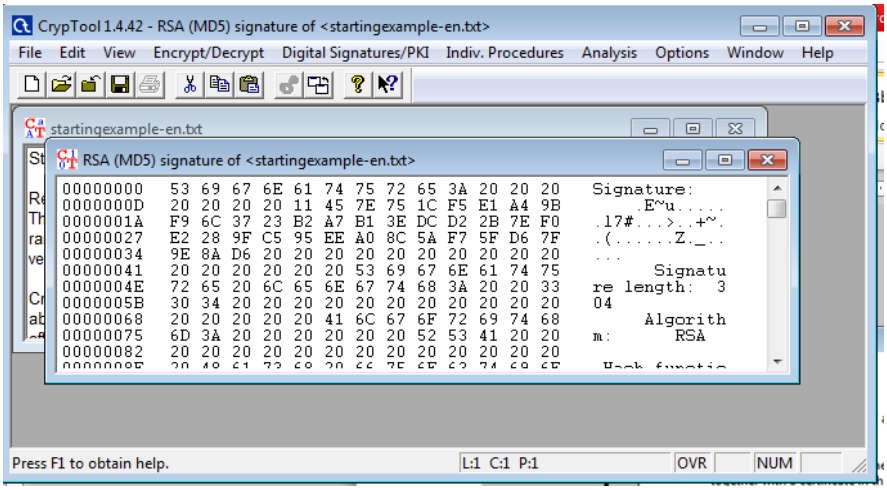


Fig. No. 12.15

X. Conclusion

……

……

……

XI. Practical Related Questions

1. Explain the term Honeypot and list its types.
2. Explain host based IDS.
3. Enlist the mobile security threats.

Space for answer

……

……

……

XII. References/Suggestions for further reading

1. https://www.infosecinstitute.com/resources/cryptography/cryptography-fundamentals-part-3-hashing/
2. https://www.signnow.com/esignature/cryptographic-signature
3. https://www.youtube.com/watch?v=dvLawz6MbUw&t=194s

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

*Practical No.13: Configure firewall settings on any operating system

I. Practical Significance

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO5 - Implement security techniques to prevent internet threats.

IV. Laboratory Learning Outcome(s)

LLO 13.1 Configure firewall

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Step 1: Secure your firewall

If an attacker is able to gain administrative access to your firewall it is "game over" for your network security. Therefore, securing your firewall is the first and most important step of this process. Never put a firewall into production that is not properly secured by at least the following configuration actions:

- Update your firewall to the latest firmware.
- Delete, disable, or rename any default user accounts and change all default passwords. Make sure to use only complex and secure passwords.
- If multiple administrators will manage the firewall, create additional administrator accounts with limited privileges based on responsibilities. Never use shared user accounts.
- Disable simple network management protocol (SNMP) or configure it to use a secure community string.

Step 2: Architect your firewall zones and IP addresses

In order to protect the valuable assets on your network, you should first identify what the assets (for example, payment card data or patient data) are. Then plan out your network structure so that these assets can be grouped together and placed into networks (or zones) based on similar sensitivity level and function.

For example, all of your servers that provide services over the internet (web servers, email servers, virtual private network (VPN) servers, etc.) should be placed into a dedicated zone that will allow limited inbound traffic from the internet (this zone is often called a demilitarized zone or DMZ).

Servers that should not be accessed directly from the internet, such as database servers, must be placed in internal server zones instead. Likewise, workstations, point of sale devices, and voice over Internet protocol (VOIP) systems can usually be placed in internal network zones.

Generally speaking, the more zones you create, the more secure your network. But keep in mind that managing more zones requires additional time and resources, so you need to be careful when deciding how many network zones you want to use.

If you are using IP version 4, Internal IP addresses should be used for all of your internal networks. Network address translation (NAT) must be configured to allow internal devices to communicate on the Internet when necessary.

Once you have designed your network zone structure and established the corresponding IP address scheme, you are ready to create your firewall zones and assign them to your firewall interfaces or sub interfaces. As you build out your network infrastructure, switches that support virtual LANs (VLANs) should be used to maintain level-2 separation between the networks.

Step 3: Configure access control lists

Now that you have established your network zones and assigned them to interfaces, you should determine exactly which traffic needs to be able to flow into and out of each zone.

This traffic will be permitted using firewall rules called access control lists (ACLs), which are applied to each interface or sub interface on the firewall. Make your ACLs specific to the exact source and/or destination IP addresses and port numbers whenever possible. At the end of every access control list, make sure there is a "deny all" rule to filter out all unapproved traffic. Apply both inbound and outbound ACLs to each interface and sub interface on your firewall so that only approved traffic is allowed into and out of each zone.

Whenever possible, it is generally advised to disable your firewall administration interfaces (including both secure shell (SSH) and web interfaces) from public access. This will help to protect your firewall configuration from outside threats. Make sure to disable all unencrypted protocols for firewall management, including Telnet and HTTP connections.

Step 4: Configure your other firewall services and logging

If your firewall is also capable of acting as a dynamic host configuration protocol (DHCP) server, network time protocol (NTP) server, intrusion prevention system (IPS), etc., then go ahead and configure the services you wish to use. Disable all the extra services that you don't intend to use.

Step 5: Test your firewall configuration

In a test environment, verify that your firewall works as intended. Don't forget to verify that your firewall is blocking traffic that should be blocked according to your ACL configurations. Testing your firewall should include both vulnerability scanning and penetration testing.

Once you have finished testing your firewall, your firewall should be ready for production. Always remember to keep a backup of your firewall configuration saved in a secure place so that all of your hard work is not lost in the event of a hardware failure.

Now remember, this is just an overview to help you understand the major steps of firewall configuration. When using tutorials, or even if you decide to configure your own firewall, be sure to have a security expert review your configuration to make sure it is set up to keep your data as

safe as possible.

Firewall management

With your firewall in production, you have finished your firewall configuration, but firewall management has just begun. Logs must be monitored, firmware must be updated, vulnerability scans must be performed, and firewall rules must be reviewed at least every six months. Last of all, be sure to document your process and be diligent about performing these ongoing tasks to ensure that your firewall continues to protect your network.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01

VIII. Precaution to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System

IX. Procedure to be followed

Install firewall on any operating system.

1. Open settings

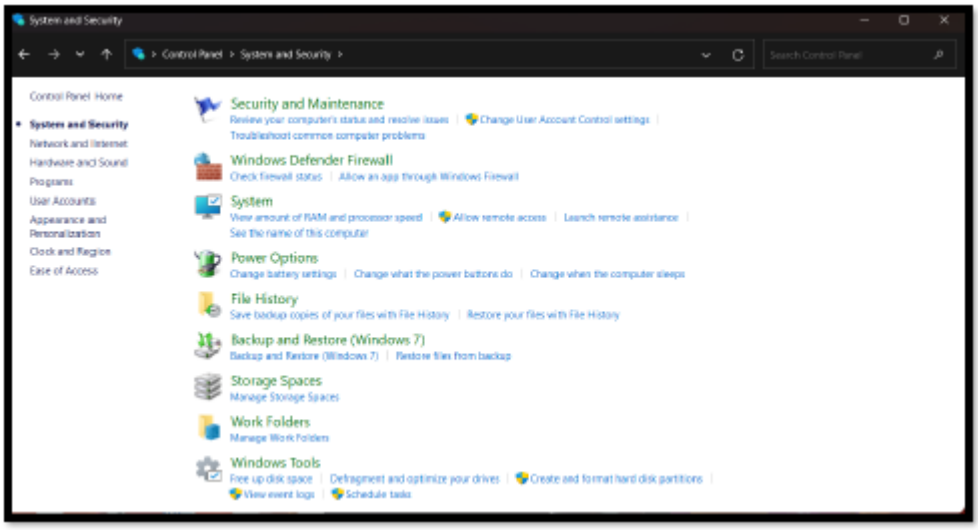


Fig. No.13.1

2. Select System and Security

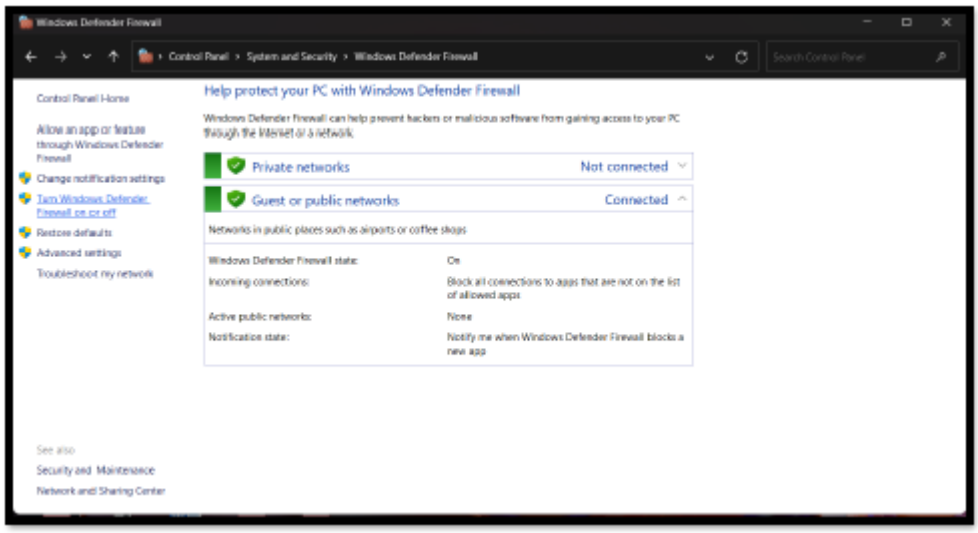


Fig. No.13.2

Figure 13.2

3. Click on "Turn Windows Defense Firewall on or off"

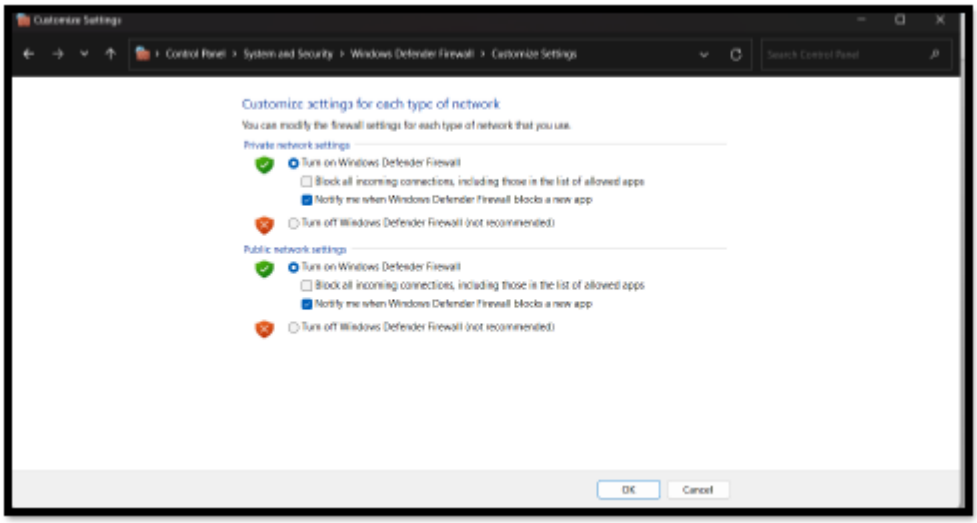


Fig. No.13.3

Configure firewall settings on any operating system.

1. Open settings

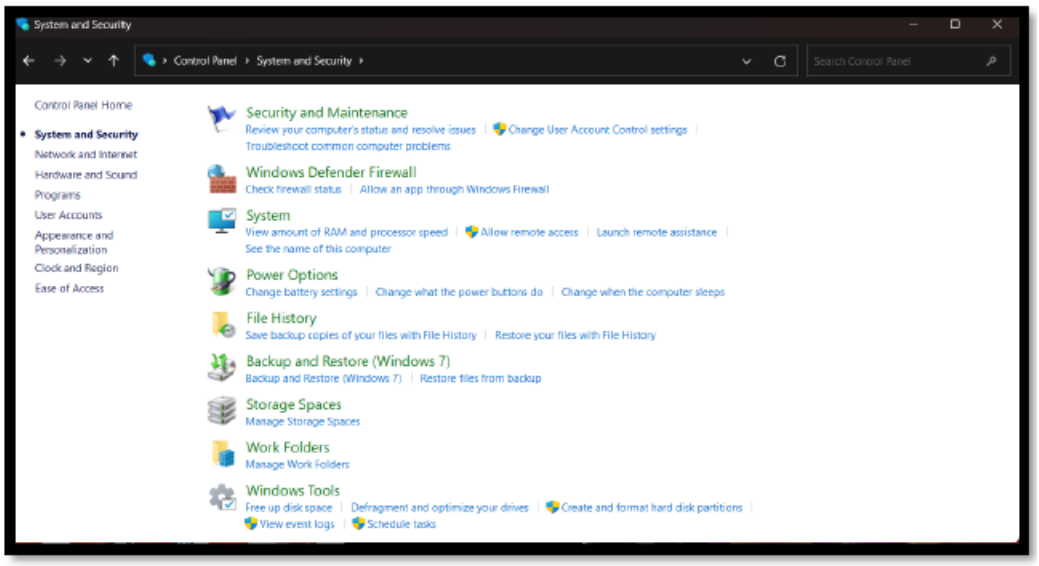


Fig. No.13.4

2. Select System and Security

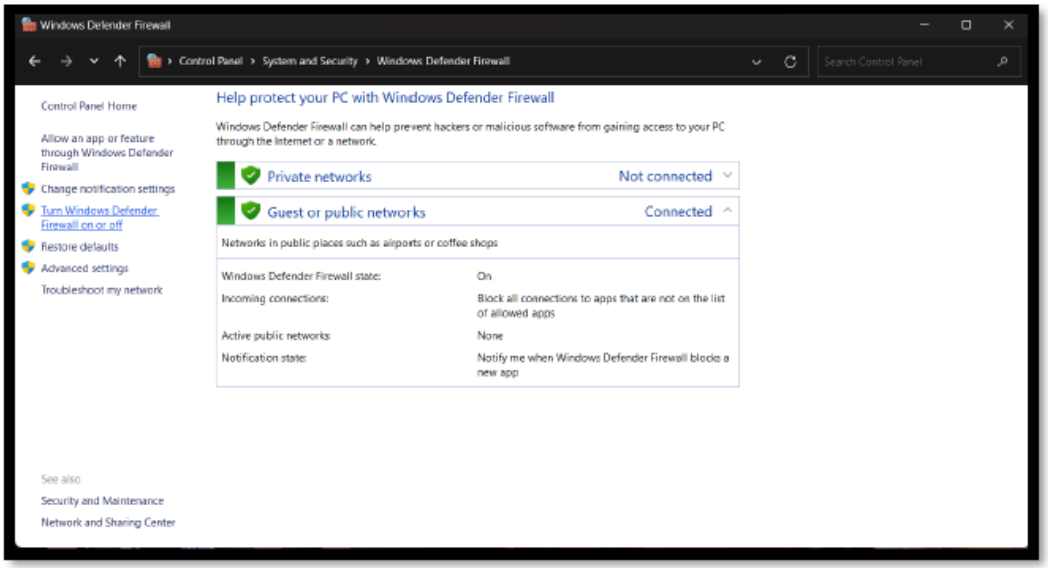


Fig. No.13.5

3. Click on "Turn Windows Defense Firewall on or off"

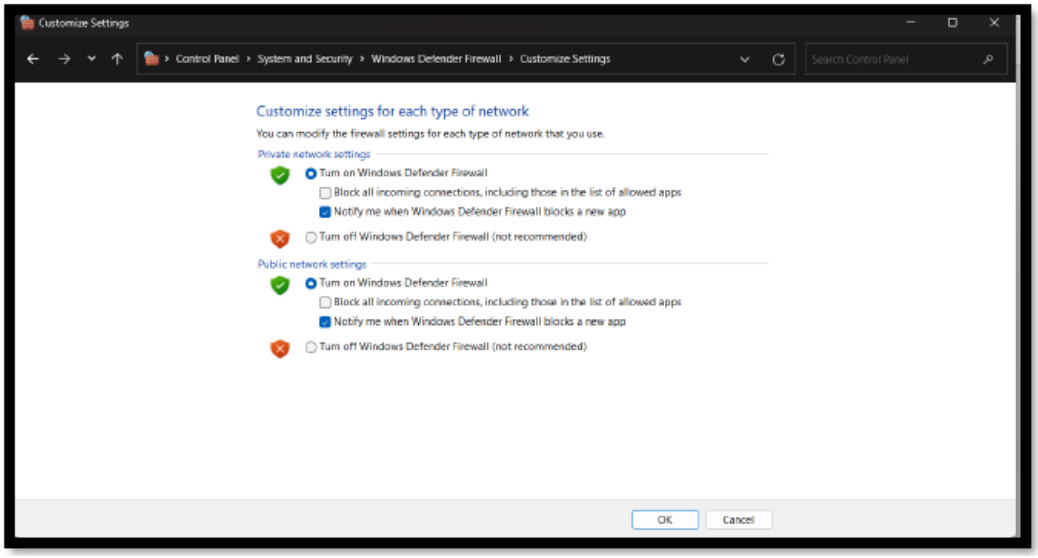


Fig. No.13.6

4. Click "OK"

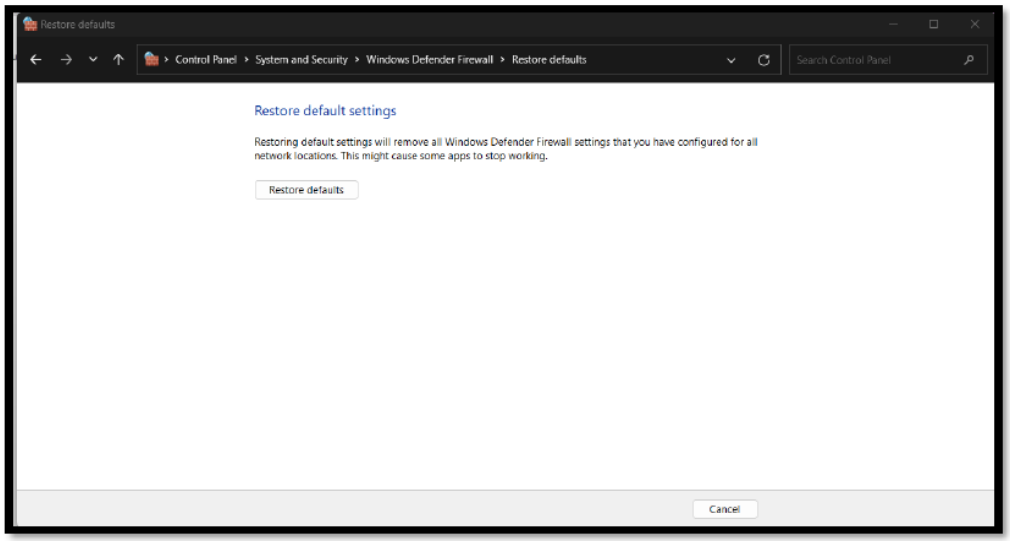


Fig. No.13.7

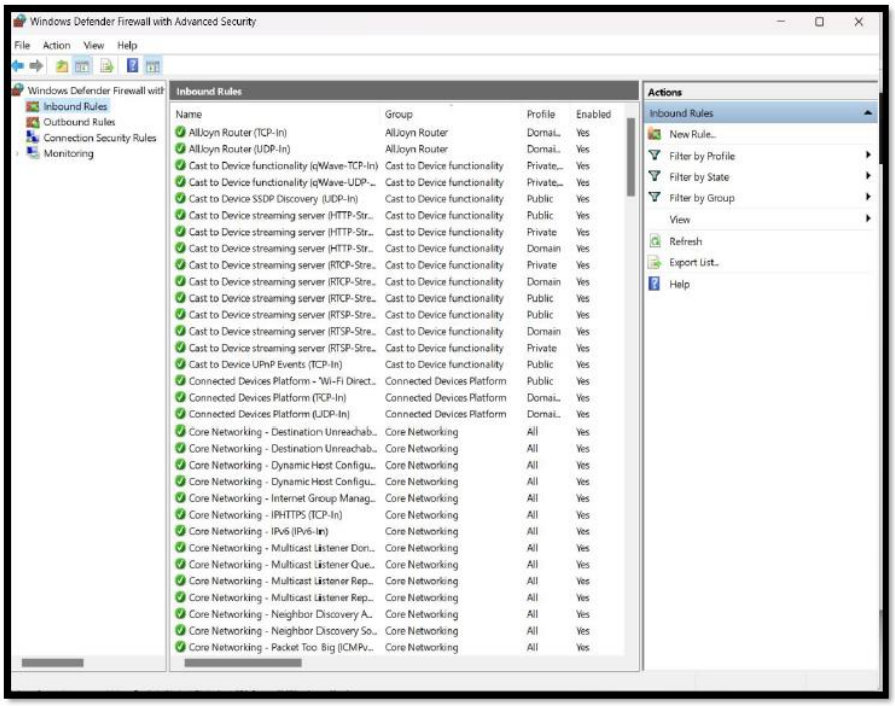


Fig. No.13.8

X. Conclusion

……

……

……

XI. Practical Related Questions

1. List types of firewall?
2. What is intrusion detection system?
3. What is DMZ?
4. Describe packet filter router firewall with diagram?
5. Explain the needs of firewalls?

Space for answer

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://www.fortinet.com/resources/cyberglossary/firewall-configuration
2. https://www.securitymetrics.com/blog/how-configure-firewall-5-steps

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No.14: Send a test mail securely using any open-source tool (Example- Pretty Good Privacy with GnuPG)

I. Practical Significance

Data that can be read and understood without any special measures is called plaintext or cipher text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO5 - Implement security techniques to prevent internet threats.

IV. Laboratory Learning Outcome(s)

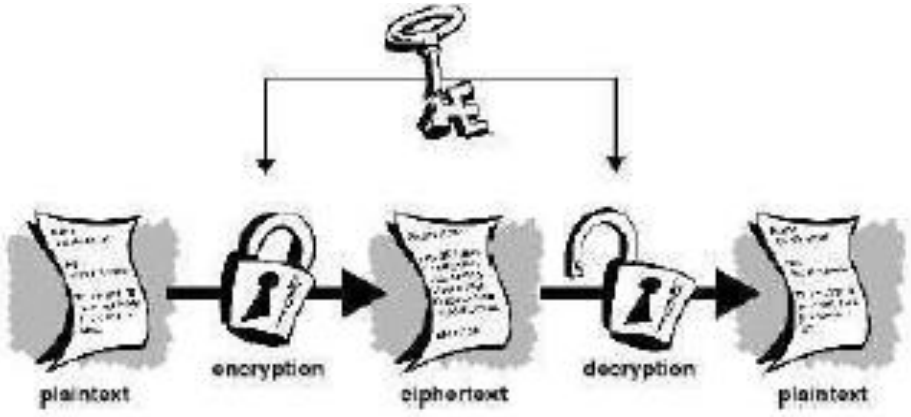
LLO 14.1 Implement email security

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government.



Key management and conventional encryption

Conventional encryption has benefits. It is very fast. It is especially useful for encrypting data that is not going anywhere. However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution. Recall a character from your favorite spy movie: the person with a locked briefcase handcuffed to his or her wrist. What is in the briefcase, anyway? It's probably not the missile launch code/ biotoxin formula/ invasion plan itself. It's the key that will decrypt the secret data.

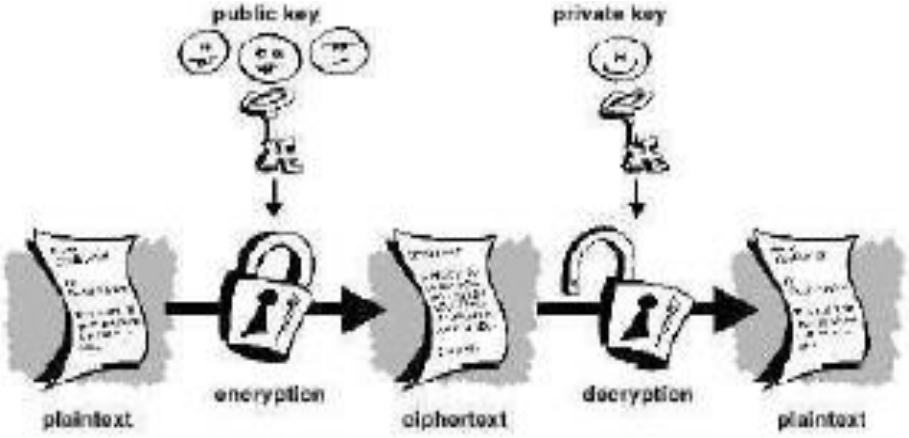
For a sender and recipient to communicate securely using conventional encryption, they must

agree upon a key and keep it secret between themselves. If they are in different physical locations, they must trust a courier, the Bat Phone, or some other secure communication medium to prevent the disclosure of the secret key during transmission. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key. From DES to Captain Midnight's Secret Decoder Ring, the persistent problem with conventional encryption is key distribution: how do you get the key to the recipient without someone intercepting it?

Public key cryptography

The problems of key distribution are solved by public key cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975.

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met. It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.



Public key encryption

The primary benefit of public key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Some examples of public-key cryptosystems are Elgamal (named for its inventor, Taher Elgamal), RSA.

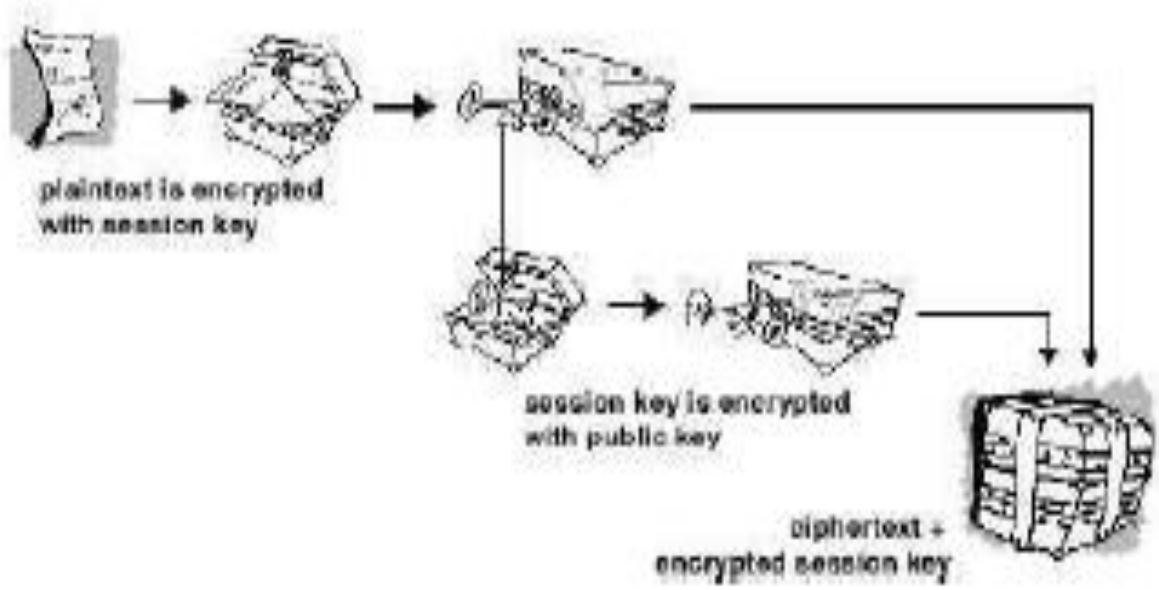
Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks (or small children with secret decoder rings). Public key encryption is the technological revolution that provides strong cryptography to the adult masses. Remember the courier with the locked briefcase handcuffed to his wrist? Public-key encryption puts him out of business (probably to his relief).

How PGP works

PGP combines some of the best features of both conventional and public key cryptography. PGP is

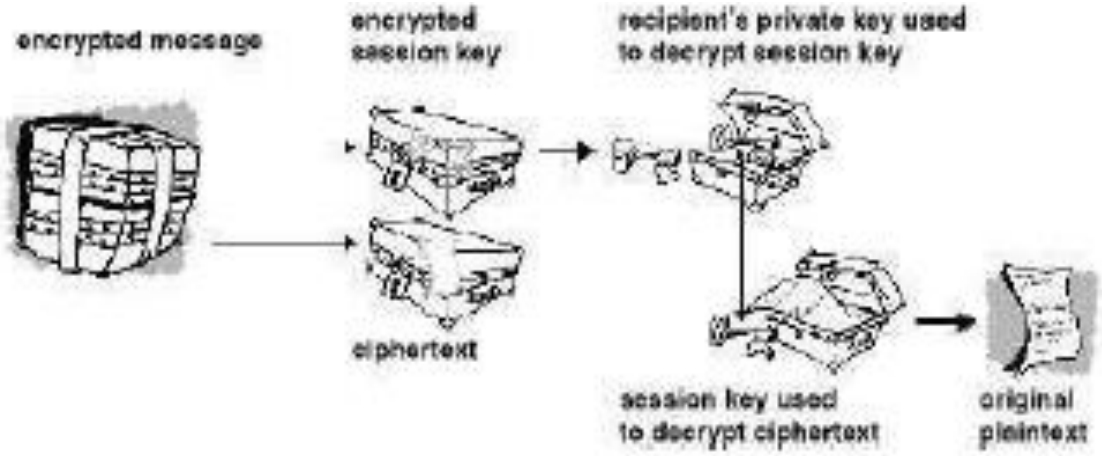
a hybrid cryptosystem. When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security. Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis. (Files that are too short to compress or which don't compress well aren't compressed.)

PGP then creates a session key, which is a one-time-only secret key. This key is a random number generated from the random movements of your mouse and the keystrokes you type. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.



How PGP encryption works

Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.



How PGP decryption works

The combination of the two encryption methods combines the convenience of public key encryption with the speed of conventional encryption. Conventional encryption is about 1, 000 times faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. Used together, performance and key distribution are improved without any sacrifice in security.

Keys

A key is a value that works with a cryptographic algorithm to produce a specific cipher text. Keys are basically really, really, really big numbers. Key size is measured in bits; the number representing a 1024-bit key is darn huge. In public key cryptography, the bigger the key, the more secure the cipher text.

However, public key size and conventional cryptography's secret key size are totally unrelated. A conventional 80-bit key has the equivalent strength of a 1024-bit public key. A conventional 128-bit key is equivalent to a 3000-bit public key. Again, the bigger the key, the more secure, but the algorithms used for each type of cryptography are very different and thus comparison is like that of apples to oranges.

While the public and private keys are mathematically related, it's very difficult to derive the private key given only the public key; however, deriving the private key is always possible given enough time and computing power. This makes it very important to pick keys of the right size; large enough to be secure, but small enough to be applied fairly quickly. Additionally, you need to consider who might be trying to read your files, how determined they are, how much time they have, and what their resources might be. .

Keys are stored in encrypted form. PGP stores the keys in two files on your hard disk; one for public keys and one for private keys. These files are called key rings. As you use PGP, you will typically add the public keys of your recipients to your public key ring. Your private keys are stored on your private key ring. If you lose your private key ring, you will be unable to decrypt any information encrypted to keys on that ring.

Tool :

GnuPG (Gnu Privacy Guard), often referred to as GPG, is a free and open-source implementation of the OpenPGP standard as defined by RFC 4880 (also known as PGP). GPG is a powerful tool for encrypting, decrypting, and signing data and communications. It provides the core functionalities needed to secure data and is widely used in various applications.

Key Features of GnuPG :

1. Open Source:

GnuPG is free software and is available under the GNU General Public License (GPL). This ensures that it can be freely used, modified, and distributed.

2. Standards Compliant:

GnuPG adheres to the OpenPGP standard, making it compatible with other OpenPGP-compliant software, including commercial PGP products.

3. Encryption and Decryption:

GPG can encrypt and decrypt files and communications, using a combination of symmetric-key and public-key cryptography for secure data transfer.

4. Digital Signatures:

GPG supports creating and verifying digital signatures to ensure the authenticity and integrity of data.

5. Key Management:

GPG provides robust tools for generating, managing, and distributing cryptographic keys. It supports key servers for public key distribution and includes features for key signing and trust management.

6. Web of Trust:

GPG supports the Web of Trust model, allowing users to sign each other's keys to establish a network of trust relationships.

7. Scripting and Automation:

GPG can be easily integrated into scripts and automated workflows, making it suitable for a wide range of applications from email encryption to securing software distributions.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	GPG4win(Pretty Good Privacy with GnuPG)	01

VIII. Precaution to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System

IX. Procedure

1. To install GPG on Windows, download and install the **"Kleopatra"** application from "https://www.gpg4win.org/download.html". After installing start the **"Kleopatra"** application.

Fig.No. 14.1

2. After installing click on Next.

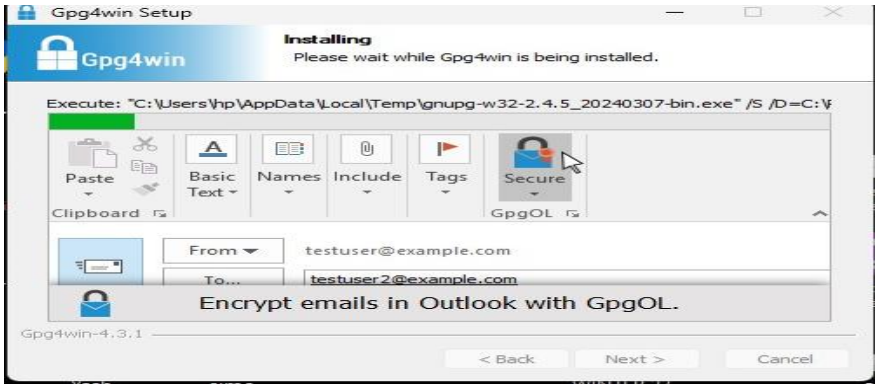


Fig. No. 14.2

3. Write the path for the destiation folder. You can also browse it. After metioning the correct destiation folder path click on install.

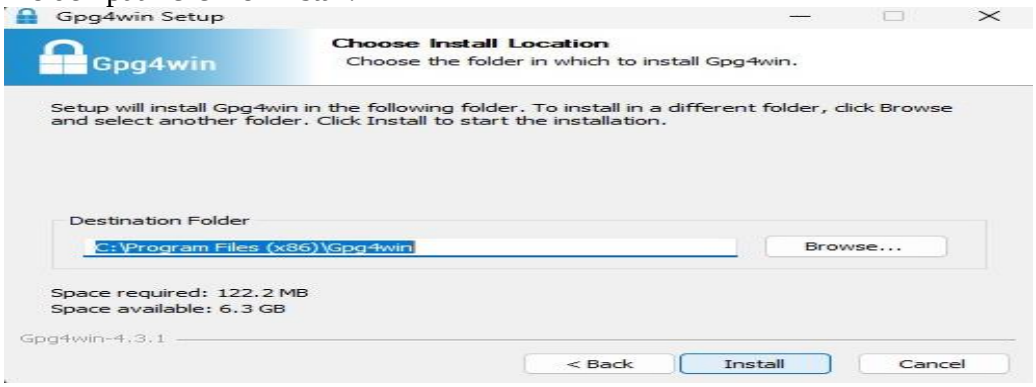


Fig. No. 14.3

4. This will open welcome page of "Kleopatra" application.

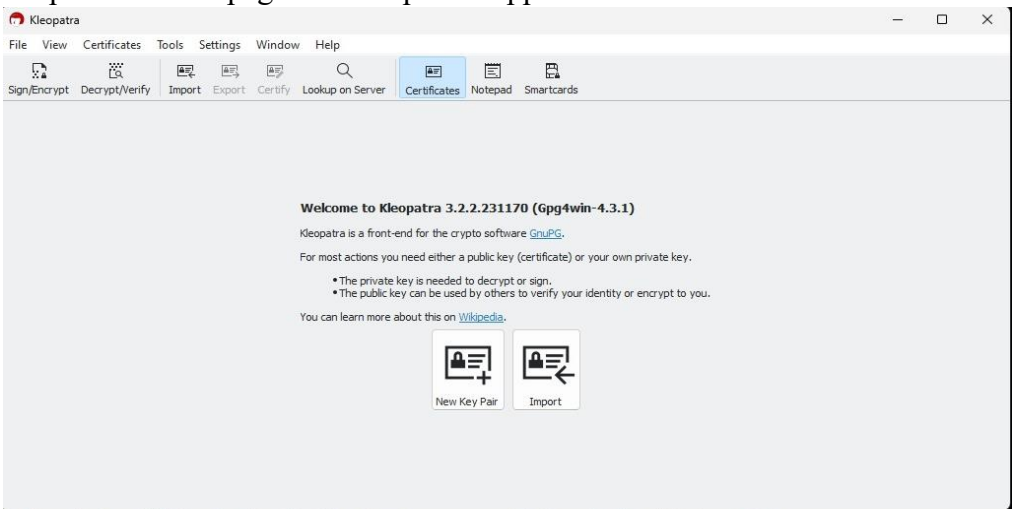


Fig. No 14.4

5. On the welcome click on "Certificates" option. This will open the "Create OpenPGP Certificate" dialogue box. Specify the Name and Email address in the fields and once you mention click on "Advanced Settings…" button. (Key generation)

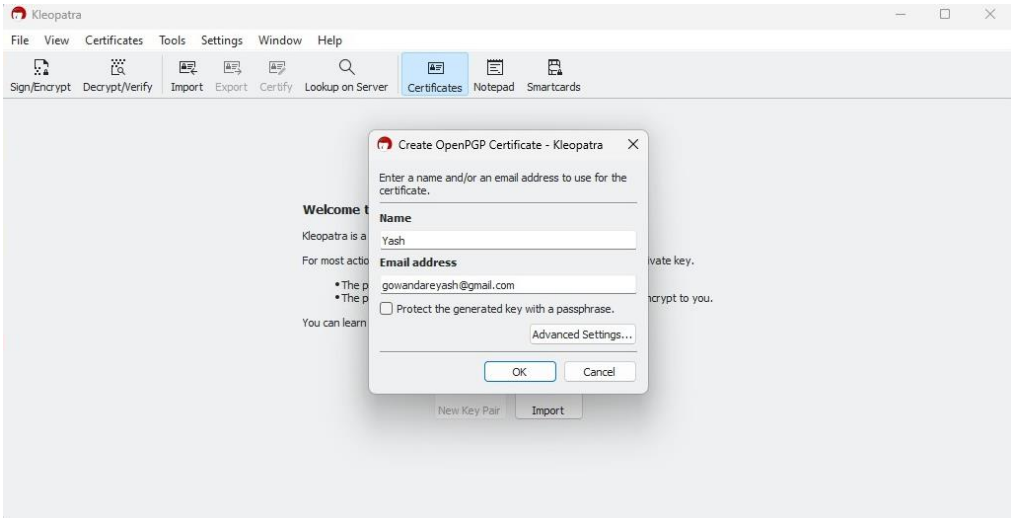


Fig. No. 14.5

6. Provide the additional settings according to your requirements and finally click on "OK".

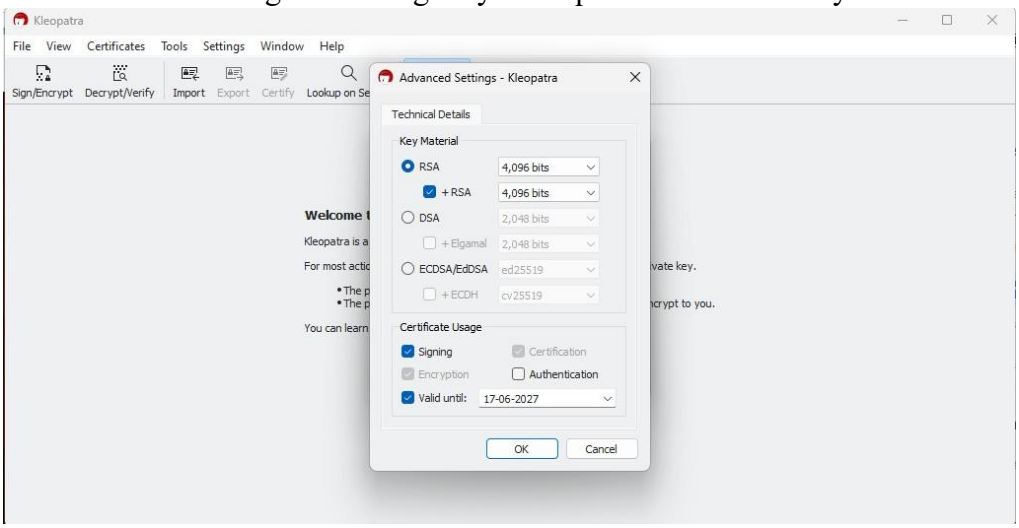


Fig. No. 14.6

7. Once you click on "OK" it will create a certificate with the Name, Email, User-IDs, Valid Until and Key-ID you have provided to it. Click on the Name field of created certificate and select "Export…" or press Ctrl+E from the drop down menus. (Export the key)

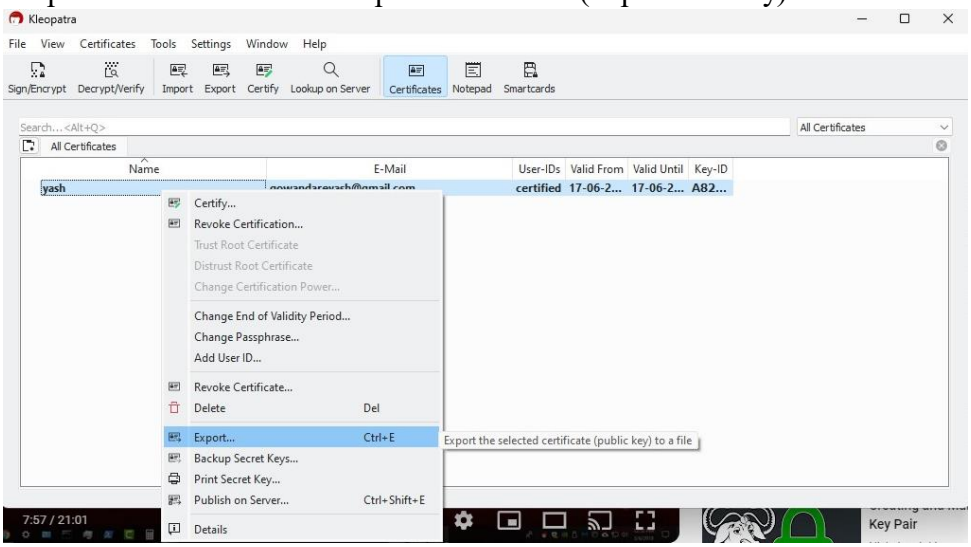


Fig. No. 14.7

8. Click on the Email field and select the "Backup Security Keys.." option from the drp down list provided. (Backup private key)

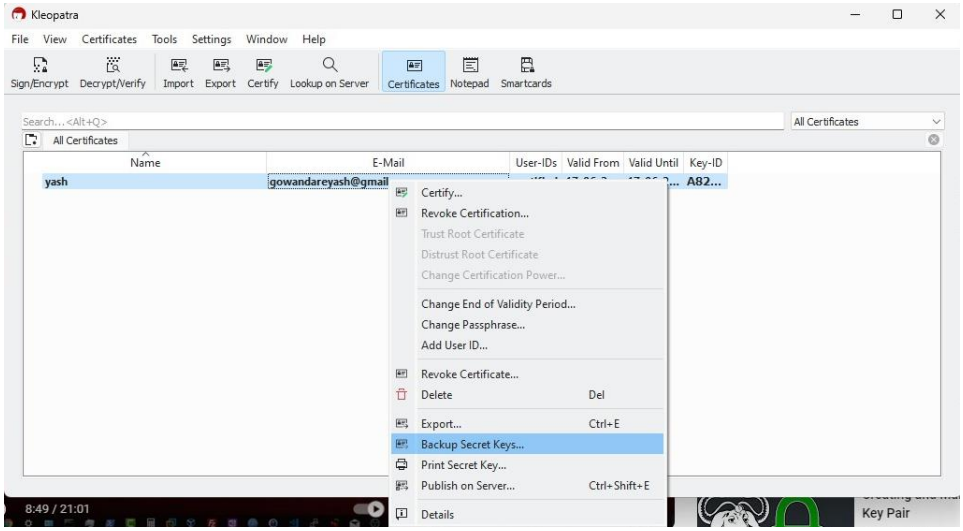


Fig. No.14.8

9. Copy the public key and paste in a new .txt file.

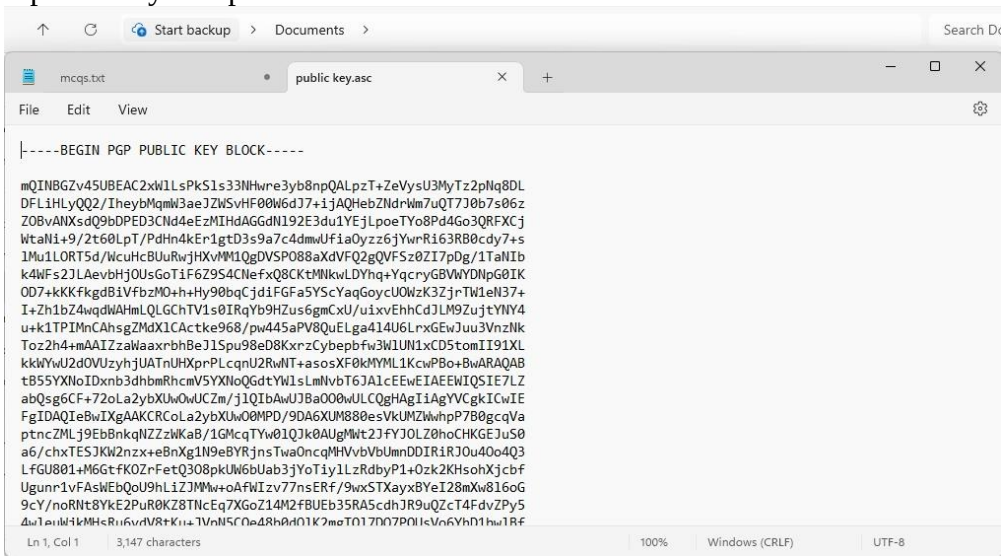


Fig. No.14.9

10. Create a demo file for encryption.

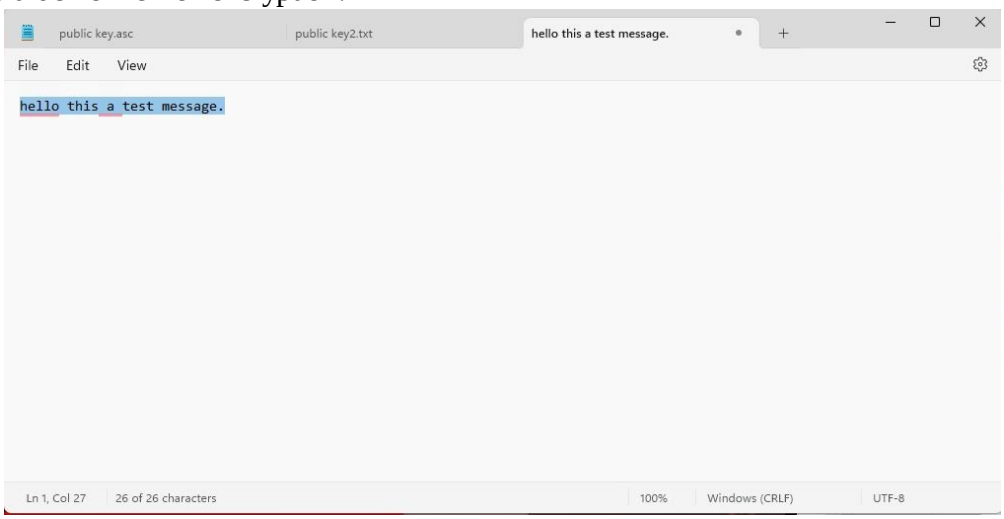


Fig. No. 14.10

11. Select the public key.

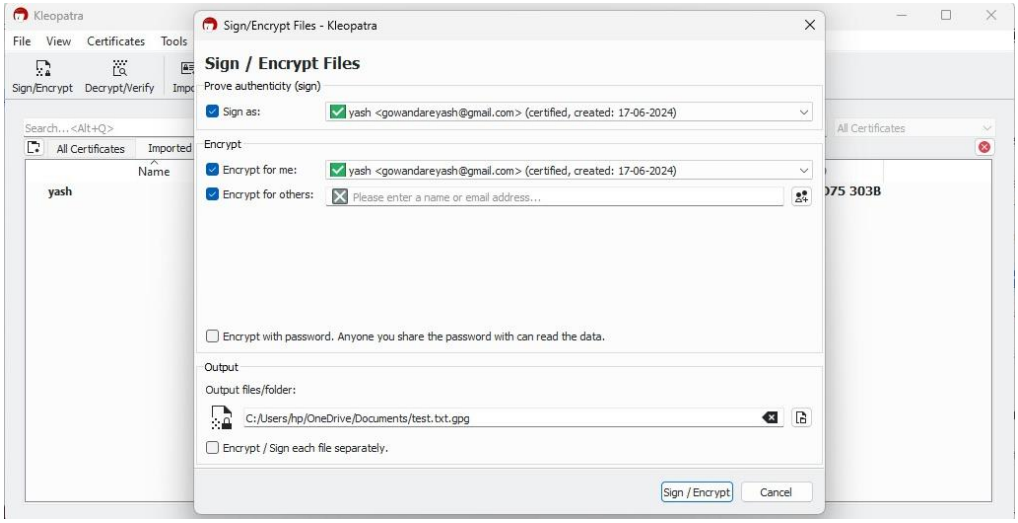


Fig. No. 14.11

12. You can also Sign as emailid from the drop down arrow. Onced you fill all the required information. Click on "Sign/Encrypt" button.

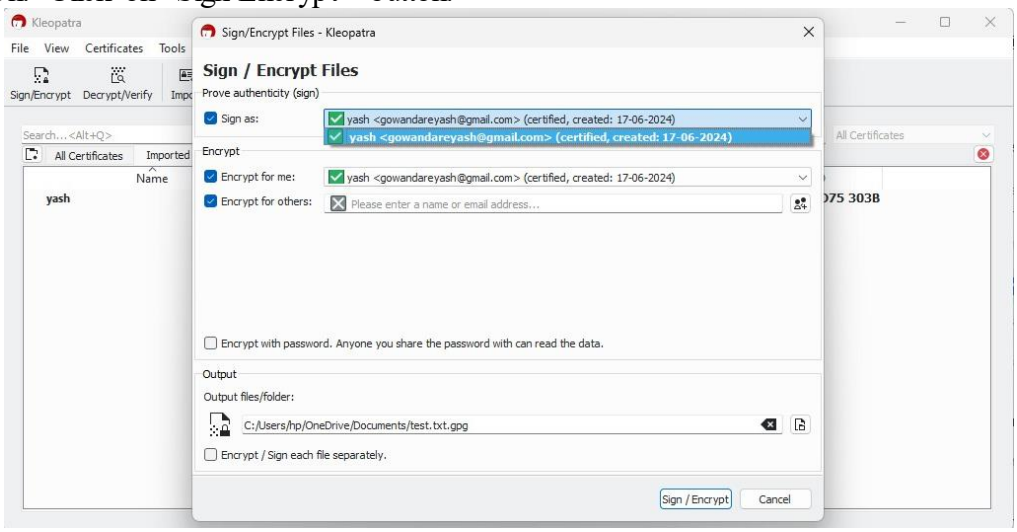


Fig. No. 14.12

13. You can select one or more certificates.

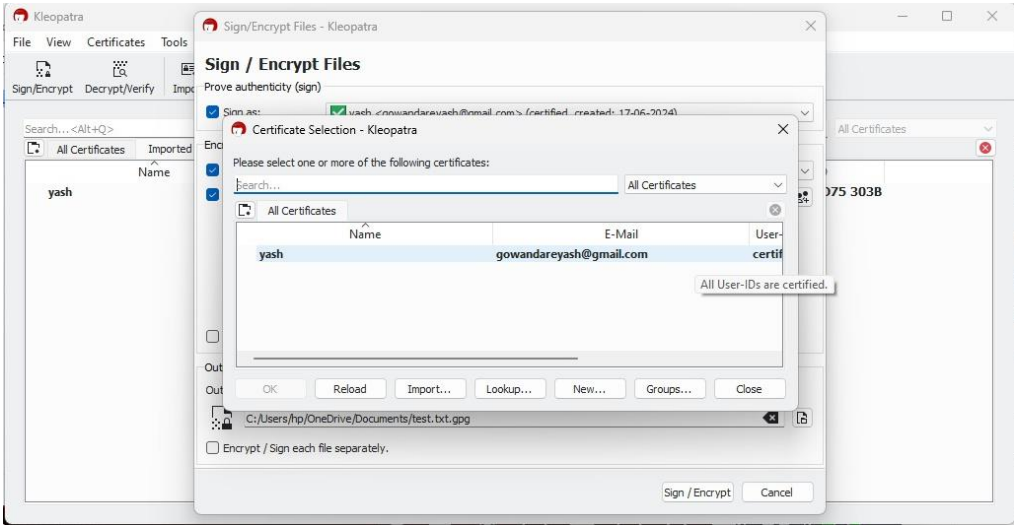


Fig. No.14.13

14. Wait for the All operations to be completed.

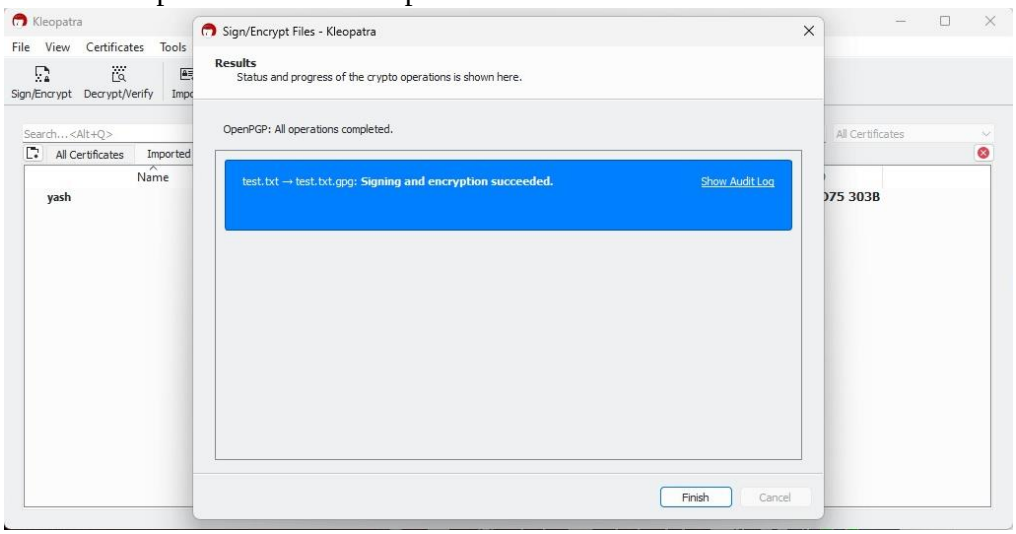


Fig. No. 14.14

15. Enter the public key password in the passpharse field.

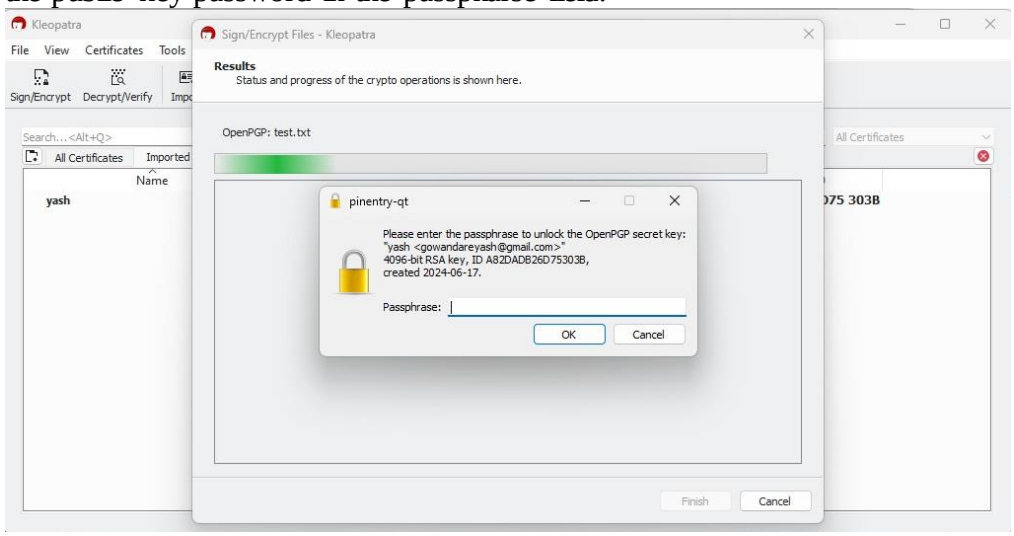


Fig. No.14.15

16. Select Decrypt as well as select the encrypted file which we have to decrypt.

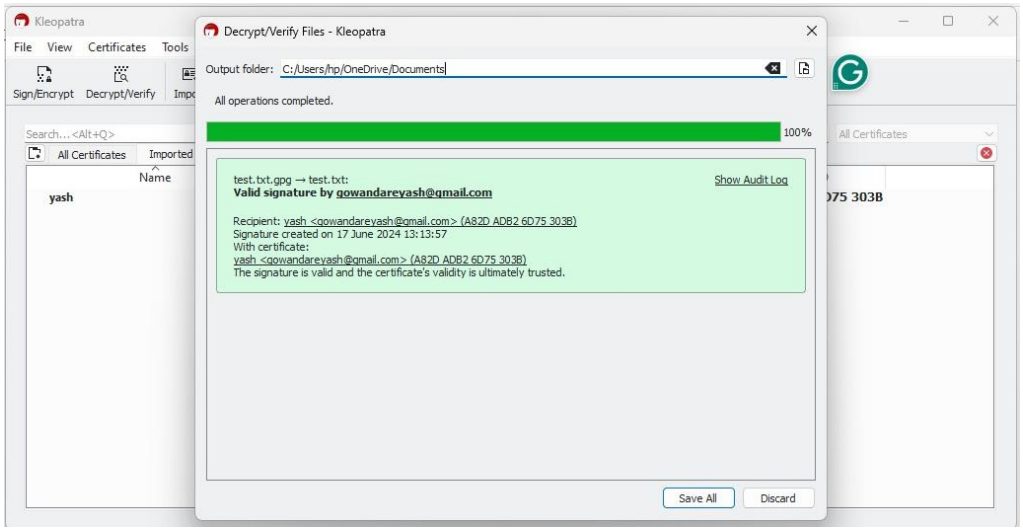


Fig. No. 14.16

17. Selection of the encryted file

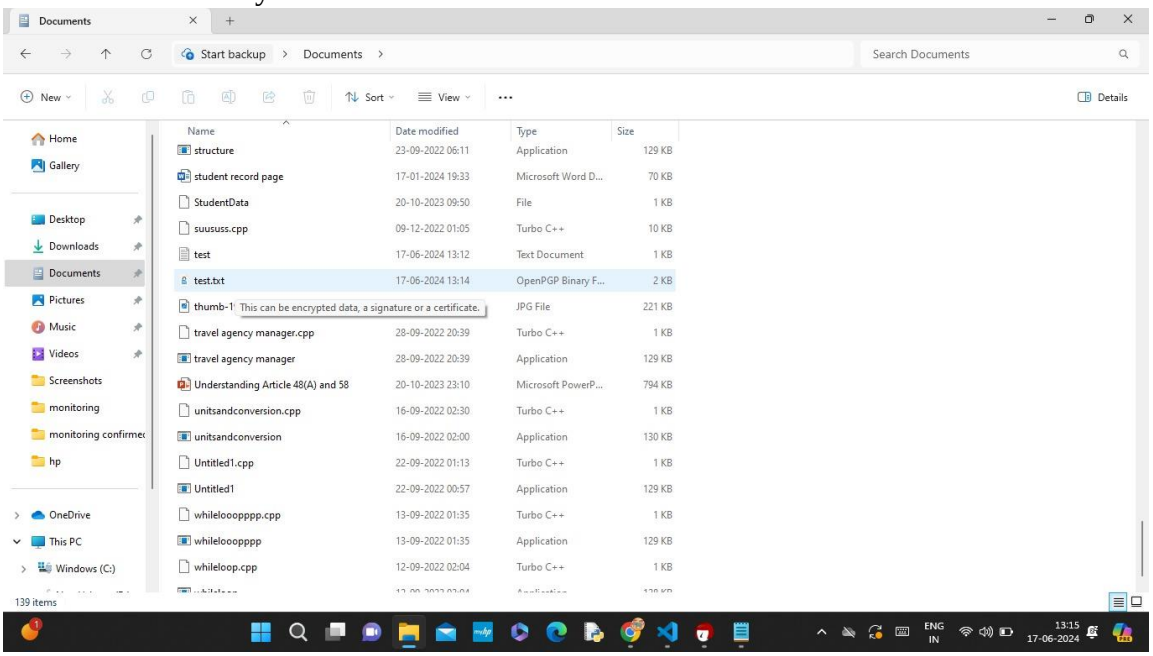


Fig. No.14.17

18. Finally we get a Decrypted message.

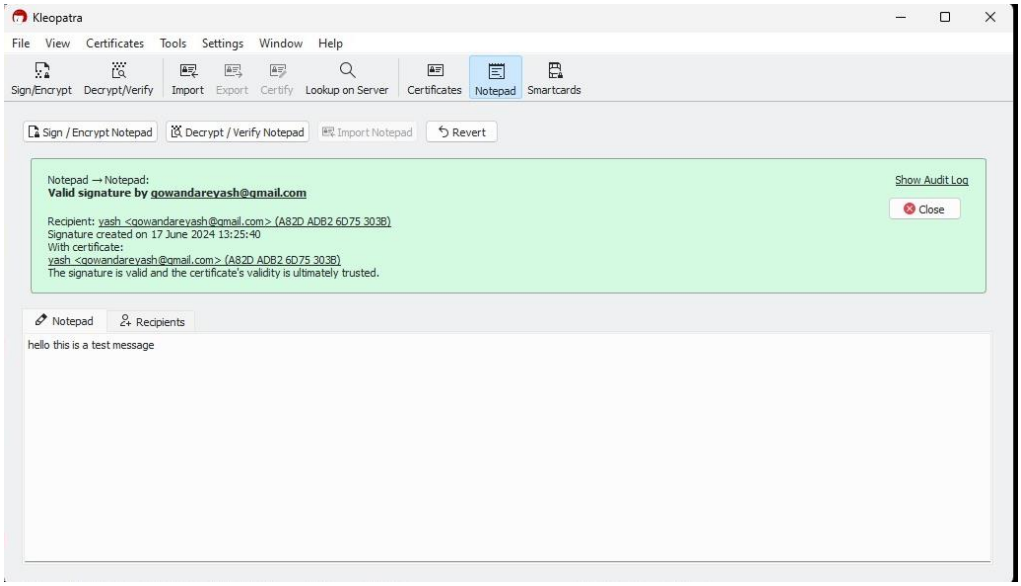


Fig. No. 14.18

X. Conclusion

……

……

……

XI. Practical Related Questions

1. Email security?
2. List types of email security techniques?
3. What is SMTP & S/MIME protocol?

Space for answer

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://www.digitalocean.com/community/tutorials/how-to-use-gpg-to-encrypt-and-sign-messages

2. https://www.fortinet.com/resources/cyberglossary/pgp-encryption

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/Output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	

Practical No.15: Set up security policies for any web browser and Email account (Example: setting filter, spam for email security. Low security apps settings, cookies, synchronization for web browser)

I. Practical Significance

- Browsers have become a gateway for security breaches. Whether it's data theft or targeted ransomware attacks, browsers are being used by cybercriminals as the point of contact to attack organizations. On noticing this trend, browser vendors are coming up with their own set of security precautions in the form of browser security settings that should be enabled to protect end users from such threats. An email security policy significantly reduces the risk of falling victim to cyber threats such as phishing, malware, and ransomware, which often enter through email systems. By setting guidelines on how to handle and secure email communications, it ensures that sensitive data remains confidential and is not exposed to unauthorized entities.

II. Industry / Employer Expected Outcome(s)

1. Implement policies and guidelines to maintain data security and privacy during data transmission.

III. Course Level Learning Outcome(s)

CO1 - Identify types of attacks which causes threat to Information Security.

CO5 - Implement security techniques to prevent internet threats.

IV. Laboratory Learning Outcome(s)

LLO 10.1 Apply browser settings.

V. Relevant Affective Domain related Outcomes

1. Follow safely practices
2. Maintain tools and equipment.
3. Follow ethical practices.

VI. Relevant Theoretical Background

Browser Security Plus offers three different sets of policies to address the above challenge. They are as follows:

1. Data Leakage Prevention
2. Threat Prevention
3. Browser Customization

Each of these policies is a collection of browser settings and configurations provided by Chrome, Internet Explorer, Edge, and Firefox browsers brought together in order to cater to specific requirements. This gives IT administrators the option to deploy security policies to different browsers in various computers as needed, all from one place. Once these settings have been configured and deployed to a computer from Browser Security Plus, end users won't be able to make changes to the settings. This ensures that recommended security settings are always enabled on the end users' computers.

- **Configurations to prevent data leakage through browsers**
  Deploy data security policy to ensure Data Leakage Prevention. You can manage passwords, disable auto fill option, ensure that users can't delete the browser history, prevent third-party cookies from being saved and so much more.
- **Configurations to prevent threats**

Threat prevention policy helps IT administrators rest assured that the computers are safe from web-based threats. IT admins can enable safe browsing for Chrome browser and Smart Screen filter for Microsoft Edge and Internet Explorer. These two settings shield users from websites containing malicious programs imbedded in them and drive-by attacks.

- **Configurations to enhance browsing experience**

Browser customizations, on the other hand, enhance the browsing experience for the end users. IT admins can enable or disable images or audio, set a desired homepage, deploy bookmarks remotely, and much more.

Optimizing your browser's settings is a critical step in using the Internet securely and privately. Today's popular browsers include built-in security features, but users often fail to optimize their browser's security settings on installation. Failing to correctly set up your browser's security features can put you at a higher risk for malware infections and malicious attacks. This installation of our "Cyber security 101" series provides our tips for securing several of today's most popular browsers, including Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer. While it is impossible to guarantee complete protection from cyber threats, following these tips will greatly increase the security of your web browser.

Tips for Secure Browsing with Google Chrome

Settings" menu or by navigating to "chrome://settings/."

- **Enable phishing and malware protection:** Make sure that Chrome's phishing and malware protection feature is enabled under the "Privacy" section. This feature will warn you if a site you're trying to visit may be phishing or contain malware.
- **Turn off instant search:** The Instant search feature should be turned off for optimal security. While it offers some convenience in searching, having this feature enabled means that anything you type in the address bar is instantly sent to Google.
- **Don't sync:** Disconnect your email account from your browser under the "Personal Stuff" tab. Syncing your email account with your Chrome browser means that personal information such as passwords, autofill data, preferences, and more is stored on Google's servers. If you must use sync, select the "Encrypt all synced data" option and create a unique passphrase for encryption.
- **Configure content settings:** Click "Content settings" under the "Privacy" section and do the following:
    - **Cookies:** Select "Keep local data only until I quit my browser" and "Block third-party cookies and site data." These options ensure that your cookies will be deleted upon quitting Chrome and that advertisers will not be able to track you using third-party cookies.
    - **JavaScript:** Select "Do not allow any site to run JavaScript." It is widely recommended that JavaScript be disabled whenever possible to protect users from its security vulnerabilities.
    - **Pop-ups:** Select "Do not allow any site to show pop-ups.
    - **Location:** Select "Do not allow any site to track my physical location."
- **Configure passwords and forms settings:** Disable Autofill and deselect "Offer to save passwords I enter on the web" under the "Passwords and forms" section. Doing so will prevent Chrome from saving your logins, passwords, and other sensitive information that you enter into forms.

VII. Required Resources

Sr. No.	Name of the Resources	Specifications	Qty
1	Computer system	Any desktop or laptop computer with basic configuration	01
2	Operating System	Windows/Linux	01
3	Software	Web Browser	01

VIII. Precaution to be followed

1. Handle Computer System with care
2. Be caution while performing files related operations in computer System

IX. Procedure

1. Email security policies:

A. Email Account :

Step 1: Open an Gmail account

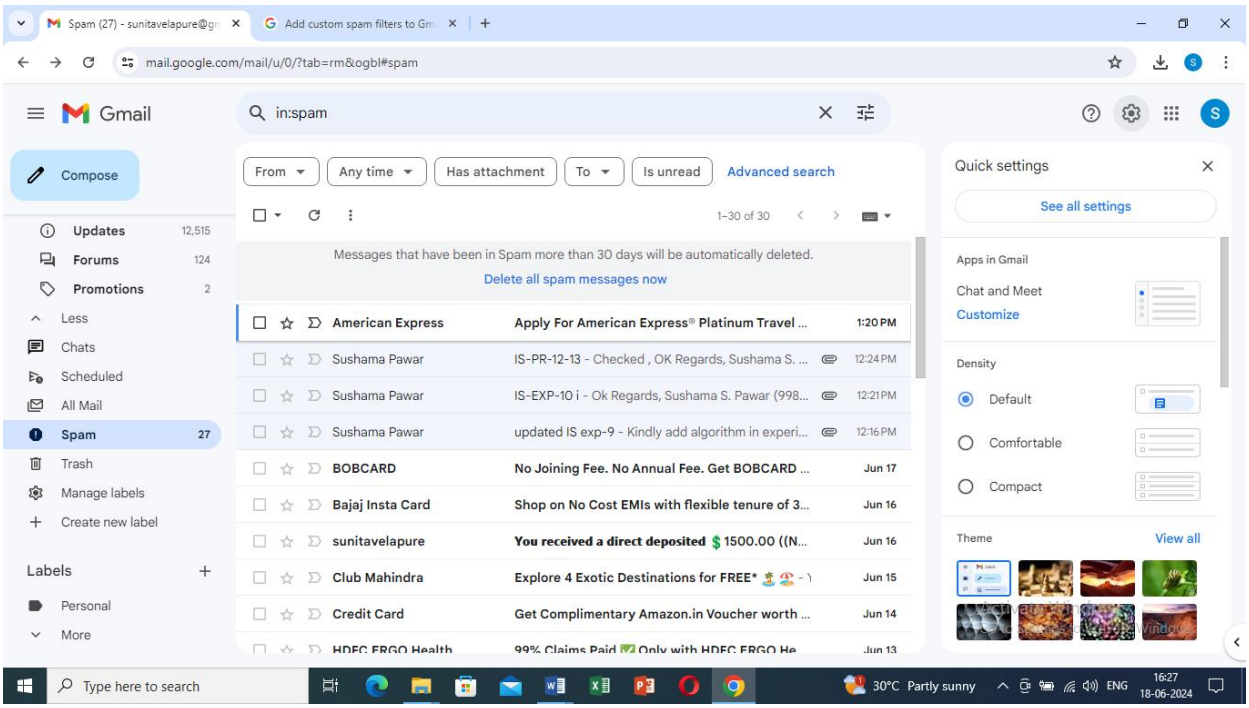


Fig. No. 15.1

Step 2: Click on settings. Click on see all settings

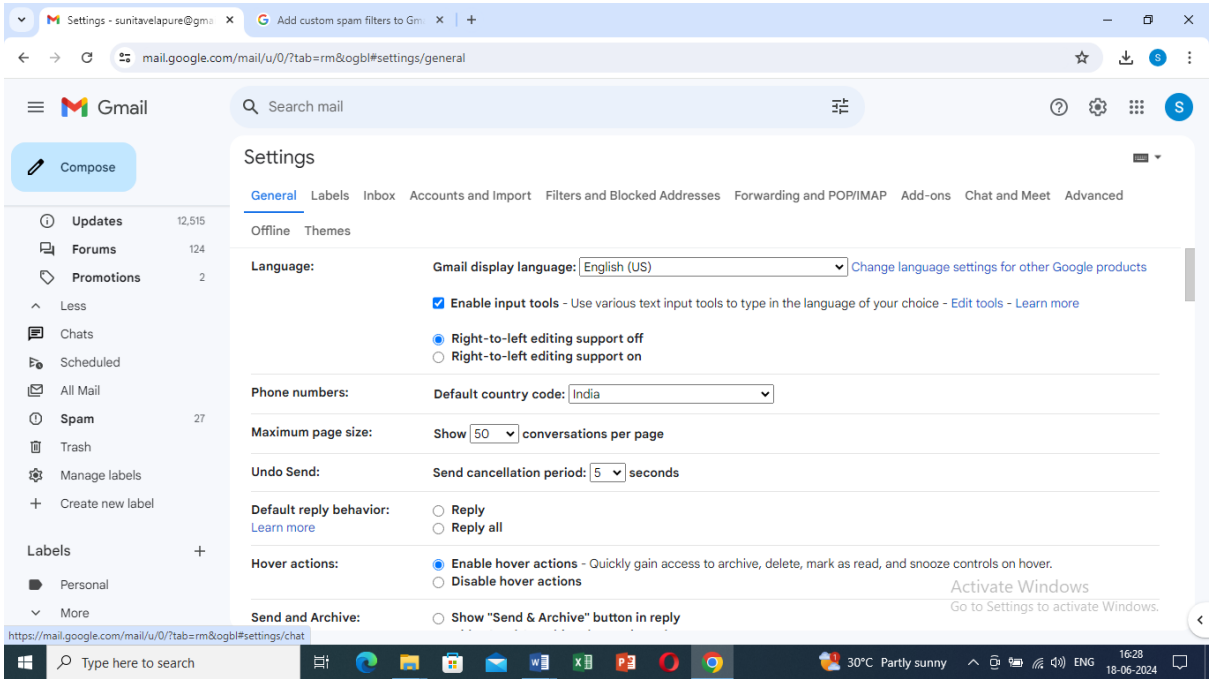


Fig. No. 15.2

Step 3: Click on filter and blocked addresses

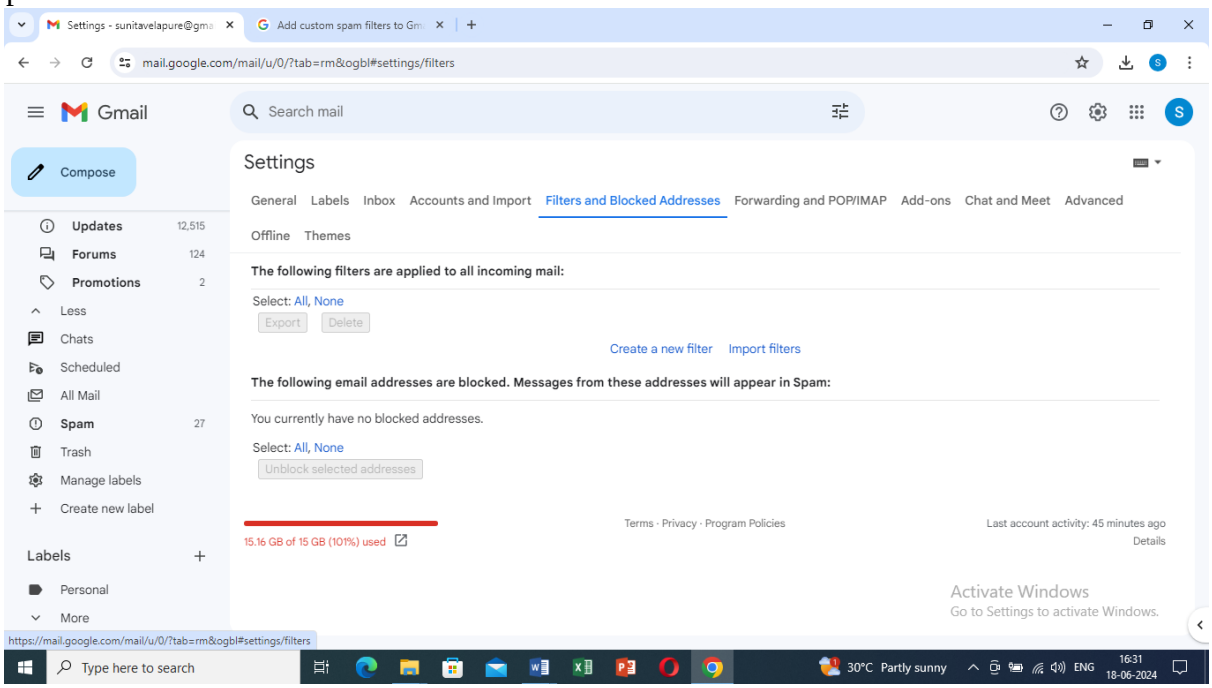


Fig. No. 15.3

Step 4: Click on create new filter.

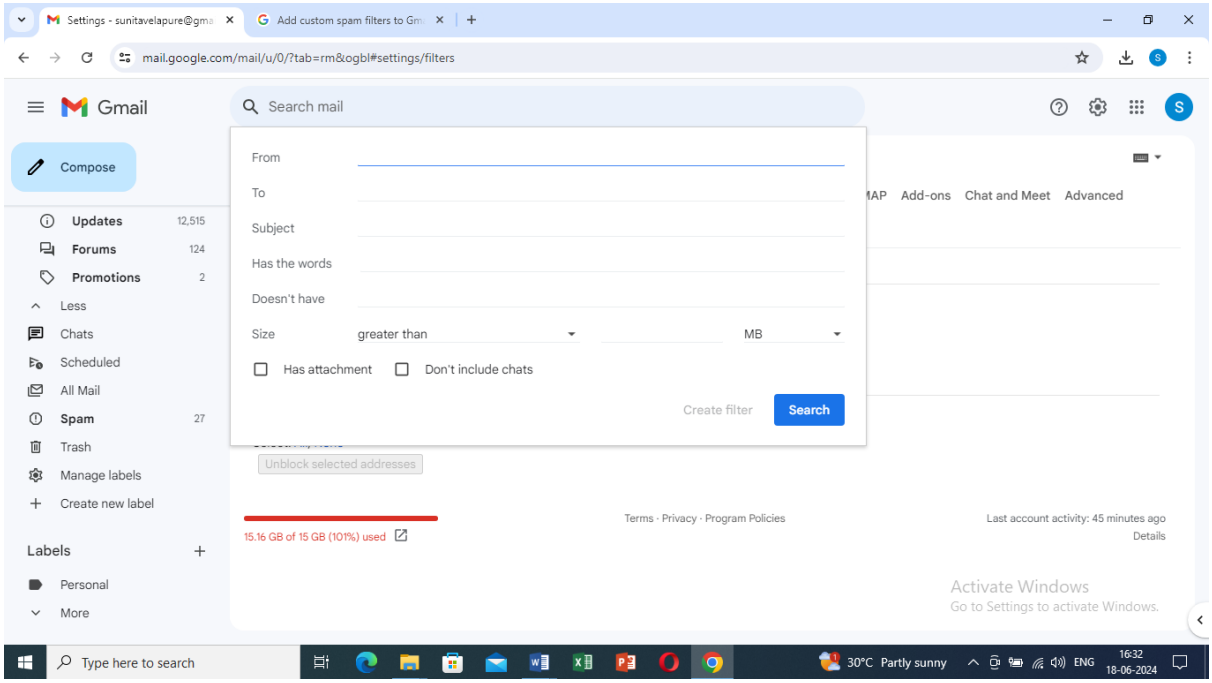


Fig. No. 15.4

Step 5: You can also change labels in settings option.

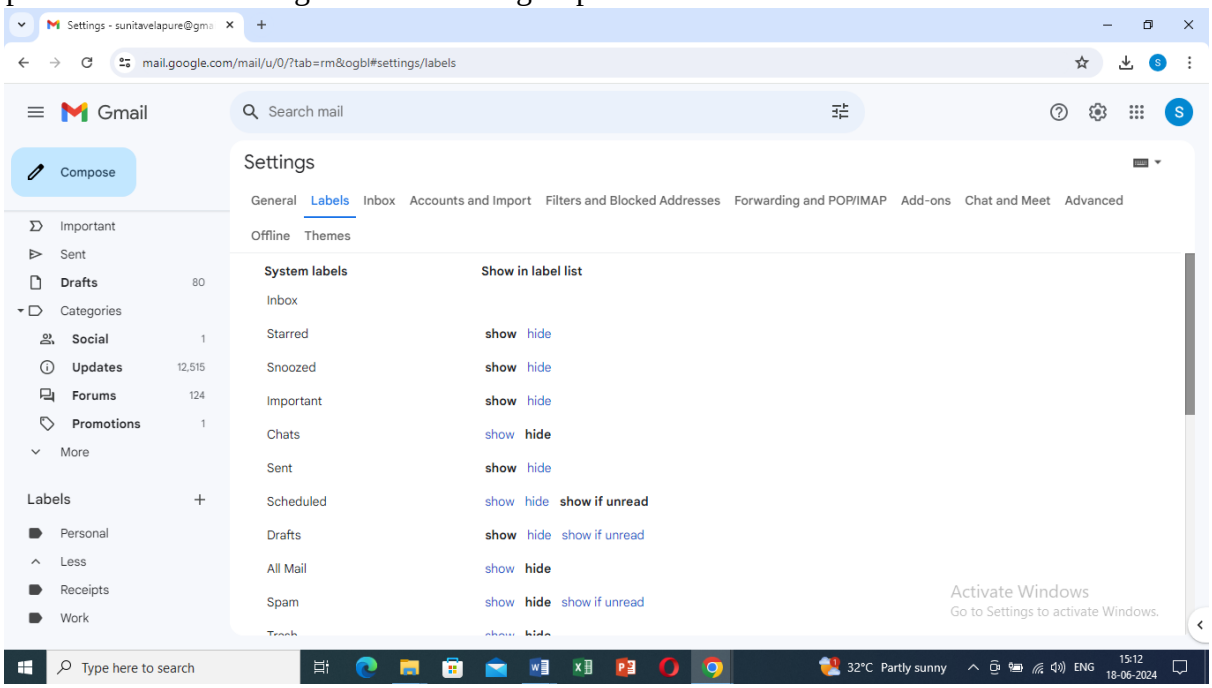


Fig. No. 15.5

B. Spam mail: Add custom spam filters to Gmail

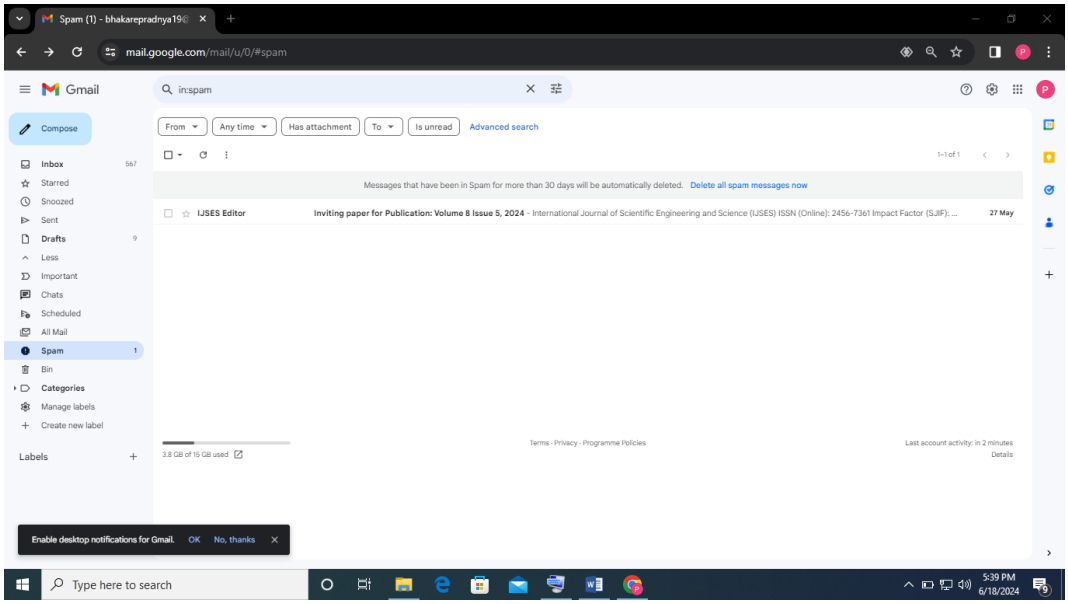


Fig. No. 15.6

Customize Gmail's default spam filtering for Google Workspace. *This article is for administrators. If you're using Gmail, learn how to* mark or unmark spam in your Gmail account. By default, Gmail scans all email messages for spam. When Gmail detects a spam message, the message is delivered to the recipient's spam folder. You can't turn off Gmail's spam scanning. However, you can use the **Spam** setting to create spam filters to customize Gmail's spam scanning behavior.

You can set up custom spam filters so that:

- Messages from senders on an approved senders list aren't marked as spam.
- Messages from senders in your domains aren't marked as spam.
- Spam messages are put in quarantine, so you can review them before they're delivered to recipients.
- Messages from bulk senders are scanned more closely for spam.

2. Browser Settings:

A. Change your cookie settings

1. On your computer, open **Chrome**.
2. At the top right, click More **Settings**.

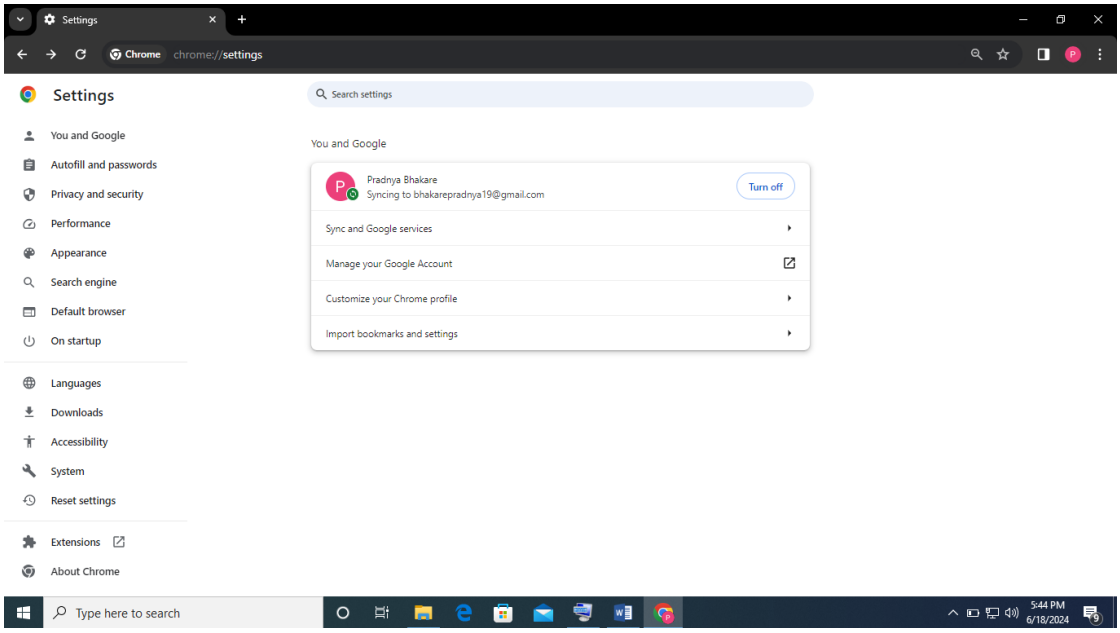


Fig. No. 15.7

3. Click Privacy and security. Third-party **cookies**. Tip: If you are part of the Tracking Protection test group, follow the "Tracking Protection" instructions instead.

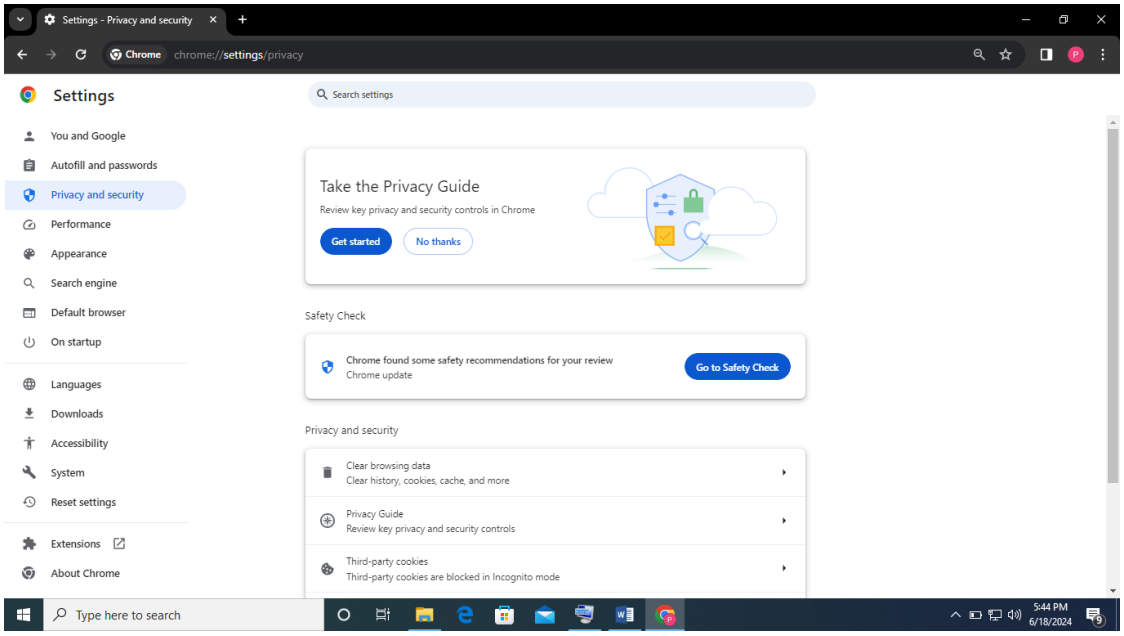


Fig. No. 15.8

4. Select an option: Allow third-party **cookies**.

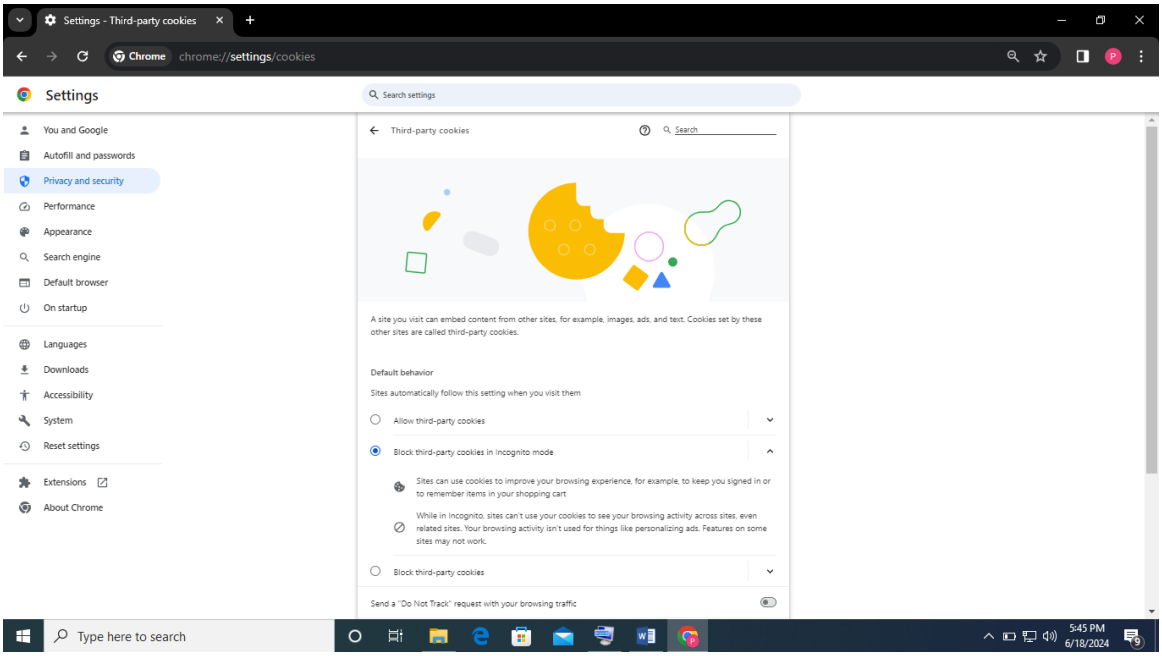


Fig. No. 15.9

You can also achieve this by:

Click on the chrome menu (the three dots at the top right). Select settings. Under the Privacy and security section click the Cookies and other site data. In the General settings section you are able to change the settings, such as allow all cookies, block third-party cookies or block all cookies.

B. Less security app settings in web browser.

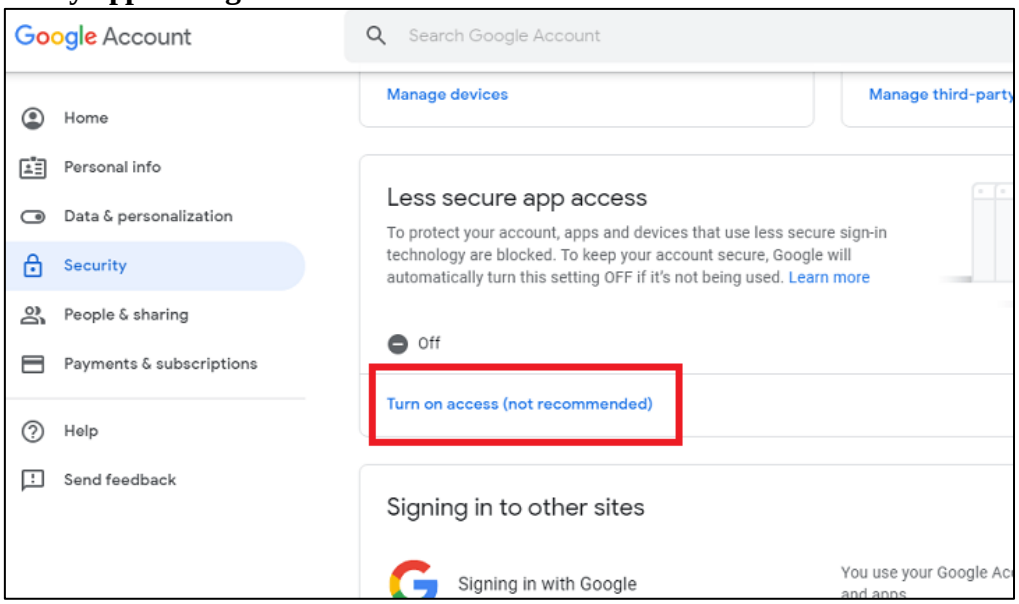


Fig. No. 15.10

Manage access to less secure apps

1. Sign in to your Google Admin console. ...
2. In the Admin console, go to Menu Security Access and data control. ...
3. (Optional) To apply the setting only to some users, at the side, select an organizational unit (often used for departments) or configuring group (advanced).

C. To manage a user's access to less secure apps

You can allow users to turn on or off access to less secure apps or disable their access to less secure apps.

1. Sign in to your Google Admin console.
2. Sign in using an *administrator account*, not your current account adityachavan@gmail.com
3. In the Admin console, go to Menu **Security Access and data control less secure apps**.
4. (Optional) to apply the setting only to some users, at the side, select an **organizational unit** (often used for departments) or configuration **group** (advanced).

D. Group settings override organizational units.

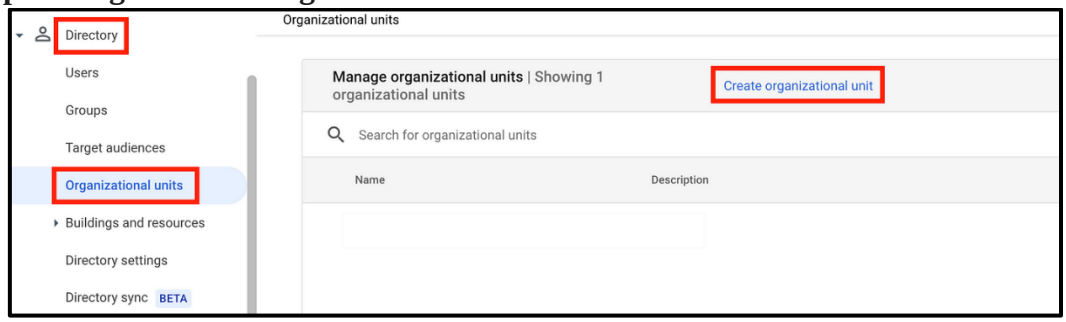


Fig. No. 15.11

1. Select the setting for less secure apps:
   - **Disable access to less secure apps (Recommended)**: Users can't turn on access to less secure apps. If you select this option while a less secure app already has an open connection with a user account, the app will time out when it tries to refresh the connection. Timeout periods vary per app.
   - **Allow users to manage their access to less secure apps**: Users can turn on or off access to less secure apps.
2. Click **Save.** Or, you might click **Override** for an organizational unit.
3. To later restore the inherited value, click **Inherit**.

E. Synchronization for web browser

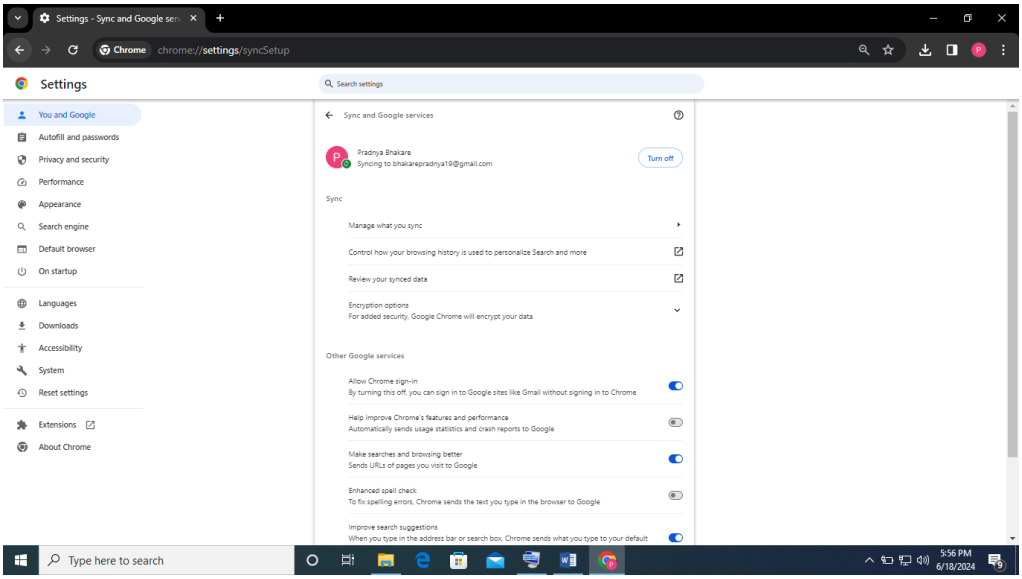


Fig. No. 15.12

Choose what info is synced

1. On a trusted computer, open Google **Chrome web browser**.

2. At **the** top right, click more. **Settings**.
3. Under "You and Google," click **Sync** and Google services. ...
4. Under "**Sync**," click Manage what you **sync**.
5. Turn off "**Sync** everything."
6. Turn off any data you don't want synced to **your** account.
7. On the top right-hand menu of Google Chrome, open the menu and select Settings.
8. If you have not signed into your Google account, select "Turn on sync..." and sign in when prompted.
9. Once signed in, any bookmarks and settings should automatically sync. ...
10. Select "Manage what you sync.

X. Conclusion

……

……

……

XI. Practical Related Questions

1. Explain Cookies and enlist its types.
2. Explain the different types of cyber-attacks that can target web browsers.

Space for answer

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

XII. References/Suggestions for further reading

1. https://www.manageengine.com/browser-security/policy-deployment.html
2. https://youtu.be/Q8dfVHPvG0?si=t1efndZ0u5wPkqb-

XIII. Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Correctness of flow of procedure	
2.	Debugging ability	
3.	Quality of Input/output displayed.(messaging and formatting)	
	Weightage- Product related: 40%	**Marks-10**
4.	Answer to sample questions	
5.	Submission of assignment on time.	
	Total 25	
	Dated Signature of Course Teacher	