

### DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

**A**

**MINI PROJECT REPORT**

ON

**“Data Encryption and Decryption System Java Project ”**

Submitted in the partial fulfillment of the requirements in the 4th semester of

### BACHELOR OF ENGINEERING IN

**INFORMATION SCIENCE AND ENGINEERING**

BY

### DHRUV GULATI 1NH18IS031

***Under the guidance of***

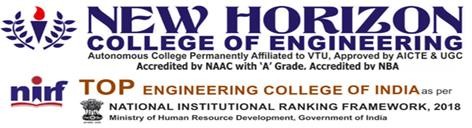
### Mrs. Ms.Rafega Beham

Assistant Professor, Dept. of ISE, NHCE

### DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING NEW HORIZON COLLEGE OF ENGINEERING

(Autonomous College Permanently Affiliated to VTU, Approved by AICTE, Accredited by NBA & NAAC with ‘A’ Grade)

Ring Road, Bellandur Post, Near Marathalli, Bangalore-560103, INDIA



# CERTIFICATE

Certified that the project work entitled “**Data Encryption and Decryption System Java Project *”***carried out by Mr.DHRUV GUALTI, USN 1NH18IS031, a bonafide student of 4th sem in partial fulfillment for the award of Bachelor of Engineering in Information Science and Engineering of the Visveswaraiah Technological University, Belgaum during the year 2019-2020. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated.The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said Degree.

Signature of the Guide Signature of the HOD Signature of the Principal

Mrs. Ms.Rafega Dr. R.J Anandhi Dr.Manjunatha

Data Encryption and Decryption System Java Project

ORIGINALITY REPORT

20%

SIMILARITY INDEX

## %

INTERNET SOURCES

20%

PUBLICATIONS

## %

STUDENT PAPERS

PRIMARY SOURCES

# 1 O.O. Khalifa, M.D.R. Islam, S. Khan, M.S. Shebani. "Communications cryptography", 2004 RF and Microwave Conference (IEEE Cat.

5%

No.04EX924), 2004

Publication

3%

# 2 T. R. Devi. "Importance of Cryptography in Network Security", 2013 International Conference on Communication Systems and Network Technologies, 2013

Publication

2%

# 3 "The Attitudes and Events Leading To American Involvement In World War I", AS and A Level/History/International History, 1945-1991,

2005-06-06

Publication

1%

# 4 Ioannis Kostaras, Constantin Drabo, Josh Juneau, Sven Reimers, Mario Schröder, Geertjan Wielenga. "Pro Apache NetBeans", Springer Science and Business Media LLC, 2020

Publication

# 5 Neha Gupta, Nidhi Sharma. "Dwt and Lsb based Audio Steganography", 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), 2014

1%

Publication

1%

# 6 Jan Schäfer, Arnd Poetzsch-Heffter. "Writing concurrent desktop applications in an actor- based programming model", Proceedings of the 3rd International Workshop on Multicore Software Engineering - IWMSE '10, 2010

Publication

1%

# 7 György Kovács, Zoltán Varga, Márk Mihalik. "Chapter 35 Optimal Formation of Logistics Networks", Springer Science and Business Media LLC, 2017

Publication

1%

# 8 "Grundlegende Algorithmen mit Java", Springer Science and Business Media LLC, 2008

Publication

1%

# 9 "Security and Authentication through Text Encryption and Decryption based on Substitution Method", International Journal of Innovative Technology and Exploring Engineering, 2019

Publication

1%

# Kessler, Gary. "An Overview of Cryptographic Methods", Best Practices, 2000.

Publication

# Joyanes Aguilar, Luis, and María Luisa Díez Platas. "Appendix D : Java Language Guide", Handbook of Object Technology, 1998.

Publication

# Sara Capotosti, Martina Scacco, Luca Nelli, Giacomo Dell'Omo, Michele Panuccio. "Hypatia- trackRadar: A software for animal tracking using marine surveillance radars", Ecological Informatics, 2019

Publication

# Vaskaran Sarcar. "Interactive Object-Oriented Programming in Java", Springer Science and Business Media LLC, 2020

Publication

# Altaf T. Shah, Vikramsingh R. Parihar. "Overview and an approach for QR-code based messaging and file sharing on android platform in view of security", 2017 International Conference on Computing Methodologies and Communication (ICCMC), 2017

Publication

# "Pro Java Programming", Springer Science and Business Media LLC, 2005

Publication

# Vaskaran Sarcar. "Interactive C#", Springer Science and Business Media LLC, 2018

1%

1%

<1%

<1%

<1%

<1%

Publication

# Xiaozhen Xue, Yulei Pang, Akbar Siami Namin. "Feature Selections for Effectively Localizing Faulty Events in GUI Applications", 2014 13th International Conference on Machine Learning and Applications, 2014

Publication

# Brahma Dathan, Sarnath Ramnath. "Object- Oriented Analysis, Design and Implementation", Springer Science and Business Media LLC, 2015

Publication

# Alvaro Camarillo, José Ríos, Klaus-Dieter Althoff. "Chapter 18 PLM Applied to Manufacturing Problem Solving: A Case Study at Exide Technologies", Springer Science and Business Media LLC, 2019

Publication

# Talukder, . "Java Client-Side Security", Architecting Secure Software Systems, 2008.

Publication

# "Automated Software Design Reusability using a Unique Machine Learning Technique", International Journal of Innovative Technology and Exploring Engineering, 2020

Publication

# Chenggang Zhen, Peng Cheng. "Analysis the

<1%

<1%

<1%

<1%

<1%

# development and security policy of third-party online payment platform", 2010 3rd International Conference on Computer Science and Information Technology, 2010

Publication

# Bill Buchanan. "Handbook of Data Communications and Networks", Springer Nature, 1999

Publication

# "Novel Algorithms and Techniques In Telecommunications, Automation and Industrial Electronics", Springer Science and Business Media LLC, 2008

Publication

<1%

<1%

<1%

Exclude quotes: Off Exclude matches Off

Exclude bibliography: On

## Abstract:

The main idea of **Data Encryption and Decryption System Java Project** is to provide the secured communication between various clients in the network. The Data Encryption and Decryption System is software, which tries to alter the originality of the text into some encrypted form. The major task is to provide the user the flexibility.

In this project we use cryptography techniques for encryption and decryption of message. While transmitting packet from source to destination we encrypt packet and transmit the packet at the receiving side decryption is done using a key that is only available to the user. When there is any data hacking at the middle of the network it is not possible to decrypt the packet.

Data encryption translates data into the other form, or code so that only people with access to the password can use it. Encrypted data is also known as cipher text. Encryption is one of the most popular and effective data security method

.The purpose of this code is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks. The above project provides confidentiality ad drive key security initiatives including authentication, integrity and non –repudiation. Authentication allows for the verification of a message’s origin. Integrity provides proof that the message’s content has not been changed from the sent time. Non repudiation ensures that a message sender cannot deny sending the message.

Data Encryption system project is implemented in Java Platform. We use java because it is one of the mostly used software all over the world. Java provide Serve let concept and may other feature.

# ACKNOWLEDGEMENT

Any achievement, be it scholastic or otherwise does not depend solely on the individual efforts but on the guidance, encouragement and cooperation of intellectuals, elders and friends. A number of personalities, in their own capacities have helped me in carrying out this project. I would like to take an opportunity to thank them all.

First and foremost I thank the management, **Dr. Mohan Manghnani,** Chairman, New Horizon Educational Institutions for providing necessary infrastructure and creating good environment.

I would like to thank **Dr.Manjunatha**, Principal, New Horizon College of Engineering, Bengaluru, for his constant encouragement and facilities extended to us towards completing my project work.

I extend my sincere gratitude to **Dr. R J Anandhi**, Head of the Department, Information Science and Engineering, New Horizon College of Engineering, Bengaluru for her valuable suggestions and expert advice.

I deeply express my sincere gratitude to my guide **Mrs.Rafega Beham, Assistant Professor**, Department of ISE, NHCE, Bengaluru, for her able guidance, regular source of encouragement and assistance throughout this project.

I thank my Parents, and all Faculty members of Department of Information Science and Engineering for their constant support and encouragement.

Last, but not the least, I would like to thank my peers and friends who provided me with valuable suggestions to improve my project.

**DHRUV GULATI 1NH18IS031**

|  |  |  |
| --- | --- | --- |
| **CONTENT** |  |  |
| **Cover page Certificate Acknowledgment Abstract** | **i ii iii 2** |
| **CHAPTER 1 BREIF INTRODUCTION ABOUT THE HISTORY** | **3-7** |
| 1.1 Introduction | 3 |
| 1.2 History | 3 |
| 1.3 Purpose of Cryptography | 3 |
| 1.4 Objective | 4 |
| 1.5 Scope | 5 |
| 1.6 Theoretical Background | 5 |
| 1.7 Feasibility Study | 5 |
| 1.8 Application of Cryptography | 6 |
| 1.9 Problem Defination | 7 |
| 1.10 Software Required | 7 |
| 1.11 Hardware Required | 7 |
| **CHAPTER 2 CONCEPTS USED IN PROJECT** |  | **9-10** |
| **CHAPTER 3 OBJECT ORIENTED CONCEPTS** |  | **11-16** |
| **CHAPTER 4 SOURCE CODE AND SNAPSHOTS** |  | **16-24** |
| **CHAPTER 5 CONCLUSION AND REFERENCES** |  | **25-26** |

**CHAPTER 1**

**BRIEF INTRODUCTION TO PROJECT**

* 1. **Introduction:**

Cryptography in greek means: *kryptos – “*secret”*; graphos – “*writing”. It is an art and science of preparing coded or secured communications. The enciphering process usually involves an algorithm and a key. An encryption algorithm is a particular method of scrambling—a computer program or a written set of instructions. The key specifies the actual scrambling process. The original communication may be a written or broadcast message or a set of digital data. One essential aspect for secure communications is that of cryptography, which is the focus of this presentation. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient.

* 1. **History:**

The first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to wartime battle plans. A more recent example can be seen during WORLD WAR - 1 : Before the United States entered World War I, the German government tried to provoke a war between the United States and Mexico. On January 19, 1917, the German foreign secretary, Arthur Zimmermann, sent an encoded telegram to his diplomatic representatives in Mexico, asking them to propose a secret alliance with the Mexican government. But British intelligence officers intercepted and quickly decoded the message, sending it on to President Woodrow Wilson. A huge public outcry ultimately resulted in an American declaration of war against Germany.

It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications.

## The purpose of Cryptography

In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

Authentication*:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or addressbased, both of which are notoriously weak.)

Privacy/confidentiality*:* Ensuring that no one can read the message except the intended receiver.

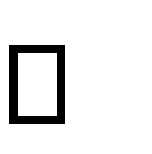
Integrity*:* Assuring the receiver that the received message has not been altered in any way from the original.

Non-repudiation*:* A mechanism to prove that the sender really sent this message. As, stated above PRIVACY and authentication are of utmost importance today, due to the presence of innumerable HACKERS, and due to the fact that the entire world is becoming a global village .Thanks to the technology , today right from bank transactions to matrimony all take place in a fraction of a second with the help of internet.

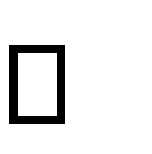
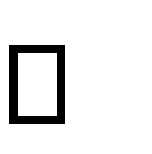
Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication, without which the entire computer community would collapse.

## Objective

The main objective of our project is to encrypt/decrypt the textual files for personal and professional security. Encryption and Decryption protects privacy of our email messages, documents and sensitive files by encrypting them using RSA algorithm to provide high protection against unauthorized data access. Every day hundreds and thousands of people interact electronically, whether it is through emails, e-commerce, etc. through internet. The Internet is comprised of millions of interconnected communication and transfer of information around the world. People use emails to correspond with one another .The www is used for online business, data distribution, marketing, research, learning and a myriad of other activities. Sending sensitive messages over the Internet is very dangerous as all emails are transmitted in an unsecured form and anybody - ISP, your boss, etc. can read your emails. If you want to send sensitive information via email, simply paste the encrypted text into your email or attach the encrypted file, all the recipient has to do is decrypt your text or file. Encryption and Decryption works with text information and files. Just select what you want to encrypt, and Encryption and Decryption software helps you keep documents, private information and files in a confidential way.

* 1. **Scope:** The scope of our project is presently specific. Both the sender and the receiver must have this software installed on their systems to encrypt/decrypt and compress/decompress the files transmitted between them. This includes all the users who want to interact electronically, whether it is through emails, ecommerce, etc. through internet in order to keep their private information confidential.

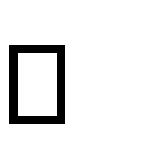
Each step is clearly stated and user will not face any ambiguity in using the software.



The software provides clarity in its functionality even to naïve users. No complexity is involved.

## Theoretical background :

### The Existing System

As observed the current encryption/decryption softwares doing the encryption and decryption task are all very complicated in their functionality. The method of encryption/decryption and key generation of current system for a new user to understand is complex in nature.

### The Proposed System

The proposed system is quiet simple to use. It is not complex in its functionalities. It is easy for a naïve user to use it. If you want to send sensitive information via email, simply paste the encrypted text into your email or attach the encrypted file, all the recipient has to do is to decrypt your text or file.Encryption and Decryption works with text information and files. Just select what you want to encrypt, and Encryption and Decryption software helps you keep documents, private information and files in a confidential way.

## FEASIBILITY STUDY:

After investigation it is essential to determine whether the project is feasible or not. In feasibility study is tested whether the system to be developed would be able to accomplish its task on the working grounds. Its impact was also found to be not adverse. It was found that the user’s requirements would be met and the resources would be used in an effective manner. In feasibility study the important aspects related to the project were considered like the problem definition and the process for solution. The cost and benefit analysis was also done.

**Feasibility Considerations** :To do a feasibility study, the economic, technical and behavioral factors in the system development were considered. The three key considerations were as follows:

* + 1. Economic Feasibility: The project developed, Encryption and Decryption was within budget and producing the desired results. The labour or the human ware consisted of the three group members of our project. The output consisted of getting the desired results. Thus with the consideration of the inputs, the outputs were achieved successfully. The project was within limit. The inputs didn’t overdo the outputs.
    2. Technical Feasibility: Technical feasibility revolves around the technical support of the project. The main infrastructure of the project included the project labs in the college campus. The systems there were easily able to absorb the new s/w being installed. The project thus was technically feasible. The equipment and the s/w produced no problem. The project’s technical requirements were met. The project could be made to work correctly, fulfilling its task, with the existing s/w and personnel.
    3. Operational Feasibility: Operational Feasibility aims to determine the impact of the system on the users. The system developing has an influence on its users. Our system “Encryption and Decryption” was new for them but it was simple enough for any naïve person to understand. The evolution of this new system required no special training for the users. Encryption and Decryption was found to be feasible in this regard. The system developed would be user friendly and no complexities would be involved in its functionalities.

## Applications Of Cryptography:

1. Defense Services
2. Secure Data Manipulation
3. E –Commerce
4. Business Transactions
5. Internet Payment Systems
6. Pass Phrasing
7. Secure Internet Comm.
8. User Identification Systems
9. Access Control

10.Computational Security

11. Secure access to Corp Data

12.Data Security.

## PROBLEM DEFINITION

### Project Mission

The aim of our project is to develop software named ENCRYPTION AND DECRYPTION.The project encrypts and decrypts the textual files to maintain the security and integrity of data and information and toprovide high protection against unauthorized data access.

### Target:

Our target is the common man who wants to interact electronically, whether it is through emails, e-commerce, etc.through internet.Sending sensitive messages over the Internet is very dangerous.So,our project helps him to interact in a safe and secure manner in order to keep their private information confidential.

### Target Users:

The main target users of our project are the people who transmit confidential information via emails or through internet.

### Scope and Key Elements:

The scope of our project is presently specific.Both the sender and the receiver must have this software installed on their systems to encrypt/decrypt and compress/decompressthe files transmitted between them.This includes all the users who want to interact electronically, whether it is through emails, ecommerce, etc.through internet in order to keep their private information confidential.

## Software Requirements:

1.Windows 10 2.JDK

3.Eclipse Java Oxygen**:** Eclipse is an [integrated development environment](https://en.wikipedia.org/wiki/Integrated_development_environment) (IDE) used in [computer programming,](https://en.wikipedia.org/wiki/Computer_programming) and is the most widely used Java IDE.[[6]](https://en.wikipedia.org/wiki/Eclipse_(software)#cite_note-6) It contains a base [workspace](https://en.wikipedia.org/wiki/Workspace) and an extensible [plug-in](https://en.wikipedia.org/wiki/Plug-in_(computing)) system for customizing the environment. Eclipse is written mostly in [Java](https://en.wikipedia.org/wiki/Java_(programming_language)) and its primary use is for developing Java applications, but it may also be used to develop applications in other [programming languages](https://en.wikipedia.org/wiki/Programming_language) via plug-ins

## Hardware Requirements:

* Intel Pentium 4 or above
* Floppy-Drive
* CD-ROM drive
* 10 GB of free hard-disk
* keyboard and mouse
* RAM(minimum 512 MB)

## CHAPTER 2 CONCEPTS USED IN PROJECT

1. **Swing** is a [GUI](https://en.wikipedia.org/wiki/Graphical_user_interface) [widget toolkit](https://en.wikipedia.org/wiki/Widget_toolkit) for [Java.](https://en.wikipedia.org/wiki/Java_(programming_language)) It is part of [Oracle'](https://en.wikipedia.org/wiki/Oracle_Corporation)s [Java Foundation Classes](https://en.wikipedia.org/wiki/Java_Foundation_Classes) (JFC) – an [API](https://en.wikipedia.org/wiki/Application_programming_interface) for providing a [graphical user interface](https://en.wikipedia.org/wiki/Graphical_user_interface) (GUI) for Java programs.

Swing was developed to provide a more sophisticated set of GUI [components](https://en.wikipedia.org/wiki/Software_component) than the earlier [Abstract Window Toolkit (AWT).](https://en.wikipedia.org/wiki/Abstract_Window_Toolkit) Swing provides a [look and feel](https://en.wikipedia.org/wiki/Look_and_feel) that emulates the look and feel of several platforms, and also supports a [pluggable](https://en.wikipedia.org/wiki/Pluggable_look_and_feel) [look and feelt](https://en.wikipedia.org/wiki/Pluggable_look_and_feel)hat allows applications to have a look and feel unrelated to the underlying platform. It has more powerful and flexible components than AWT. In addition to familiar components such as buttons, check boxes and labels, Swing provides several advanced components such as tabbed panel, scroll panes, trees, tables, and lists.

Unlike AWT components, Swing components are not implemented by platformspecific code. Instead, they are written entirely in Java and therefore are platformindependent. The term "lightweight" is used to describe such an element.

Swing is a platform-independent, "[model-view-controller"](https://en.wikipedia.org/wiki/Model-view-controller) [GUI](https://en.wikipedia.org/wiki/GUI) framework for Java, which follows a single[-threaded](https://en.wikipedia.org/wiki/Thread_(computing)) programming model. Additionally, this framework provides a layer of abstraction between the code structure and graphic presentation of a Swing-based GUI.

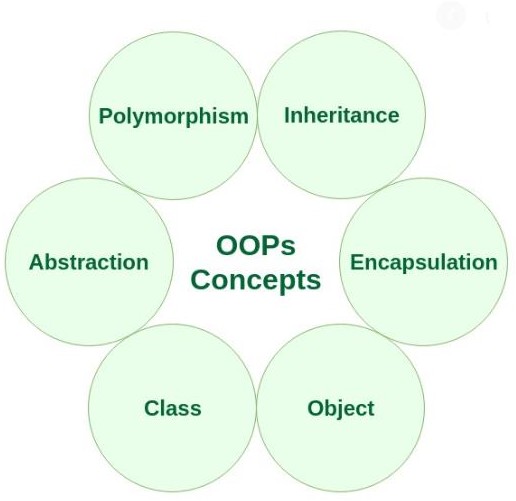
1. **Event Handling:**

**Event** is the change in the state of the object. Events are generated as a result of user interaction with the GUI components. Eg pressing a key, clicking the mouse, button click, dragging the scrollbar etc. Events are supported by a number of packages, including **java.util, java.awt, and java.awt.event. Event Handling** is the mechanism that controls the event ans decides what should happen if the event occurs.

## CHAPTER 3

**OBJECT ORIENTED CONCEPTS**

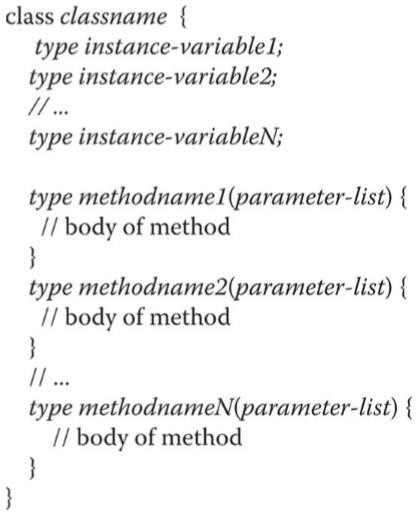
OOPS concepts in Java are the main ideas behind Java’s Object Oriented Programming. They are an abstraction, encapsulation, inheritance and polymorphism. Grasping them is key to understanding how Java works. Basically, Java OOP concepts let us create working methods and variables, then re-use all or part of them without compromising security. In Java, abstraction means simple things like objects, classes and variables represent more complex underlying code and data. It prevent in repeating the same work multiple times. Inheritance let programmers to create new classes that share some of the attributes of existing classes. Polymorphism is used to let programmers use the same word to mean different things in different contexts which may be in method overloading form or method overriding form.



**Figure 1: OBJECT ORIENTED CONCEPTS IN JAVA**

* 1. **CLASS :**

A class can be defined as a blueprint (template) that describes the behaviors or state that object of its type support and includes or represents the set of the properties or methods that are common to all object of one type. It includes modifiers, class name, super class, and body. We declare its exact form and nature, by specifying the data that it contains and the code that operates on that data while defining a class. A class is declared by the use of the class keyword. The methods and variables defined within the class are called members of the class. The class is at the core of JAVA. All the concepts to be implemented in Java must be encapsulated within a class.



**Figure 2: GENERAL FORM OF A CLASS**

* 1. **OBJECT:**

Objects have states and behaviors. For example: a dog is an object having states color, name, breed and behaviors wagging, barking, eating. Object is an instance of a class. For obtaining objects of a class first we need to declare a variable of the class type then, we must acquire an actual, physical copy of the object and assign it to that variable using new operator which at run time dynamically allocates memory for an object and return a reference to it.

* 1. **INHERITENCE:**

When one class acquire the properties of another class it is called inheritance. A class that is inherited is called superclass and the class that does the inheriting is called a subclass. In-order to inherit a class extend keyword is used. Inheritance is one of the cornerstones of object- oriented programming because it allows the creation of hierarchical classifications. There are five types of inheritance – single level inheritance, multi-level inheritance, hierarchical inheritance, multiple inheritance and hybrid inheritance. Among them hybrid inheritance is not possible in Java and multiple inheritance is only possible in interface concept.

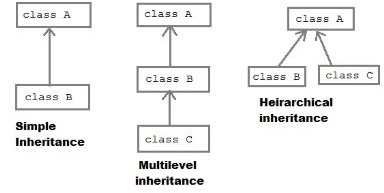
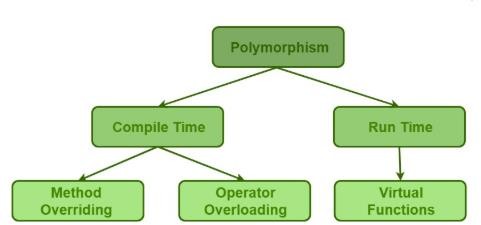


Figure 4: COMMONLY USED INHERITANCE TYPES

* 1. **POLYMORPHISM:**

Polymorphism in Java is a concept by which we can perform a single action in different ways. Polymorphism is derived from two Greek words: poly(many) and morphs(forms). There are two types of polymorphism in Java: compile time polymorphism and runtime polymorphism. Polymorphism can be perform by method overloading and method overriding. Dynamic method dispatch is runtime polymorphism where a call to an overridden method is resolved at runtime rather than compile time. Method overloading is said to be done when a class have more than one method with same name but different argument list. Method overriding is said to be done when a method which is declared in parent class is also declared in child class.



**Figure 5: TYPES OF POLYMORPHISM**

* 1. **ABSTRACT CLASS:**

When one class is declared abstract which may or may not include abstract methods is called abstract class. Abstract class can be sub classed but cannot be instantiate. Abstract class are similar to interfaces. Here we can declare fields that are not static and final, and define public, protected, and private concrete methods. Java abstract class can implement interfaces without even providing the implementation of interface methods. It is used to provide common method implementation to all the subclasses or to provide default implementation.

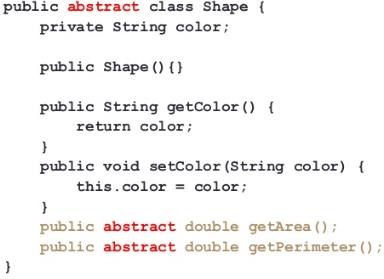


Figure 6: EXAMPLE OF ABSTRACT CLASS

* 1. **MULTITHREADING:**

Multithreading is the method of executing two or more threads simultaneously to maximum utilization of CPU. Here two thread run concurrently hence also known as concurrency in Java. Multiple threads don’t allocate separate memory area, hence they save memory. There is asynchronous behavior of the programs in multithreading but when there is a need to access the shared resources by two or more threads then synchronization approach is utilizes. It is the specialized form of multitasking.

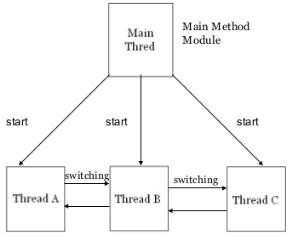


Figure 7: MULTITHREADED PROGRAM GRAPH

* 1. **I/O FUNCTIONS:**

Java I/O is used to process the input and produce the output. Java use stream concept to make I/O operation fast. The java.io package contains all the classes required for input output operation. A stream is an abstraction that either produces or consumes information. A stream is linked to a physical device by the Java I/O system. Same I/O classes and methods can be applied to different types of devices.

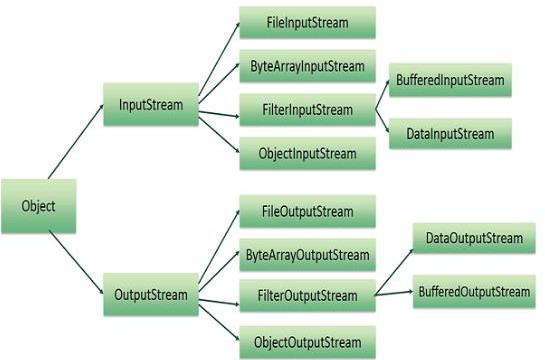


Figure 8: OVERVIEW OF I/O STREAMS

* 1. **JAVA PACKAGES:**

A mechanism for partitioning the class name space into more manageable chunks is the package in Java. The package is both a naming and visibility control mechanism. To create a package, simply include a package command as the first statement in the source file. The package statement defines a name space in which classes are stored. If no package statement is written, the class are put into default package. Import statement is used to bring certain classes or entire packages into visibility.



Figure 9: IMPORTING ONE PACKAGE TO ANOTHER

* 1. **EXCEPTION HANDLING:**

Java exception is an object that describes an exceptional (error) condition that has occurred in the piece of code. When error arises an object representing that exception is created and thrown in the method that caused the error which may choose whether to handle or pass the exception. There are five keywords in Java exception handling – try, catch, throw, throws, and finally. The risky statement to be monitored is contained within try block, if exception occur it is thrown and exception is catch and handled. Throw keyword manually throw an exception. Exception thrown out of method is specified by throws clause. The code that must be executed after a try block completes is put in finally block.

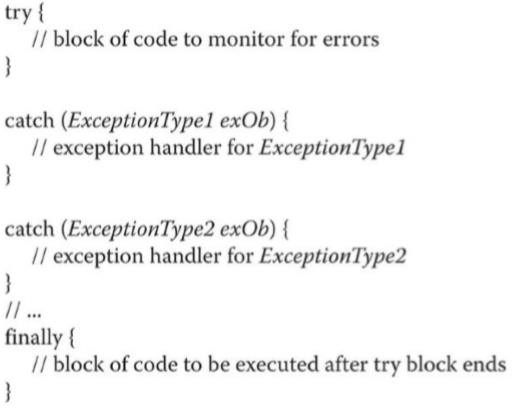
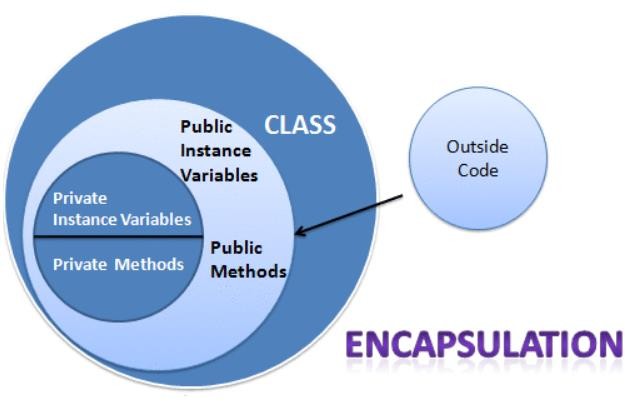


Figure 10: GENERAL FORM OF EXCEPTION HANDLING

* 1. **ENCAPSULATION:**

Encapsulation is one of the most important principles of Object-Oriented Programming. It is a mechanism of wrapping the data(variables) and code acting on the methods together as a single unit. Here the variables or data of a class is hidden from any other class and can be accessed only through any member function of own class in which they are declared. Data are hidden from other classes with the help of data hiding concept which is achieved by making the members or methods of the class as private and the class is exposed to the end user or the world without providing any details behind implementation using the abstraction concept, so it is also known as combination of data-hiding and abstraction. Encapsulation can be achieved by declaring all variables in the class as private and writing public methods in the class to set and get the values of variables.



**Figure 11: ENCAPSULATION**

## CHAPTER 4

* 1. **SOURCE CODE**

public class mini extends JPanel implements ActionListener {

char[]str={'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'

,'0','1','2','3','4','5','6','7','8','9'};

char[]str1={'!','@','#','$','%','^','&','\*','(',')','','=','\_','+','`','|','{','}','[',']',';',':',',','<','>','/'

,'a','b','c','d','e','f','g','h','i','j'};

String k=""; String l=""; char[] a=new char[50]; char[] b=new char[50];

JLabel plain\_lbl,enc\_lbl,dec\_lbl; JTextField tplain\_txt,tenc\_txt,tdec\_txt; JButton bencrypt,bdecrypt,bclear,bexit; Font f1;

public mini()

{

f1=new Font(Font.MONOSPACED,Font.BOLD,20);

plain\_lbl=new JLabel("Plain Text"); enc\_lbl=new JLabel("Encrypted Text");

dec\_lbl=new JLabel("Decrypted Text");

plain\_lbl.setFont(f1); enc\_lbl.setFont(f1); dec\_lbl.setFont(f1);

//JTextField

tplain\_txt=new JTextField(20); tenc\_txt=new JTextField(20); tdec\_txt=new JTextField(20); tenc\_txt.setEditable(false); tdec\_txt.setEditable(false);

tplain\_txt.setFont(f1); tenc\_txt.setFont(f1); tdec\_txt.setFont(f1);

//JButton

bencrypt=new JButton("Encryption"); bdecrypt=new JButton("Decryption"); bclear=new JButton("Clear"); bexit=new JButton("Exit");

bdecrypt.setEnabled(false);

bencrypt.setFont(f1); bdecrypt.setFont(f1); bclear.setFont(f1); bexit.setFont(f1);

setLayout(null);

add(plain\_lbl); add(tplain\_txt); add(enc\_lbl); add(tenc\_txt); add(dec\_lbl); add(tdec\_txt); add(bencrypt);

add(bdecrypt); add(bclear); add(bexit);

plain\_lbl.setBounds(20, 20, 200,30); tplain\_txt.setBounds(220,20,200,30);

enc\_lbl.setBounds(20,80,200,30); tenc\_txt.setBounds(220,80,200,30); dec\_lbl.setBounds(20,140,200,30); tdec\_txt.setBounds(220,140,200,30);

bencrypt.setBounds(30,200,160,30); bdecrypt.setBounds(240,200,160,30);

bclear.setBounds(30,240,160,30);

Enter Any text !", bexit.setBounds(240,240,160,30);

bencrypt.addActionListener(this); bdecrypt.addActionListener(this);

bclear.addActionListener(this); bexit.addActionListener(this);

}

public void actionPerformed(ActionEvent ae)

{

String action=ae.getActionCommand(); if(action.equals("Encryption"))

{

k=tplain\_txt.getText().toString().toLowerCase(); if(k.equals(""))

{

tplain\_txt.setFocusable(true); JOptionPane.showMessageDialog(this, "Please "Warning",JOptionPane.WARNING\_MESSAGE);

} else

{

bdecrypt.setEnabled(true); bencrypt.setEnabled(false); a=k.toCharArray();

for(int i=0;i<k.length();i++)

{

for(int j=0;j<36;j++)

{

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

{ a[i]=str1[j]; j=36;

}

}

}

for(int i=0;i<k.length();i++)

{ l=l+a[i] ;

}

tenc\_txt.setText(l);

l="";

}

}

{

else if(action.equals("Decryption"))

String x=tenc\_txt.getText().toString(); String y="";

if(x.equals(""))

{

JOptionPane.showMessageDialog(this,"NoEncryptedMessage","Warning",JOpt ionPane.WARNING\_MESSAGE);

}

else

{

b=x.toCharArray(); for(int i=0;i<x.length();i++)

{

for(int j=0;j<36;j++)

{

if(b[i]==str1[j])

{

b[i]=str[j]; j=36;

}

}

}

for( int i=0;i<x.length();i++)

{

y=y+b[i];

}

tdec\_txt.setText(y); y="";

}

}

else if(action.equals("Clear"))

{

tplain\_txt.setText(""); tenc\_txt.setText(""); tdec\_txt.setText(""); tplain\_txt.setFocusable(true);

bdecrypt.setEnabled(false); bencrypt.setEnabled(true);

}

else if(action.equals("Exit"))

{

System.exit(0);

}

}

public static void main(String[] args) {

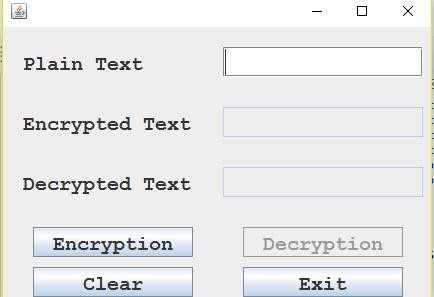
JFrame n=new JFrame(); n.getContentPane().add(new mini()); n.setSize(440,310); n.setVisible(true);

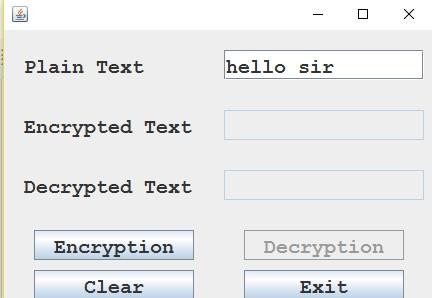
n.setDefaultCloseOperation(JFrame.EXIT\_ON\_CLOSE);

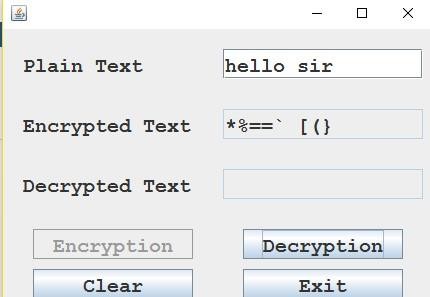
}

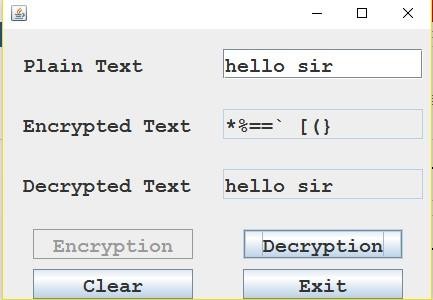
}

## SNAPSHOTS OF OUTPUT:









**CHAPTER 5**

* 1. **Conclusion:**

The main aim of this Project was to present the importance of various modern cryptographic techniques with respect to security and privacy. Today the world has transformed into a global village making privacy and security an immediate concern. . Without a secure network advancements like online banking, eshopping , would not have been possible .The very basic of network security is cryptography. Moreover The defense , would not be able to pass information related to national security without the use of cryptography , but again cryptography can also be a major threat to a nation’s security , as even the terrorist are making use of this technique to pass there messages . It is believed that alQaeda had used steganographic techniques to encode messages into images, and then transported these via email and possibly via NET to prepare and execute the September 11, 2001 Terrorist Attack. The mathematical explanation of RSA and DES algorithms proofs why these are commonly used even today.

Steganography is a fascinating and effective method of hiding data that has been used throughout history . There are many good reasons as well to use this type of data hiding, including watermarking or a more secure central storage method for such things as passwords, or key processes. Regardless, the technology is easy to use and difficult to detect. We hope that we are, to some extent, able to present our idea on this progressive field in a simple and concise manner.

Cryptography protects users by providing functionality for the encryption of data and authentication of other users. This technology lets the receiver of an electronic message verify the sender, ensures that a message can be read only by the intended person, and assures the recipient that a message has not be altered in transit. This paper describes the cryptographic concepts of symmetric key encryption, public-key encryption, types of encryption algorithms, hash algorithms, digital signatures, and key exchange. The Cryptography

Attacking techniques like Cryptanalysis and Brute Force Attack. This Project provides information of

Network Security Needs and Requirements. Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that today, secrecy is not the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well known and well-documented because they are also well-tested and well-studied! In fact, *time* is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys.

## References:

 [www.outguess.com](http://www.outguess.com/)

 [www.wikipedia.com](http://www.wikipedia.com/)

 [www.transcrypt.com](http://www.transcrypt.com/)

 [https://www.javatpoint.com](https://www.javatpoint.com/)