THE BISHOPS SCHOOL – CAMP

COMPUTER PROJECT SYNOPSIS

Implementation of Cryptography in Java

Name: Omkar S. Nath
Class: 10 – D
Roll Number: 35
Computer Code: 230438

ACKNOWLEDGEMENT

I would like to thank my computer teachers for their teaching and guidance throughout this project.

I would like to thank my headmaster, Mr. J. Edwin, and my principal, Mr. F. R. Freese, for managing the school and providing an enriching school environment.

I would like to thank my parents for providing me with the necessary support.

INDEX

INTRODUCTION

JAVA:

Java is a computer programming language that is class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers 'write once, run anywhere' (WORA), meaning that code that runs on one platform does not need to be recompiled to run on another. Java applications are typically compiled to bytecode (class file) that can run on any Java virtual machine (JVM) regardless of computer architecture. Java is, as of 2014, one of the most popular programming languages in use, particularly for client-server web applications, with a reported 9 million developers. Java was originally developed by James Gosling at Sun Microsystems (which has since merged into Oracle Corporation) and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++, but it has fewer low-level facilities than either of them.

BLUEJ:

BlueJ is an integrated development environment (IDE) for the Java programming language, developed mainly for educational purposes, but also suitable for small-scale software development.

BlueJ was developed to support the learning and teaching of object-oriented programming, and its design differs from other development environments as a result. The main screen graphically shows the class structure of an application under development (in a UML-like diagram), and objects can be interactively created and tested. This interaction facility, combined with a clean, simple user interface, allows easy experimentation with objects under development. Object-oriented concepts (classes, objects, communication through method calls) are represented visually and in its interaction design in the interface.

BlueJ is the primary recommended learning software for the Java section of the Computer Application course in ICSE schools all over India, where it is considered the de facto software for learning the basics of Object Oriented Programming and has proven extremely popular due to its ease of use and wide support in schools and

educational centers. However, it is not necessary that code that is written in the actual laboratory tests and final examinations be written in BlueJ, instead any IDE that supports Java can be used.

CRYPTOGRAPHY:

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

ABOUT THE PROGRAM:

This program aims to take the Plain Text and Key from the user and generate the Cipher Text using various symmetric key encryption algorithms. The Plain Text can be obtained from the Cipher Text using the same Key by applying the respective decryption algorithm. This feature is demonstrated using multiple algorithms.

SYSTEM REQUIREMENT

HARDWARE:

1. CPU: Pentium® 4 CPU 2.00GHz
2. RAM: 2.02GHz. 0.99GB of RAM
3. Monitor: Dell LCD Monitor
4. Mouse: UMax Optical USB Mouse
5. Keyboard: Logitech Keyboard
6. Speaker: ZenStar Speakers

SOFTWARE:

1. Operating System: Microsoft Windows XP
2. Integrated Development Environment (IDE): BlueJ

CONCLUSION

The developed code can be used to encrypt and decrypt messages using the same Key. The Cipher Text can be then sent over any communication media where, even if it is intercepted, it will be difficult for the eavesdropper to interpret and understand the message.

FUTURE ENHANCEMENT

1. These cryptographic algorithms can be applied to files such as text, image and video files also.
2. More complex cryptographic algorithms, such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) can be implemented.
3. The User Interface (UI) can be made graphical in nature to make the program easy to use.

BIBLIOGRAPHY

1. ‘Computer Applications A Text Book for Class X’ By Sumita Arora.
2. ‘Cryptography and Network Security’ By William Stallings.
3. Encyclopedia Britannica.
4. Encyclopedia Encarta.
5. Encyclopedia Wikipedia.
6. ‘Frank Computer Applications For ICSE Class IX’ By Sonia Sabharwal.
7. ‘Frank Computer Applications For ICSE Class X’ By Sonia Sabharwal.
8. ‘Programming with Java A Primer’ By E Balagurusamy.

This page intentionally left blank.