International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169
Volume: 1 Issue: 7 628 – 631

A Java Based Network Security on Wireless Network communication

Abstract: Now a day a Wireless networking provides many advantages, but it also integrated with new security threats and alters the organization's overall information security risk profile. Security of data and privacy issues are important to individuals and organizations especially where exchange of data is done through computer networks. Organizations invest time and resources to reduce the threat and occurrence of data insecurity. Encryption is one of the many methods adopted because of its adaptability to electronic communication channels we are encrypting and decrypting a message from a server to a client, in which the message is encrypted on the server side and decrypted on the client side for some security purposes. Though there are many methods to handle such situations like data security encryption plays a vital role. We all see how DES works for countering those threats, when a data is transfer from server to client.

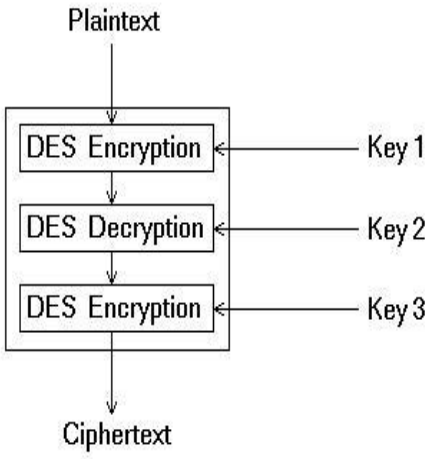
Keywords: Wireless Network, Wireless Security, Wireless Threat, Encryption, Decryption

*****

I. INTRODUCTION

Communication is a constant activity that human beings engage in naturally. Computer systems and devices replicate this human activity in exactly the same way. When human beings communicate messages are sent from the sender with the assumption that the receiver interprets the message correctly. In computer communications, messages must be in a specific format or code for the receiver to interpret it correctly. The communication between computers takes place in the form of requests, messages e.g. electronic mail, Twitter etc..; file transfer, image sharing and data retrieval. The transmission of requests, messages, files transfer and data retrieval is threatened by interceptors or hackers who illegally obtain the message or a copy of the message.

In this work, an application program was developed to provide encryption and decryption facilities for network communication using the algorithms DES. The java application program is intended for use with programs used for writing, editing or sending textual data between remote users on a computer network. Wireless networks consist of four basic components: The transmission of data using radio frequencies; Access points that provide a connection to the organizational network and/or the Client devices (laptops, PDAs, etc.); and Users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.



LITERATURE REVIEW

A variety of wireless technologies have been standardized and commercialized, but no single technology is considered the best because of different coverage and bandwidth limitations.

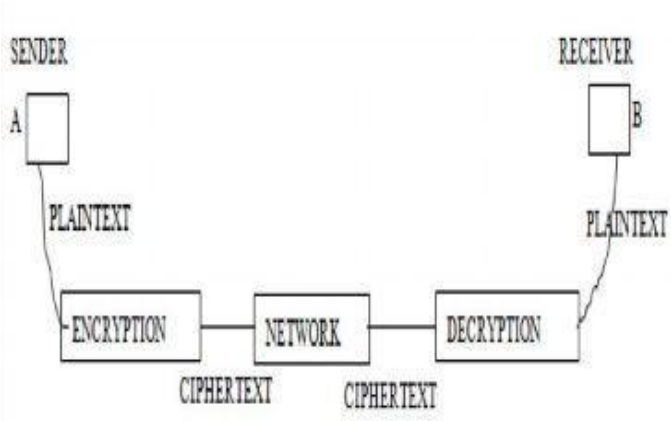
SecretKeySpec class : This class specifies a secret key in a provider-independent fashion and is only useful for raw secret keys that can be represented as a byte array and have no key parameters associated with them, e.g., DES or Triple DES keys.

Cipher class : This class provides the functionality of a cryptographic cipher for encryption and decryption. It forms the core of the Java Cryptographic Extension (JCE) framework. Its getInstance() method

is called to get the object based on algorithm. Then the init() method is called for initializing the object with encryption mode and key.

CipherInputStream class: It is composed of an InputStream and a Cipher so that read() methods return data that are read in from the underlying InputStream but have been additionally processed by the Cipher. The Cipher must be fully initialized before being used by a CipherInputStream. It is used for decryption and does read and then update operation.

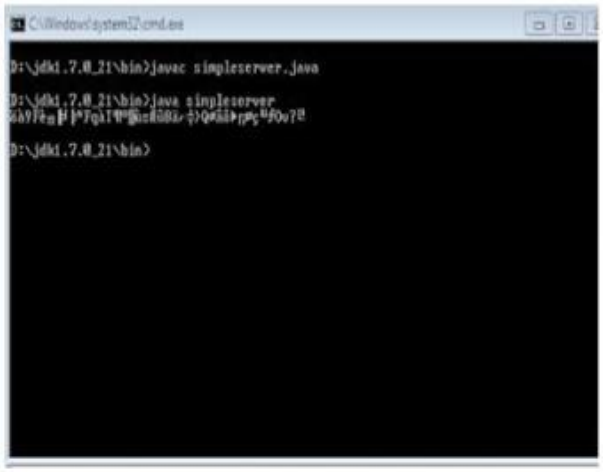
CipherOutputStream Class: Just like above it is also composed of a stream and cipher and the cipher must be fully initialised before using this stream. It is used for encryption purpose.

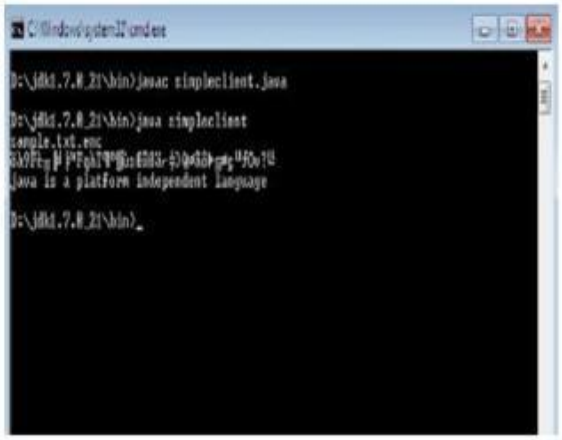


Client/Server Communication

At a basic level, network-based systems consist of a server, client, and a media for communications shown in Fig. A computer running a program that makes a request for services is called client machine. A computer running a program that offers requested services from one or more clients is called server machine. The media for communication can be wired or wireless network.

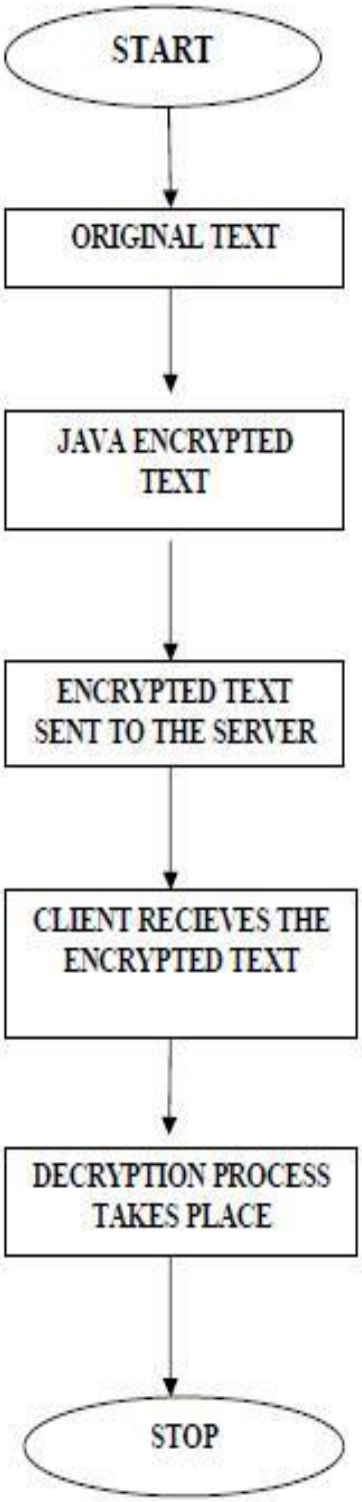
Here are the screenshots of an encrypted and a decrypted message.

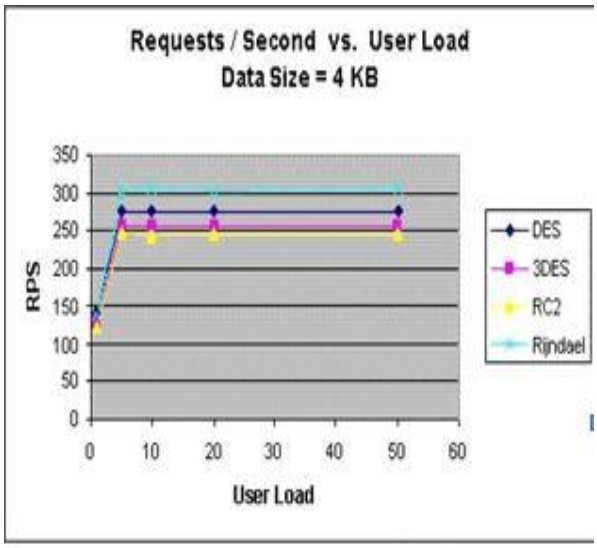


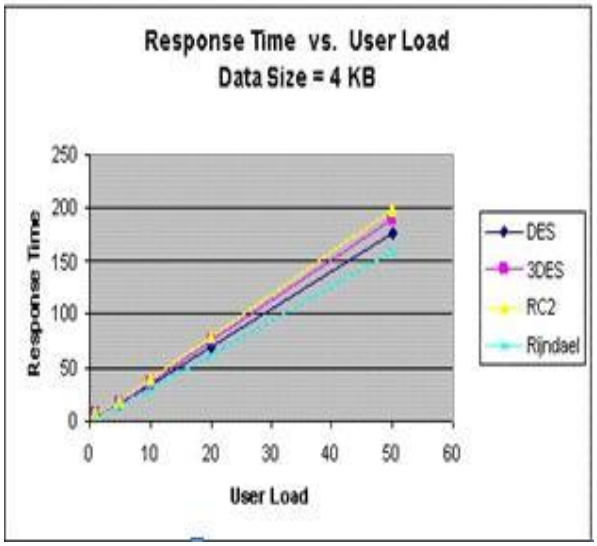


RESULTS AND DISCUSSION

Flow chart represents the results obtained by performing encryption and decryption activities for DES. When a message passes through a network, data security is an essential one which the user n secure it through many ways and the well known way is to encrypt the message is DES.







CONCLUSION

The java-based application was able to implement encryption using the Data Encryption Standard (DES). While passing the messages through a network data security is important. The reason why we chose DES is because of its adaptability and integrity. The application has helped in enhancing reliability of data /information communication among computers; acted as a means of authentication between the sender and the receiver of a message, maintained the confidentiality of the data rather than control access to data, and served as a deterrent to would-be cryptanalyst the procedure to determine the decryption

key is such a large word size, that is, breaking it down into two of four units before processing using assembly code could not be undertaken due to time constraints. The system was designed, implemented and tested using sample data on a wireless network.DES is one of the way through which the datas can be secured.

REFERENCES:

[1] Wireless Network Security: Vulnerabilities, Threats and Countermeasures by Min-kyu Choi[1)], Rosslin John Robles[1)], Chang-hwa Hong[2)], Tai-hoon Kim[1)] School of Multimedia, Hannam University, Daejeon, Korea.

[2] Graham, E., Steinbart, P.J. (2006) Wireless Security.

[3] A Java-based Data Encryption Application for Network Communication
by Oluwaseyitanfunmi Osunade

AUTHORS:

C.KARTHIKEYAN (LECTURER,
MUTHAYAMMAL ENGINEERING COLLEGE)

M.PRINCY (LECTURER,
MUTHAYAMMAL ENGINEERING COLLEGE)

FENELLA ANN FOWLER
(GTECH, VELLORE)