ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

A Java-based Data Encryption Application for Network Communication

Oluwaseyitanfunmi Osunade

Abstract*— 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 with two major algorithms used. The RSA and DES algorithms are used for securing data. In this work, an application program was developed to provide encryption and decryption facilities for network communication using both algorithms. The java application is intended for use with programs used for writing, editing or sending textual data between remote users. The results indicate a successful implementation of the two algorithms in one application program.

***Index Terms*—Algorithms, Computer Networks, Data Encryption, Data Transmission, Security.**

I. INTRODUCTION

Communication is a natural and constant activity that human beings engage in. 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. There are several formats or codes such as hexadecimal, binary, portable document format (PDF), text file (.txt), in which computer messages can be sent. Each computer must understand the formats or codes used. The receiving computer must have the necessary facility to understand the message sent if it is to respond to the sender's message in the right manner.

The communication between computers takes place in the form of requests, messages e.g. electronic mail, tweet and status; 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. The message obtained may be used for evil intentions such as blackmail, disruption of services, intellectual property violations and identity theft. This concern for security of the message from spying attacks and theft gave birth to the field of cryptography. Cryptography is a method of securing messages by using secret keys to disguise messages so as to stop unauthorized access to the message. Cryptography provides different mechanisms for encrypting, decrypting and authenticating communications between computers such as digital signature, time stamp and data encryption standard (DES) and Rivest Shamir Adilman (RSA).

In this work, an application program was developed to provide encryption and decryption facilities for network communication using both algorithms i.e. DES and RSA. 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.

II. LITERATURE REVIEW

Computer communication occurs when two or more computers communicate messages over transmission media such as twisted pair cables or airwaves. Figure 1 show the stages in the communication between two computers when cryptography is employed. The message to be encrypted called plaintext is scrambled using secret keys to get cipher text such that other people cannot determine what the content is, unless the receiving computer knows the key for decrypting the cipher text. The Internet, a large communication system, has increased the numbers of users who use computing devices for communication of data, messages and requests. The increase in use has raised concerns for secured communications. Reference [1] identified some threats to secured communications such as pathway blockage, alteration and interception. Pathway blockage is a scenario whereby the flow of information is entirely blocked. This causes denial of services to the users connected. This is achieved by either totally cutting the transmitting media or tampering with the flow of information from the source. Alteration means the context of messages is modified before it is received at the destination host. Interception is a situation whereby a copy of the message is obtained without disrupting the normal flow of information. Over the years several methods, codes and

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

ciphers have been developed, called cryptography, to prevent these threats to messages communicated between two computing devices.

The growth of cryptography has been on the same level with the breaking of codes and ciphers called cryptanalysis. The Spartans' Stick method was the first recorded use of cryptography in correspondence as early as 400BC [2]. A cipher device called the scytale was employed for secret communications between military commanders. The scytale consisted of a tapered baton around which was spirally wrapped a strip of parchment or leather on which the message was written. When unwrapped the letters were scrambled and thus formed the cipher. However, when the strip was wrapped round another baton of identical proportion to the original, the plaintext re-appeared [2]. In the earliest and simplest ciphers, a character was the unit of data and involved either substitution or transposition.

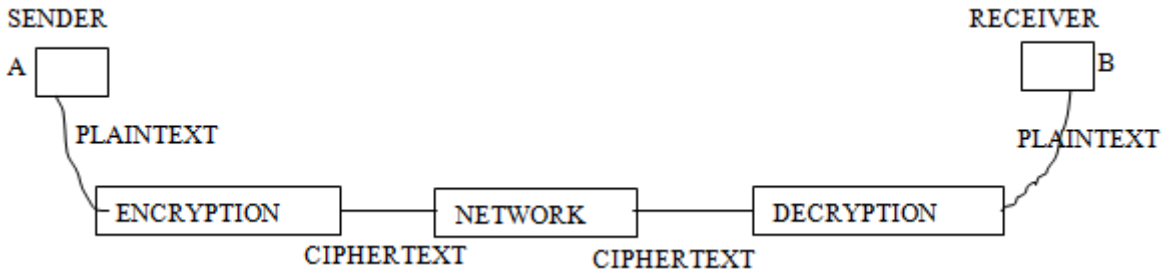

Fig 1: Communication Path between Two Communicating Devices

Substitution and transposition are the basic operations carried out in most ciphers. Substitution involves the replacement of a character by another character or replacement of a character by a different character for each occurrence. An S-Box (Substitution-box) is a basic component of symmetric key algorithms which performs substitution. Transposition requires that the character retain their plaintext form but change their positions to create the cipher text. The text is organized into a two-dimensional table and the columns are interchanged according to a key. This is not very secure because the character frequencies are preferred and the attacker can find the plaintext through trial and error. A permutation box (or P-box) transposes bits across S-boxes inputs by bit-shuffling while retaining diffusion while transposing [3]. In block ciphers, the S-boxes and P-Boxes are used to make the relation between the plaintext and the cipher text difficult to understand.

A. DES

An example of a complex block cipher is the data encryption standard (DES). In DES instead of substituting one character at a time, it substitutes 8 characters (8 bytes) at a time, using complex encryption and decryption algorithms [4]. It was designed by IBM in 1977 as the standard encryption method for non military and later endorsed and adopted by the U.S government and non-classified uses. It has been the encryption standard of the banking and financial communities since then.

The DES algorithm encrypts a 64 bit plaintext using a 56 bit key. But every eight bit of the key bit is used for parity checking and is ignored thus producing a 48 bit key that is fixed in length. The plaintext is subjected to 19 different and complex procedures to create a 64 bit cipher text. The algorithm consists of two transposition blocks, one swapping block and 16 complex blocks called iteration blocks or Feistel cipher block [5]. A Feistel cipher or network is a symmetric structure used in the construction of block ciphers. The same operations are performed on all the 16 iteration blocks but each uses a different key derived from the original key. Figure 2 shows how the DES model works.

According to [6] – [7], the first 64 bits plaintext is broken down into two equal parts of 32 bits. The first 32 bits is referred to as right half (R_1) and the second as the left half (L_1). Thereafter the Festiel function will be performed on it as follows:

- The first half is expanded into 48 bits, this is achieved by repeating the edge bits of each successive 4 bit byte. The resulted bits are then XOR with the 48 bits key. S-box operations are now performed on the 48 bits to select a new 32 bits.
- The previous right 32 bits now become the next left 32 bits (swapping)

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

- After the 16th round, the right and the left halves are joined and a final permutation completes the process [8].

Mathematically, encryption under DES is of the form:

$B = L_i f_i$

$L = R_{i-1}$

$R_i = L_{i-1}$ (+) $F(R_{i-1}, K_i)$ while,

Decryption is

$R_i = L_{i-1}$

$L_{i-1} = R_i$ (+) $f(L_i, K_i)$

Where (+) is the component - wise addition mod- 2 (XOR),

K is the 32-bit portion of the key used in round 1, and f is function with 32-bit output.

A lot of block ciphers use the Feistel cipher block, including the Data Encryption Standard (DES). The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule [9]. Therefore the size of the code or circuitry required to implement such a cipher is almost reduced by half. Symmetric-key algorithms are a class of algorithms for cryptography that use related or identical cryptographic keys for both decryption and encryption. The encryption key is related to the decryption key, in that they may be identical or there is a simple transformation to go between the two keys. The keys represent a shared secret between two or more parties that can be used to maintain private information.

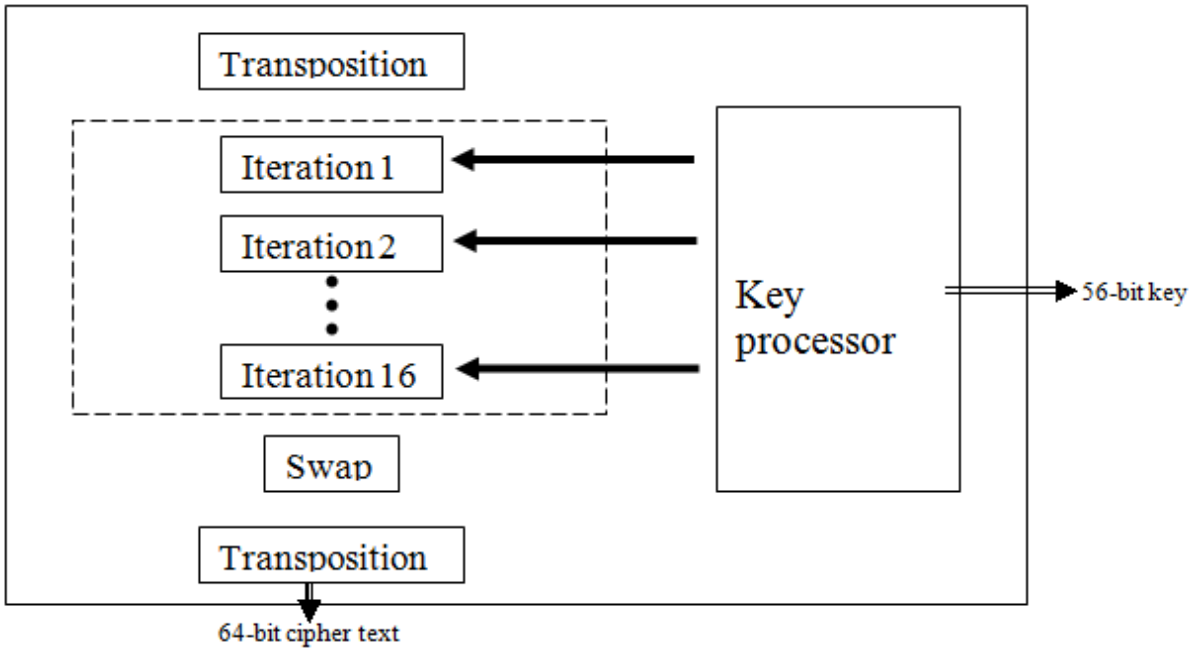

Fig 2: DES Model

Symmetric-key algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt the bits of the message one at a time, and block ciphers take a number of bits and encrypt them as a single unit. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks. Examples of well-known symmetric algorithms include Two fish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, 3DES, and IDEA. Symmetric ciphers are often used to achieve other cryptographic purposes than just encryption. Encrypting a message does not guarantee that the message is not changed while encrypted. A message authentication code, constructed from symmetric ciphers, is added to a cipher

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

text to ensure that changes to the cipher text will be known by the receiver. Symmetric ciphers also can be used for non-repudiation purposes according to ISO 13888-2 standard and to build hash functions from block ciphers.

Many modern block ciphers such as the DES are based on a construction proposed by Horst Feistel. Feistel's construction makes it possible to build invertible functions from other functions that are themselves not invertible [10]. Symmetric ciphers have historically been susceptible to known-plaintext attacks, chosen plaintext attacks, differential cryptanalysis and linear cryptanalysis. Careful construction of the functions for each round of iteration can greatly reduce the chances of a successful attack [11] – [12].

B. RSA

In cryptography, RSA (which stands for Rivest, Shamir and Adelman who first publicly described it) is an algorithm for public-key cryptography [13]. RSA is suitable for signing as well as encryption and was the first great advance in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations.
The RSA algorithm involves three steps: key generation, encryption and decryption. RSA involves a public key that is known to everyone for encrypting messages and a private key for decryption. The keys for the RSA algorithm are generated the following way:

- Choose two distinct prime numbers p and q.

For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

- Compute n = pq.

n is used as the modulus for both the public and private keys

- Compute $\varphi(n) = (p - 1)(q - 1)$, where φ is Euler's totient function.
- Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e,\varphi(n)) = 1$, i.e. e and $\varphi(n)$ are co prime.
- e is released as the public key exponent.

e having a short bit-length and small Hamming weight results in more efficient encryption - most commonly 0x10001 = 65537. However, small values of e (such as 3) have been shown to be less secure in some settings [14].

- Determine $d = e^{-1} \bmod \varphi(n)$; i.e. d is the multiplicative inverse of e mod $\varphi(n)$.

This is often computed using the extended Euclidean algorithm.

- d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the private (or decryption) exponent d which must be kept secret.

III. METHODOLOGY

The application program developed is divided into three modules which are contained in two java classes. These modules are:

1 DES encryption module
2 RSA encryption module
3 RSA/DES decryption module

Figure 3 presents the schematic diagram of the program modules while Figure 4 presents the program flowchart.

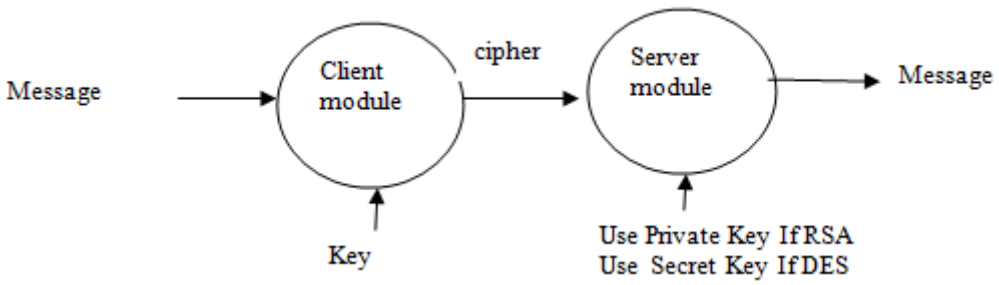

Fig 3: Program Modules

The application was written using Java Software Development Kit. The program is modular and uses a hybrid of object and event oriented techniques in accordance with the Java programming language. Java programs can be executed on any computer that has a Java Virtual Machine (JVM) present.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

The input to the program must be in the form of the text to be encrypted. The text is entered into the application during execution. After encryption, the encrypted text is displayed in the text window. This encrypted text can then be sent over the channel to the server application. Decryption of the text, which takes place at the server application, will result in the decrypted text being displayed in the output text window.

IV. RESULTS AND DISCUSSION

Figure 5 to Figure 11 presents the results obtained by performing encryption and decryption activities for both DES and RSA. The RSA encryption module presents the user with a dialog box which prompts the user to enter the prime number p and q to be used for generating the public and private keys. On clicking the encryption button, the public and private keys are generated, and the public key is used to encrypt the text.
The decryption button, on the server application, handles the decryption of both RSA and DES encryption files. It prompts for private keys in RSA decryption. The program is capable of distinguishing between text encrypted by the RSA and DES algorithms.

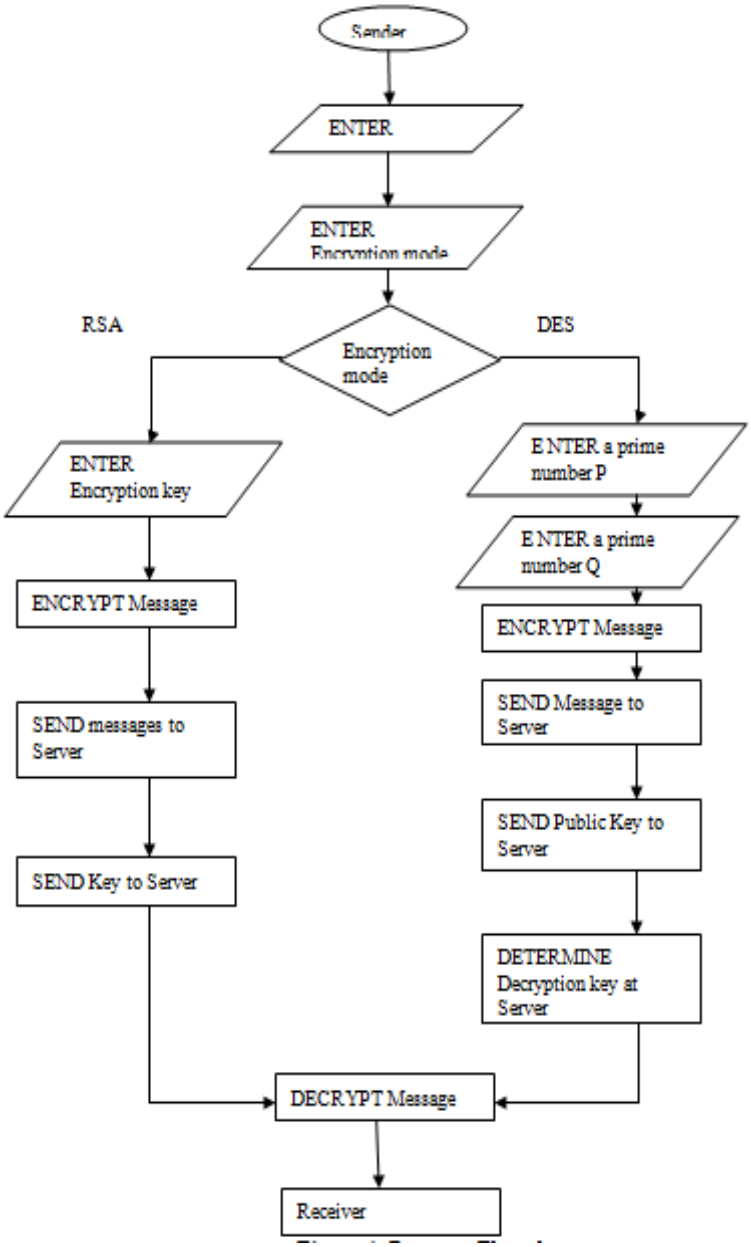

Fig 4: Program Flowchart

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

RSA

Figure 5 shows the Input message before encryption, while figure 6 and 7 show the system prompting for a prime number. Figure 8 shows the text output after the encryption while figure 9 shows the sever side prompting for RSA private key before decryption.

Fig 5: Message before Encryption

Fig 6: The System Prompting For Prime Number p

Fig 7: The System Prompting For Prime Number q

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

Fig 8: The Text Output after RSA Encryption

Fig 9: The Server Side Prompting For RSA Private Key before Decryption

DES

The text content is entered before encryption at the Client Side. Figure 10 shows the encryption key input box, while figure 11 shows the encrypted text.

Fig 10: Pressing the Encrypt Button

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

Fig 11: Encryption at Client side

V. CONCLUSION

The java-based application was able to implement encryption using the Rivest-Shamir-Adelman (RSA) strategy and the Data Encryption Standard (DES). 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. In order to totally fulfill the principle of "exhaustive search" which is one of the pillars on which the RSA method was based, the value of n given by p x q has to be very big, to a size of between 150 and 200 digits. The system was designed, implemented and tested using sample data on a computer network.

REFERENCES

[1] Neumann P (1994). Computer Security. Issues in Science and Technology, pp.50-54.

[2] Cohen F (1995). A Short History of Cryptography. http://all.net/edu/curr/ip/Chap2-1.html. retrieved 12 February 2011.

[3] Chalmers University of Technology (2007). Cryptography. Computer Science and Engineering Department, Chalmers University of Technology. http://www.cs.chalmers.se/Cs/Grundutb/Kurser/krypto/lect03-2x2.pdf. Retrieved 12 February 2011.

[4] NIST, (1999), U.S. Department of Commerce/National Institute of Standards and Technology, Data Encryption Standard (DES), FIPS-Pub.46. Federal Information Processing Standards Publication. (Reaffirmed 1999 October 25).

[5] Forouzan BA (2005). Data Communication and Networking. 3rd Edition Tata McGraw-Hill Publishing Company limited.

[6] Whitfield D, Hellman M (1976). Privacy and Authentication: An Introduction to Cryptography. Proceedings of IEEE, Vol. 67, No 3, pp. 397-427.

[7] NIST, (1980), U.S. Department of Commerce/National Institute of Standards and Technology, FIPS 81: DES Modes of Operation. Computer Security Resource Center. Federal Information Processing Standards Publication. (Reaffirmed 1980 December 2 http://www.itl.nist.gov/fipspubs/fip81.htm. retrieved 12 February 2011).

[8] Schneier C (1996). Applied Cryptography. John Wiley & Sons, Inc., New York pp.20-250.

[9] Feistel H (1973). Cryptography and Computer Privacy. Scientific American 228(5), pp15-23.

[10] Feistel H (1974). Block Cypher Cryptographic System. US Patent 3,798,359 March 19, 1974.

[11] Hombrebueno DJS, Sicat GCE, Niguidula JD, Chavez EP, Hernandez AA (2009). Symmetric Cryptosystem Based on Data Encryption Standard Integrating HMAC and Digital Signature Scheme Implemented in Multi-cast Messenger Application. ICCEE, vol. 2, pp.327-334, 2009 Second International Conference on Computer and Electrical Engineering, 2009.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

[12] Coppersmith D (1994). The data encryption standard (DES) and its strength against attacks. IBM Journal of Research and Development, 38(3), 243–250. http://web.archive.org/web/20070615132907/http://www.research.ibm.com/journal/rd/383/coppersmith.pdf. retrieved 12 February 2011.

[13] Rivest R, Shamir A, Adleman L (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21 (2): 120–126. doi:10.1145/359340.359342.

[14] Boneh D (1999). Twenty Years of attacks on the RSA Cryptosystem. Notices of the American Mathematical Society (AMS) 46 (2): 203–213.

AUTHOR BIOGRAPHY

Oluwaseyitanfunmi Osunade, Dept of Computer Science, University of Ibadan, Nigeria. E-mail: o.osunade@ui.edu.ng