IJIRSET

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Analysis of Network Data Encryption & Decryption Techniques in Communication Systems

Ezeofor C. J.[1], Ulasi A. G.[2]

Lecturer, Department of Electronic and Computer Engineering, University of Port Harcourt, Rivers State, Nigeria[1]

PG student, Department of Information Technology, Federal University of Technology, Owerri, Imo State, Nigeria [2]

ABSTRACT: This paper presents analysis of network data encryption and decryption techniques used in communication systems. In network communication systems, exchange of information mostly occurs on networked computers, mobile phones and other internet based electronic gadgets. Unsecured data that travels through different networks are open to many types of attack and can be read, altered or forged by anyone who has access to that data. To prevent such an attack, data encryption and decryption technique is employed. In order to visualize the effect and evaluate the performance of the encryption and decryption of each technique used in communication systems, Visual Basic simulation program that encrypt and decrypt data were developed, written and tested. Different data block sizes were captured and plotted against total time response taken during data encryption using Microsoft Excel. The graph result shows the superiority of RSA and AES algorithms over other algorithms in terms of the processing speed and time. DES has worm holes in its security mechanism whereas Blowfish, AES, and RSA do not have any. Further analysis was made based on the graph result obtained on each data encryption techniques.

KEYWORDS: DES, AES, RSA, DSA, Cipher text, Symmetric encryption, Asymmetric encryption

I. INTRODUCTION

Encryption is one specific element of cryptography in which one hides data or information by transforming it into an undecipherable code [1]. Encryption typically uses a specified parameter or key to perform the data transformation. Some encryption algorithms require the key to be the same length as the message to be encoded, yet other encryption algorithms can operate on much smaller keys relative to the message. Encryption is most used among transactions over insecure channels of communication, such as the internet, automatic teller machines (ATMs), mobile telephones, and many others. Encryption can be used to create digital signatures which allow a message to be authenticated [2]. Decryption is an opposite of encryption which transforms the encrypted data into original form. The block diagram in figure 1.1 shows encrypting and decrypting data process in the network communication systems.

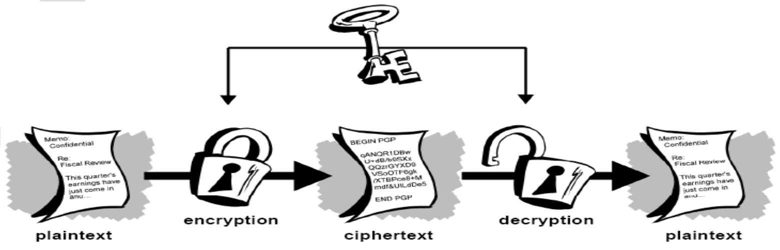


Figure 1.1: Block diagram of data Encryption and Decryption [2]

A. Symmetric Encryption

In Symmetric encryption, one key is used for both encryption and decryption. This means the person encrypting the message must send the key to the recipient before they can decrypt it. The Data Encryption Standard (DES), Advanced

IJIRSET

DOI: 10.15680/IJIRSET.2014.0312008

Encryption Standard (AES) and Blowfish are some of examples of the conventional cryptosystem that are widely employed by the Federal Government [3].

i. Data Encryption Standard (DES): DES was the first encryption standard to be recommended by National Institute of Standards and Technology (NIST) [4]. It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974 and federal government approved encryption algorithm for sensitive but non classified information in 1977. Since that time, many attacks and methods recorded that exploit the weaknesses of DES, which made it an insecure block cipher. Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted from exportation to other countries.

ii. Advanced Encryption Standard (AES): AES is a new encryption standard recommended by NIST to replace DES. Rijndael (pronounced Rain Doll) algorithm was selected in 1997 after a competition to select the best encryption standard [5]. It is a symmetric cipher defined in Federal Information Processing (FIPS) Standard Number 197 in 2001 as the federal government approved encryption algorithm. The National Security Agency has approved 128-bit AES for use up to SECRET level and 192-bit AES for use up to TOP SECRET level. AES is based upon the Rijndael algorithm, which was invented by Joan Daemen and Vincent Rijmen. AES specifies three approved key lengths: 128-bits, 192-bits and 256-bits. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption.

iii. Blowfish: The Blowfish algorithm was first introduced in 1993. It is one of the most common public domain encryption algorithms provided by [6], one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security. This algorithm can be optimized in hardware applications though it is mostly used in software applications and suffers from weak keys problem, no attack is known to be successful against it. Blowfish is a variable length key, 64-bit block cipher. The model for symmetric cipher is shown in figure 1.2.

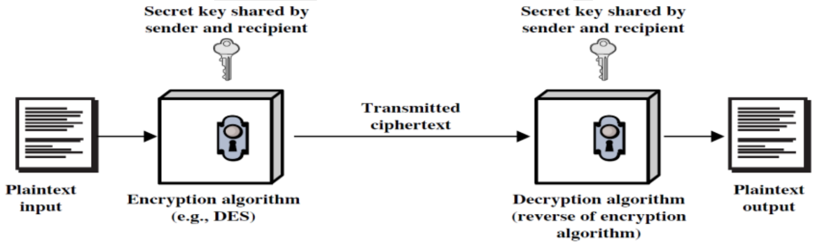

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1.2: Symmetric Cipher Model [2]

B. Asymmetric Encryption

Asymmetric encryption also known as Public-Key encryption, uses two different keys - a public key to encrypt the message, and a private key to decrypt it. This allows a user to freely distribute his or her public key to people who are likely want to communicate with him or her without worry of compromise because only someone with the private key can decrypt a message. To secure information between two users; the sender encrypts the message using the public key for the receiver, the receiver then uses the private key to decrypt the message [7]. Rivest, Adi Shamir & Leonard Adleman (RSA), Digital Signature (DSA), and EL-GAMAL are good examples of Asymmetric Encryption Algorithms.

i. Rivest, Adi Shamir, and Leonard Adleman (RSA): RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security [8]. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed Web, Internet, and computing standards.

IJIRSET

ii. *Digital Signature (DSA):* Digital signatures are implemented through public-key encryption and are used to verify the original and content of a message [9]. The recipient of the digital signature can be sure that the message genuinely came from the sender because the slightest change in the message gets reflected multi-fold in the message digest in a very obvious manner. The recipient must be sure that the message was not changes after the message digest was generated. The model for Asymmetric cipher is shown in figure 1.3.

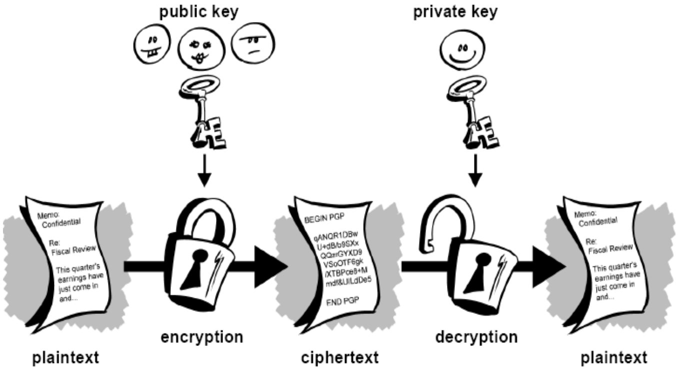

public key
private key
Memo Confidential Re: Fiscal Review This quarter's earnings have just come in and...
encryption
BEGIN PGP qANQR1DBw U+dBb9SXx QQsnGYXD9 VSoOTF6gk iXTBPce8+M mdf&LlILdDe5 END PGP
decryption
plaintext
ciphertext
plaintext

Figure 1.3: Asymmetric Cipher Model [2]

II. RELATED WORK

The related researched works are not limited to:

a. Different Data Encryption Methods Used in Secure Auto Teller Machine Transactions by Navneet and Vijay (2012) which discussed various types of encryption methods and standards which are used in secure banking data transmissions to make more data security. Data security is an important issue in current scenario of banking financial operation especially with transaction of secure and confidential data. It must be send with high security at the time of communication.

b. Protecting computer network with encryption technique by Kanaljit (2011) explained the latest authentication deals with biometric application such as fingerprint and retina scan. In today's world the protection of sensitive data is one of the most critical concerns for organizations and their customers. This, coupled with growing regulatory pressures, is forcing businesses to protect the integrity, privacy and security of critical information.

c. Research on Encryption Algorithm of Data Security for Wireless Sensor Network by Qingzhang and Zhongzhe, (2011) which explained that the authentication and encryption is the most important module in Wireless Sensor Network data security. However, sensor nodes with limited computing resources and storage resources, making the deployment of security mechanisms in the nodes need to consider their storage space, power consumption and other factors.

d. Encryption and Decryption Technique for Message Communication by Vinod and Niranjan (2011). Their report proposes a fast and secure encryption algorithm using substitution mapping, translation and transposing operations. The encryption standards such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and EES (Escrowed Encryption Standard) are widely used to solve the problem of communication over an insecure channel.

DOI: 10.15680/IJIRSET.2014.0312008

ISSN: 2319-8753

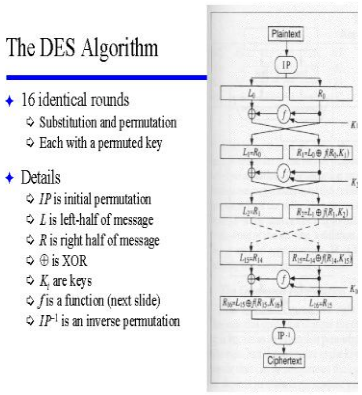
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

III. DESIGN METHODOLOGY

The selected symmetric algorithms for this research work are DES as in fig.3.1a, AES as in fig.3.1b and Blowfish as in fig.3.1c.



The DES Algorithm

- 16 identical rounds
  - Substitution and permutation
  - Each with a permuted key
- Details
  - IP is initial permutation
  - L is left-half of message
  - R is right half of message
  - ⊕ is XOR
  - K_i are keys
  - f is a function (next slide)
  - IP^{-1} is an inverse permutation

Fig. 3.1a DES Algorithm [14]

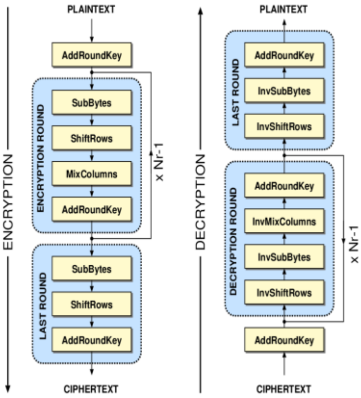


Fig. 3.1b AES Algorithm [10]

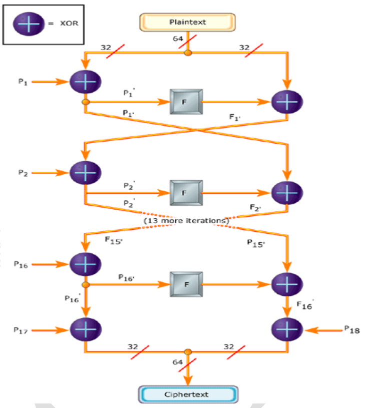
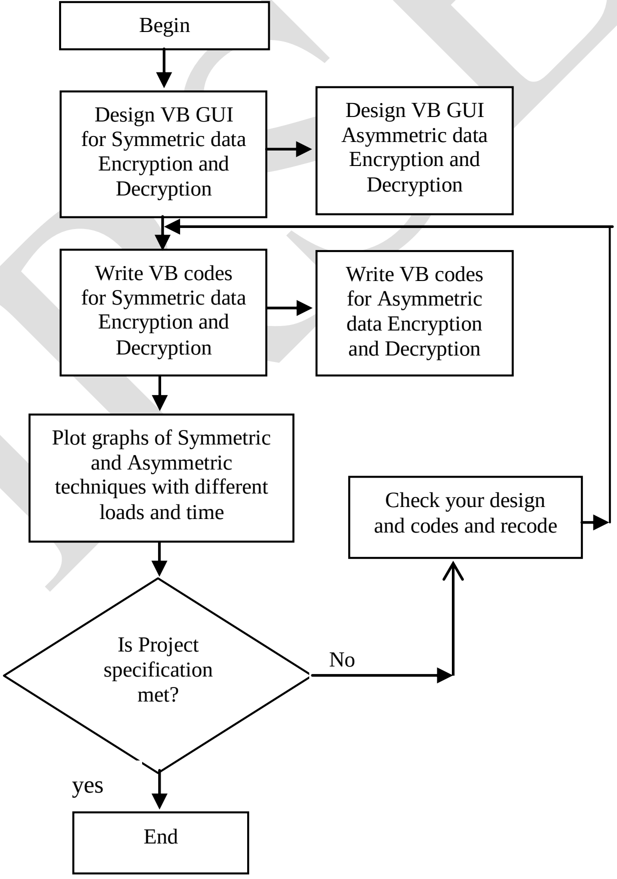


Fig. 3.1c Blowfish Algorithm [11]

The design of as ry] the steps outlined in the flow chart as shown in figure 3.2.

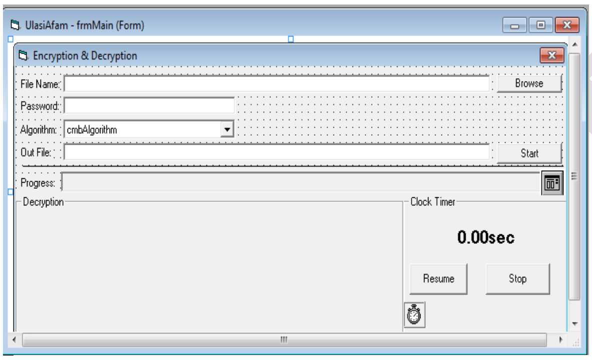


Begin
Design VB GUI for Symmetric data Encryption and Decryption
Design VB GUI Asymmetric data Encryption and Decryption
Write VB codes for Symmetric data Encryption and Decryption
Write VB codes for Asymmetric data Encryption and Decryption
Plot graphs of Symmetric and Asymmetric techniques with different loads and time
Check your design and codes and recode
Is Project specification met?
No
yes
End

Figure 3.2: Symmetric & Asymmetric Encryption flow chart

A. Graphical User Interface (GUI)of the Symmetric Encryption

The designed GUI Interface for Symmetric Encryption and decryption is shown in figure 3.3. The graphical user interface (GUI) and Visual Basic codes work in collaboration to analyse the performance of different encryption and decryption techniques employed. The GUI provides browse button that enables the user to select any file size for encryption. The password option is used to input password that would be use by the program to encrypt data. The user has option to select the required Symmetric Algorithm from the three provided. The timer option captures the time used by any selected Algorithm to encrypt file.



Algorithm: cmbAlgorithm

0.00sec

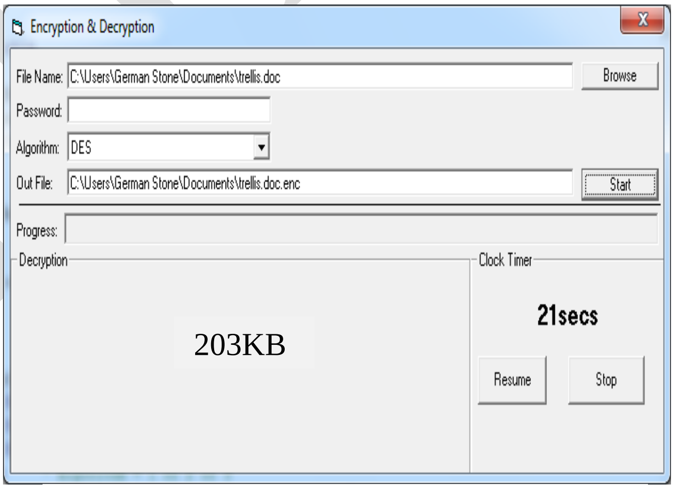
Figure 3.3: GUI interface for symmetric encryption

B. Procedures to Encrypt Data

Open Visual Basic 6.0 editor environment and click on the run menu then select start, the symmetric encryption form would display. On the encryption and decryption dialog-box, Click on the browse button and select any file size from the computer for encryption. Key in password on the space provided and selects one of the listed algorithms (DES, AES and Blowfish), then click on the start button. Look at the process bar and wait for the encryption to be done. Also watch the timer to get the total time taken by system to encrypt the chosen file. When the encryption is done, the system would notify you. Check the encrypted file in the folder where the file selected for the encryption is stored. In this experiment, different data block sizes were selected and tested. The 203kB data block size of file is selected and encrypted.

i. Time taken to encrypt 203KB using DES Algorithm

The experiment was conducted using Pentium IV computer system of 2.13GHz CPU speed. The data block size of 203kB is selected and DES Algorithm chosen. After the encryption, the time taken for the system to encrypt the data is 21secs as shown in figure 3.4a.



File Name: C:\Users\German Stone\Documents\trellis.doc

Algorithm: DES

Out File: C:\Users\German Stone\Documents\trellis.doc.enc

203KB

21secs

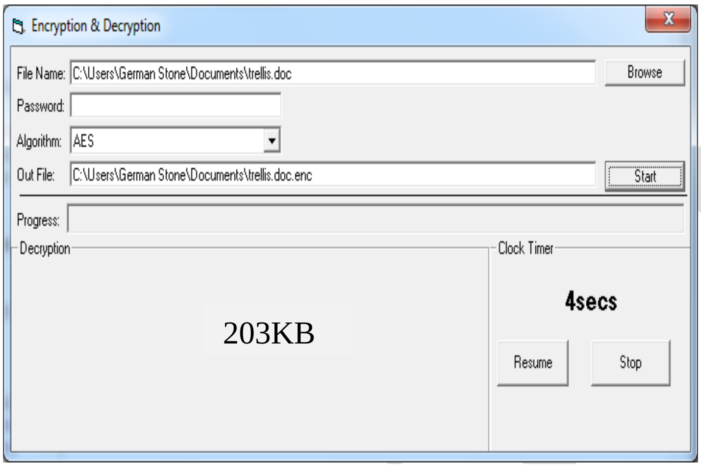
Figure 3.4a: 203KB data DES Encrypted Time

IJIRSET

DOI: 10.15680/IJIRSET.2014.0312008

ii. Time taken to encrypt 203KB using DES Algorithm

The experiment was conducted using Pentium IV computer system of 2.13GHz CPU speed. The data block size of 203kB is selected and AES Algorithm chosen. After the encryption, the time taken for the system to encrypt the data is 4secs as shown in figure 3.4b.



Encryption & Decryption

File Name: C:\Users\German Stone\Documents\trellis.doc

Password:

Algorithm: AES

Out File: C:\Users\German Stone\Documents\trellis.doc.enc

Progress:

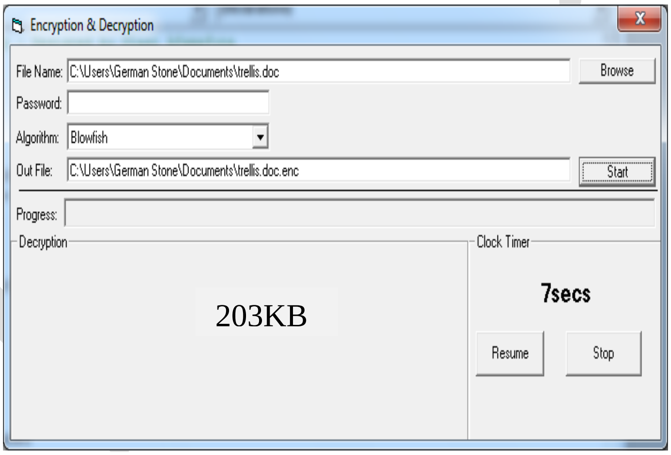
Decryption: 203KB

Clock Timer: 4secs

Figure 3.4b: 203KB data AES Encrypted Time

iii. Time taken to encrypt 203KB using Blowfish Algorithm

The experiment was conducted using Pentium IV computer system of 2.13GHz CPU speed. The data block size of 203kB is selected and Blowfish Algorithm chosen. After the encryption, the time taken for the system to encrypt the data is 7secs as shown in figure 3.4c.



Encryption & Decryption

File Name: C:\Users\German Stone\Documents\trellis.doc

Password:

Algorithm: Blowfish

Out File: C:\Users\German Stone\Documents\trellis.doc.enc

Progress:

Decryption: 203KB

Clock Timer: 7secs

Figure 3.4c: 203KB data Blowfish Encrypted Time

iv. Cipher Text of Encrypted data block size of 203KB

The cipher text of the data block size of 203KB is shown in figure 3.4d. As can be seen, most of the characters cannot appear since they do not have character representation especially block diagrams and pictures. Now, another comparison is made after the successful encryption process to make sure that all the data are processed in the right way by comparing the generated data size (the original data blocks) and the encrypted data block size generated from the process. The algorithm is evaluated in terms of the time required to encrypt the data block. All the implementations carried out were exact to make sure that the results will be relatively fair and accurate.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

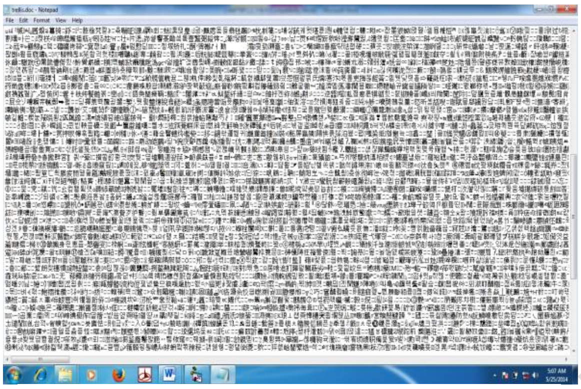
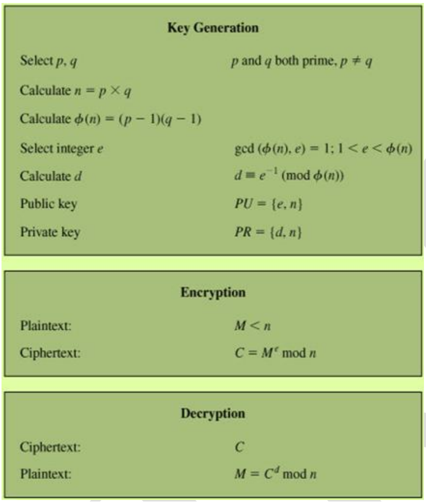


Figure 3.4d: Cipher Text for 203KB data

The selected Asymmetric algorithms for this research work are RSA as in fig.3.5a and DSA as in fig.3.5b.



Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} (\text{mod } \phi(n))$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$
Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \text{ mod } n$
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \text{ mod } n$

Figure 3.5a: RSA Algorithm [12]

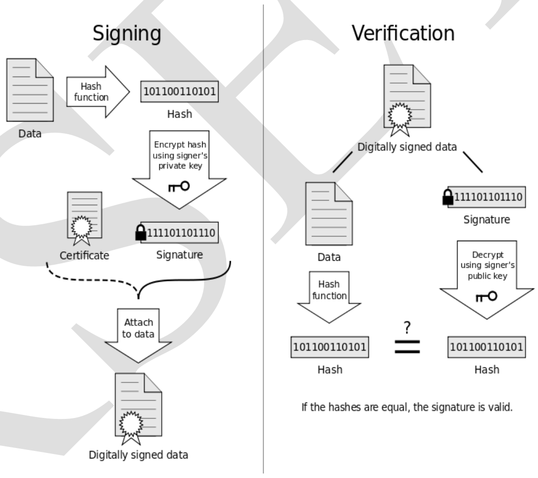


Figure 3.5b: DSA Algorithm [13]

C. RSA & DSA Encryption & Decryption GUI Interface and how it works

The RSA and DSA encryption require creation of keys namely public and private. These two keys would be used to encrypt and decrypt data send or receive on the network. When the user encrypt with public key generated at the sender's end, the user at the other end (receiver's end) would decrypt with the private key. Also when the user encrypt with private key generated at the sender's end, the user at the other end would decrypt with the public key. As shown in figure 3.6; the RSA and DSA encryption simulation environment, the first thing to do is to execute the program, generate or import keys and select the key size of your choice. Choose one of the options and click on generate/import key button. The public and private keys would be created and stored in 'TEMP' folder in computer's hard drive for future use. The creation of public and private keys automatically actives other GUI buttons in the environment. The browse button is used to add the file to be encrypted. When the file is added, click on the 'encrypt text using public key button' and the file would be encrypted using public key and display the cipher text encrypted in the textbox. The file can be sent on the network from the transmitter's end point. At the receiver's end point, click on the 'decrypt text using private key button' to re-convert the cipher text back to the normal plain text using private key which is automated in the program. The timer is used to capture total time and speed required by different computer systems to encrypt and decrypt any selected file in the computer using asymmetric GUI simulation program. The same method is used when encrypting and decrypting file using digital signature (DSA) option in the program environment.

DOI: 10.15680/IJIRSET.2014.0312008

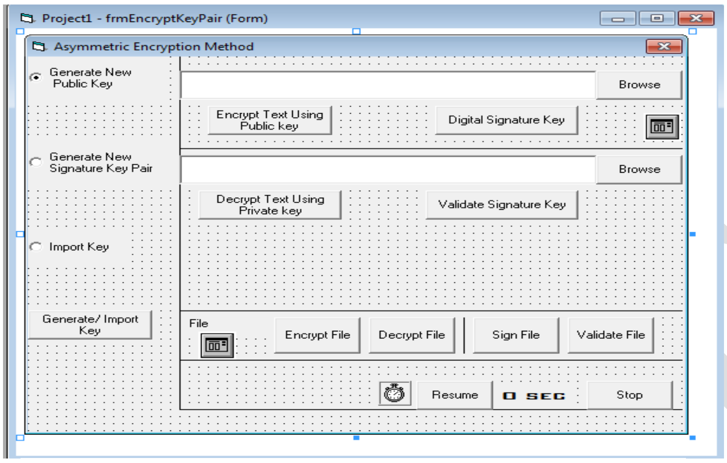

Project1 - frmEncryptKeyPair (Form)
Asymmetric Encryption Method
○ Generate New Public Key
○ Generate New Signature Key Pair
○ Import Key
Generate/ Import Key
Browse
Encrypt Text Using Public key
Digital Signature Key
Browse
Decrypt Text Using Private key
Validate Signature Key
File
Encrypt File
Decrypt File
Sign File
Validate File
Resume
0 SEC
Stop

Figure 3.6: Asymmetric RSA & DSA Encryption GUI Interface

The graphical user interface (GUI) for simulating network data symmetric and Asymmetric Encryption techniques were designed, written and tested in Visual Basic 6.0 (VB 6.0) editor environment as shown in figure 3.3 and figure 3.6 above. Two Computer systems with different processing speeds were brought and the program ran on both of them to visualize the performance effect of different chosen encryption algorithms such as DES, Blowfish, AES (Rijndael), RSA and DSA. Different data block file sizes were encrypted and time taken to encrypt each captured and noted down. This implementation is thoroughly tested and optimized to give the maximum performance of the selected algorithms which are used in today's network data encryption.

A. *Symmetric & Asymmetric encryption and decryption Performance in CPU 2.13GHz & 600MHz Systems*

Table 4.1: Comparative execution time (in seconds) of encryption algorithms in Computer CPU of 2.13 GHz

Data Block Size (bytes)	**AES** Time(s)	**DES** Time(s)	**BF** Time(s)	**RSA** Time(s)
72000	6	12	8	2
154000	8	20	10	4
203000	9	25	12	5
351000	12	40	17	8
476000	15	52	22	9.5
589000	17	64	25	11
718000	20	77	30	12
1222000	32	130	48	14
1715000	42	180	66	18
3156000	76	329	119	22

The first set of experiments was conducted in computer CPU of 2.13 GHz processing speed. Different block data sizes were selected and the algorithms tested in order to select the best out of the chosen algorithms. Table 4.1 shows the data block sizes and the output time response of each algorithm selected. The second set of experiments was conducted in Computer CPU of 600 MHz processing speed. The same block data sizes were used and the algorithms tested in order to select the best out of the chosen algorithms. Table 4.2 shows the data block sizes and the output time response of each algorithm after encryption.

IJIRSET

Table 4.2: Comparative execution time (in seconds) of encryption algorithms in Computer CPU of 600Hz

Data Block Size (bytes)	**AES** Time(s)	**DES** Time(s)	**BF** Time(s)	**RSA** Time(s)
72000	2	8	4	0.3
154000	4	16	6	1
203000	4	21	7	1.5
351000	8	36	13	3
476000	11	48	18	5
589000	13	60	21	5.5
718000	16	73	26	7
1222000	28	126	44	10
1715000	38	176	62	13
3156000	72	325	115	18

The data block sizes and time responses listed in table 4.1 and table 4.2 are plotted using Microsoft Excel. The algorithms behaviour shown on the graph results obtained are in figure 4.1 and figure 4.2. It is observed that RSA and AES have better performance over other algorithms in terms of throughput among all the symmetric Encryption techniques selected, followed by Blowfish. The result shows the superiority of RSA and AES algorithm over other algorithms in terms of the processing time. DES was seen to have worm hole in its security mechanism, Blowfish, AES, and RSA on the other hand, do not have any so far. These results have nothing to do with the other loads on the computer since each single experiment was conducted multiple times resulting in almost the same expected result. The performance graph is shown in figure 4.1.

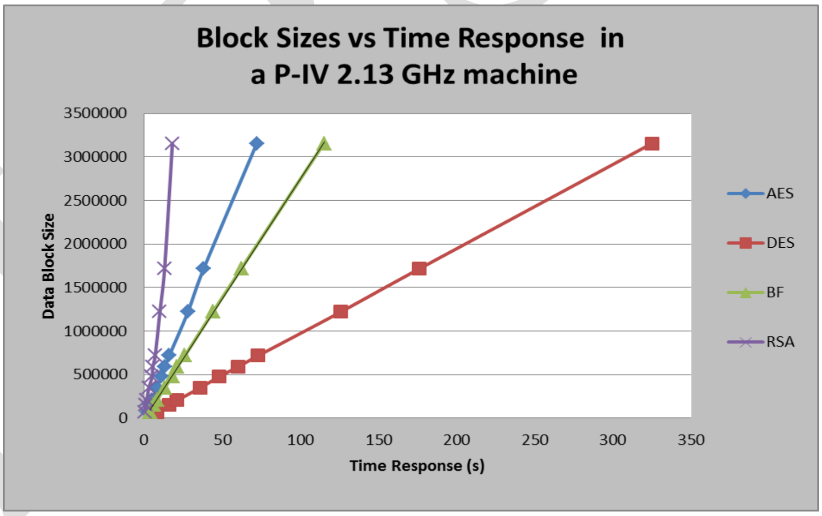


Figure 4.1: Block Sizes vs Time Response of CPU 2.13 GHz machine

DOI: 10.15680/IJIRSET.2014.0312008

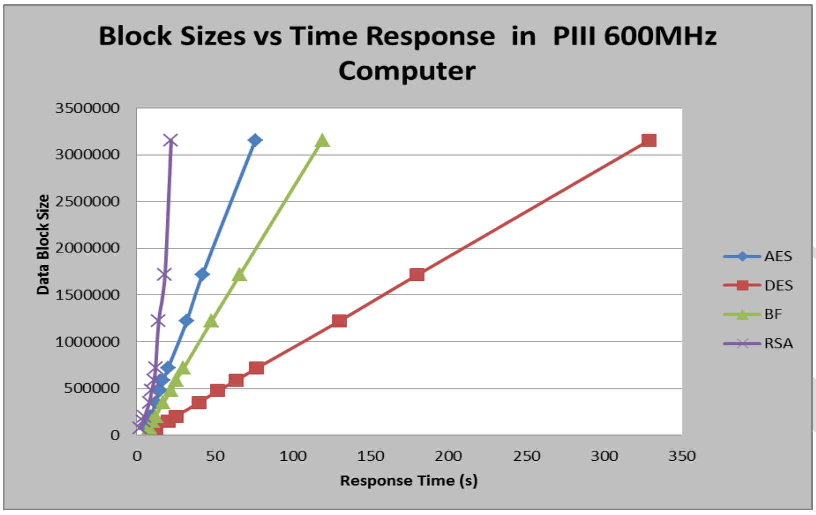


Figure 4.2: Block Sizes vs Time Response of CPU 600 MHz machine

Also it is shown that Blowfish, AES and RSA have the best performance among others. Both of them are known to have better encryption (i.e. stronger against data attacks) than the other two.

B. Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters:

i. *Computational Time:* The encryption time is considered as the time that an encryption algorithm takes to produces a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme and is calculated as the total plaintext in bytes encrypted divided by the encryption time.

ii. *Speed:* The encryption and decryption were tested in different systems of different processing speed to visualize the best performances of each algorithm.

iii. *Power consumption:* In variable key size of network data encryption algorithms, the power requirement can be analysed and compared with other algorithms by varying the key size under certain limit for same logic to generate the same condition that other algorithm follows in terms of key size.

V. CONCLUSION

The selected algorithms are AES, DES and Blowfish for symmetric and RSA and DSA for asymmetric. Several points can be concluded from the simulation results. First; there is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding. Secondly; in the case of changing packet size, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by AES. Third; in the case of changing data type such as image instead of text, it was found that Blowfish has disadvantage over other algorithms in terms of time consumption. Finally; in the case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption. It should be noted that computing in its totality is highly vulnerable if there is no security. If information that has been gathered over a period of time can just be stolen in just one second, that renders all efforts susceptible. There is every need to protect information from ‘praying eyes’ as information that can benefit or educate a group or individual can also be used against such groups or individuals.

In this research work, different data encryption techniques used in encrypting and decrypting network data; the symmetric encryption technique that uses only one key (the encryption key) to encrypt the data (examples DES, AES, Blowfish etc.) and the asymmetric encryption technique that uses two keys (a private key and a public key) to encrypt and decrypt the data (example RSA and DSA) were treated. The advice is that a user should not allow his password (key) to be viewed by anybody or written down. One should never assume that nobody is interested in stealing, destroying or damaging his data. Important data have to be encrypted.

DOI: 10.15680/IJIRSET.2014.0312008

IJIRSET

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

REFERENCES

[1] Stallings W., "Cryptography and Network Security 4th Ed," Prentice Hall, PP. 58-309, 2005.

[2] Brodney A, Asher J.,"Tales of the Encrypted"; Availablefrom:http://library.thinkquest.org/28005/flashed/index2.shtml (2009).

[3] Deepak K. D. and Pawan D.,"Performance Comparison of Symmetric Data Encryption Techniques" ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4 June 2012.

[4] Coppersmith D.,"The Data Encryption Standard (DES) Its Strength Against Attacks", IBM Journal of Research and Development, May 1994,pp. 243 -250.

[5] Chen J., Li X., Li W., Wan, W.,"An improved AES Encryption Algorithm", IET International Communication Conference on Wireless Mobile and Computing (CCWMC 2009).

[6] Bruce S., "The Blowfish Encryption Algorithm Retrieved" http://www.schneier.com/blowfish.html, 2008.

[7] Frank K. G., "Channel Attack secure Cryptographic Acceleration", 2006.

[8] Iana G. V., Anghelescu P., Serban G., "RSA Encryption Algorithm Implemented on FPGA", International Conference on Applied Electronics, pp. 1-4, 2011.

[9] Rivest, R. L., Shamir, A., & Adleman, L."Methods for Obtaining Digital Signatures and Public key cryptosystems", communication Of the ACM Vol. 21. pp. 120—126.1978.

[10] Frank kagan Giirkaynak,"Channel Attack secure Cryptographic Acceleration,2006.

[11] Blowfish [source:http://icmpnet/embedded/gifs/2003/0308/0308feat2fig1.gif]

[12] RSA[Source:http://flylib.com/books/en/3.190.1.84/1/

[13] DSA[Source:http://www.absoluteastronomy.com/topics/Digital_Signature

[14] DES[Source:http://dc532.4shared.com/joc/SrMkdWq3/preview.html

[15] Blaze M., Diffie W., Schneider B., Shimomura T., Thompson E., and Wiener M., "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security", Report of Ad Hoc Panel of Cryptographers and Computer Scientists, 1996.

[16] Brodney A, Asher J., "Tales of the Encrypted"; Availablefrom:http://library.thinkquest.org/28005/flashed/index2.shtml,2009

[17] Chandramouli R., "Battery power-aware encryption – ACM", Transactions on Information and System Security (TISSEC) Volume 9, Issue 2, May 2006.

[18] Deepak K. D. and Pawan D.,"Performance Comparison of Symmetric Data Encryption Techniques" ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4 June 2012.

IJIRSET

DOI: 10.15680/IJIRSET.2014.0312008