Int. J. Pure Appl. Sci. Technol., 27(1) (2015), pp. 1-10

International Journal of Pure and Applied Sciences and Technology

ISSN 2229 - 6107

Available online at ***www.ijopaasat.in***

Research Paper

Encryption and Decryption of Messages Using Advanced Encryption Standard and System of Nonlinear Equations

T.B. Ayokunle[1], U.S. Ogah[2] and A.P. Binitie[3,*]

[1] Department of Computer Science, Federal Polytechnic, Mubi, Adamawa State, Nigeria

[2] Department of Management Information System, Federal Polytechnic Mubi, Adamawa State, Nigeria

[3] Department of Computer Science, Federal College of Education (Technical) Asaba, Delta State, Nigeria

* Corresponding author, e-mail: (philpat4sure@gmail.com)

(Received: 30-12-14; Accepted: 18-2-15)

Abstract: *Encryption which is the coding or scrambling of information so that it can only be decoded and read by someone who has the correct decoding key has been in existence in various forms for thousands of years. Businesses, Government, Individuals, use encryption to protect their personal or secret information against unauthorized users. Despite the existence of various means of safeguarding our data against unauthorized users, Cooperate bodies, Individuals, Government agencies and parastatals kept losing their personal and secret data to Fraudsters. The study deals with encrypting and decrypting messages using Advanced Encryption Standard and System of Nonlinear Equations. In this study, Advanced Encryption Standard (AES) was introduced, which uses 128-block size as its key size. An algorithm was developed to secure messages transmission and then converted the messages into nonlinear algebraic systems of equations, which are then solved by Gaussian elimination method. The results obtained were compared with those produced by Direct Jahick Symmetric Key Algorithm (DJSA) and it was observed that they produced better result. Also it is almost impossible to break the Encryption algorithm without knowing the exact key value. This method is recommended for sending confidential data in any type of public application. Also it provides alternative to all unsecured methods of sending messages across the network.*

Keywords: Encryption, Decryption, Encoding, Decoding, Advanced Encryption Standard.

1. Introduction

Some vital information that are disseminated within offices, across offices, between branches of an organization and other external bodies and establishments at times get into the hands of the unauthorized persons who tampered with the contents of the information. If no security measures are taken, there is no doubt, such data and other sensitive information will be exposed to threats such as impersonation, corruption, repudiation, break-in or denial of services that caused serious danger on the individual or organization that are concerned [6].

A secured system should maintain the integrity, availability, and privacy of data involved in these situations. Data integrity usually means protection from unauthorized modification, resistance to penetration and protection from undetected modifications. Therefore, algorithms which help preventing interception, modifications, penetration, disclosure and enhance data or information security are now of primary importance [5]. The algorithm used is aimed at securing the message or information that is to be transmitted across the internet.

The software implementation uses AES algorithm, which replaces the data Encryption Standard (DES) that uses a 56-bit key to encrypt and decrypt information. Most conventional Ciphers require both parties to share a secret key, which is used in conjugations with an algorithm to encrypt or decrypt a file or text. In cryptography schemes, each user has a pair of keys: one private and one public. The public key is not secret- it is provided to people that might want to send an encrypted message to key's owner. The sender uses the public key to encrypt a message and the recipient then uses the private key to decrypt the incoming message. Only the matching private key will unlock the message secured by a public key.

The primary aim of this study is to encrypt and decrypt messages using Advanced Encryption Standard and System of Nonlinear Equations which leads to the following specific objectives namely,

- To introduce mathematical approach to encryption and decryption of data.
- To develop a model that will convert users messages into a system of nonlinear equation using summary algorithm.
- To hybridize the summary algorithm with Advanced Encryption Standard (AES) Algorithm for the purpose of data encryption and decryption.
- To implement the hybridized algorithm using appropriate tools.

In the last decades of the existence, computer networks is primarily used by university researchers for information transfer among academics and organizations for sharing resources such as printers, scanners [1]. Under these conditions, security was not on the priority of such shared information and resources do not pose any security risk to sender/receiver. Nowadays, the use of computer has gone beyond their early intentions. They are found in the initiatives. These phenomenal changes have brought the need for tight security to data and information and they are transported across networks

In the last five decades, computer processing speed has doubled every one and half years [3]. It therefore shows that codes that took a thousand years to break with the computer available in 1960 would take a year with computer available in 2001 and these calls for security consciousness on the part of the users. [3] Defines encryption as the coding or scrambling of information so that it can only be decoded and read by someone who has the correct decoding key Encryption is a technique that transforms data from its original, unintelligent form to an intelligent cipher form so as to prevent it from Hackers.

There are few events where encryption has played important roles. During World War II, US intelligence broke a top secret super-enciphered code in which plain text was Japanese transliterated into Latin letters. When the fact that the code was broken leaked out and was published in a Chicago newspaper, the Japanese Government refused to believe that anyone would break their code and

continued to use it for the rest of the war [3]. The America's success at cracking Japanese diplomatic codes was so distinguished that they actually discovered the plans for the pearl Harbor attack before it occurred. History tells us that this was ignored to the detriment of the US. The American's magic system was used to credit Japanese cryptosystem. It was one of the first cryptanalytic devices. The Egyptian also used a simple substitution table to send secret messages to each other.

[4] Articulate the problem of the process of protecting information through its availability, privacy, and integrity. They employed a new cryptography algorithm which uses logical operation like NOR and shifting operation

[2] Focus on the securing text messages using elliptic curve cryptography and orthogonal Frequency Division Multiplexing. The researchers addressed encryption, decryption, transmission, modulation, and demodulation in a wireless environment to secure messages sent on GSM.

[7] Examine generating cipher text using system of equations: An asymmetric approach. The researchers focused on the cryptography to inherit some features from systems of nonlinear equations in such a way that information is secured against Bruce force attack between the two parties (the sender and the receiver) to disguise text and provide enhanced confidentiality and privacy in personal communications.

2.0 Proposed Work

2.1 The Proposed Hybrid Algorithm for Encrypting

- Input: Plaintext
- Output: Cipher text
- Step 1: Input plaintext
- Step 2: Scan the plaintext and delete any repeated words
- Step 3: Supply the plaintext into summary algorithm.
- Step 4: Input the resulting equation in step 3 into Advance Encryption Standard Algorithm. (AES)
- Step 5: Use AES algorithm to perform the encryption using public key.

2.2 The Detail Summary Algorithm

- **Step 1:** Count the number of words left over after the discard of repeated words to produce the public key for the algorithm.
- **Step 2:** Assign a variable index to each character position in a word. If characters are equal, assign the variable index of its previous occurrence.
- **Step 3:** Then transform each word into the form of equations below based on the numbers of public key and sums the like terms together. Send the cipher text (systems of nonlinear equations) to the intended receiver in a carrier file using delta-encoding principle.

2.3 The Proposed Algorithm is shown below:

Step 1: Let k = 1 and
Step 2: The number of word count = n
Step 3: Write the tuple (w k)
Step 4: For k =2 to n, and
Step 5: For j =1 to i-1
Step 6: If wj =w_k then 9
Step 7: Next j
Step 8: Go to step 11 and

Step 9: Write the tuple (+j, k)
Step 10: Write the tuple (w_k, k)
Step 11: Next k
Step 12: Stop

2.4 Equation Formulation

We formulated the nonlinear equations from the following algorithms:

- **Step 1:** Summarize the text using the summary method above
- **Step 2:** Count the number of words that are left, if for example, we have n words, then an n x n nonlinear equations are formulated which must fall within the allowed region of alphabetic range and other special characters that are used.
- **Step 3:** Each word is turned to an equation whose variables must not exceed n, the number of equations permitted.
- **Step 4:** We turned a word into non-linear equation by starting with x_1 and probably added or subtracted the distance of the current character from x_1. Adding a quantity representing the position of the alphabet from the position of the variables being used. For example, E is represented by (x_1+4). This quantity is always multiplied by $x_1,x_2,\ldots..,x_n$ depending on the variable we chose from left hand side for the purpose of encryption.
- **Step 5:** The resulting equations and their equivalent delta encoding are also formed.

2.5 Model Formulation

The Newton's method for non-linear systems is introduced in this section for finding the numerical values of the unknown variables. However, the problem of finding the unknown variables is much more difficulty than for linear equations. To see how the algorithm works, we demonstrated by considering a system of two nonlinear equations of the term.

$$\begin{aligned} f_1(x_1,\ x_2) &= 0 \\ f_2(x_1,\ x_2) &= 0 \end{aligned} \qquad (3.1)$$

Let $(X_1^{(0)},\ x_2^{(0)})$ be the initial estimates to the solution and be differential at. The expansion of the tangent plane to the function

$$y = f_1(x_1, x_2) \ \ at \ \ (x_1^{(0)},\ x_2^{(0)}) \ is \ldots\ldots\ldots\ldots\ldots\ldots(3.2)$$

$$y - f_1(x_1^{(0)}, x_2^{(0)}) = \frac{\partial}{\partial x_1}\left[f_1(x_1^{(0)}, x_2^{(0)}\right](x_1 - x_1^{(0)}) + \frac{\partial}{\partial x_2}\left[f_1(x_1^{(0)}, x_2^{(0)}\right](x_2 - x_2^{(0)})\ldots\ldots\ldots\ldots(3.3)$$

Similarly, the equation of the tangent plane to the function

$$y = f_2(x_1, x_2) \quad at \ \ (x_1^{(0)},\ x_2^{(0)}) \ is$$

$$y - f_2(x_1^{(0)}, x_2^{(0)}) = \frac{\partial}{\partial x_1}\left[f_2(x_1^{(0)}, x_2^{(0)}\right](x_1 - x_1^{(0)}) + \frac{\partial}{\partial x_2}\left[f_2(x_1^{(0)}, x_2^{(0)}\right](x_2 - x_2^{(0)})\ldots\ldots\ldots (3.4)$$

The intersection of these two tangent planes with the plane is obtained by solving the systems

$$\frac{\partial}{\partial x_1}\left[f_1(x_1^{(0)}, x_2^{(0)}\right]\Delta x_1^{(0)} + \frac{\partial}{\partial x_2}\left[f_1(x_1^{(0)}, x_2^{(0)}\right]\Delta x_2^{(0)} = -f_1(x_1^{(0)}, x_2^{(0)}) \text{.....(3.5)}$$

$$\frac{\partial}{\partial x_1}\left[f_2(x_1^{(0)}, x_2^{(0)}\right]\Delta x_1^{(0)} + \frac{\partial}{\partial x_2}\left[f_2(x_1^{(0)}, x_2^{(0)}\right]\Delta x_2^{(0)} = -f_2(x_1^{(0)}, x_2^{(0)}) \quad \text{.....(3.6)}$$

Where

$$\Delta x_1^j = x_1^{j+1} - x_1^j \;\; ; j = 0,1,2,\text{.....(.37)}$$

and

$$\Delta x_2^j = x_2^{j+1} - x_2^j ; j = 0,1,2,\text{.....(3.8)}$$

We solved the above equations by Gaussian elimination and the resulting solution is used to get the exact values of the unknown variables. That is,

$x_1^{(0)} = x_1^{(1)} + \Delta x_1^{(0)}$.....(3.9)

$x_2^{(0)} = x_2^{(1)} + \Delta x_2^{(0)}$.....(3.10).

We repeated the process until f_1 *and* f_2 are close to zero or $|\Delta x|_\infty = \max_i \{|\Delta|\}$ is less than a given specified tolerance value, in which case convergence has been achieved. The Variables obtained are then substituted back into the original equations to decrypt the cipher text.

2.6 Equation Formulation

Alphabet

Alphabet	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
Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

3.0 Discussion of the Proposed Method

The following examples are used to formulate equations to explain this proposed method

Detain the Bearer

Solution: Word count = 3
Number of equations = 3

Equation

D E T A I N

$x_1(x_1+3) + x_1(x_2+3) + x_1(x_3+17) + x_1(x_1+0) + x_1(x_2+7) + x_1(x_3+11)$ (3.11)

T H E

$$x_1(x_3+17) + x_1(x_1+7) + x_1(x_2+3) \quad (3.12)$$

B E A R E R

$$x_1(x_1+1) + x_1(x_2+3) + x_1(x_1+0) + x_1(x_2+16) + x_1(x_2+3) + x_1(x_2+16) \quad (3.13)$$

$$x_1^2 + 3x_1 + x_1x_2 + 3x_1 + x_1x_3 + 17x_1 + x_1^2 + x_1x_2 + 7x_1 + x_1x_3 + 11x_1 \quad (3.14)$$

$$x_1x_3 + 17x_1 + x_1^2 + 7x_1 + x_1x_2 + 3x_1 \quad (3.15)$$

$$x_1^2 + x_1 + x_1x_2 + 3x_1 + x_1^2 + x_1x_2 + 16x_1 + x_1x_2 + 3x_1 + x_1x_2 + 16x_1 \quad (3.16)$$

$$2x12 + 2x1x2 + 2x1x3 + 41x1 = 53 \quad (3.17)$$

$$x12 + x1x2 + x1x3 + 27x1 = 33 \quad (3.18)$$

$$2\,x12 + 4\,x1x2 + 0 + 39x1 = 49 \quad (3.19)$$

$$2x12 + 2x1x2 + 2x1x3 + 41x1 = 47\text{-}53 = -6 \quad (3.20)$$

$$x12 + x1x2 + x1x3 + 27x1 = 30\text{-}33 = -3 \quad (3.21)$$

$$2\,x12 + 4\,x1x2 + 0 + 39x1 = 45\text{-}49 = -4 \quad (3.22)$$

$$J(x_1, x_2, x_3) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} \frac{\partial f_1}{\partial x_2} .... \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} \frac{\partial f_2}{\partial x_2} .... \frac{\partial f_2}{\partial x_n} .. \\ \frac{\partial f_3}{\partial x_1} \frac{\partial f_3}{\partial x_2} .... \frac{\partial f_3}{\partial x_3} \end{bmatrix} = \begin{pmatrix} 4x_1 + 41 & 2x_1 & 2x_1 \\ 2x_1 + 27 & x_1 & x_1 \\ 4x_1 + 39 & 4x_1 & 0 \end{pmatrix} \quad .....(3.23)$$

$$J(x_{1k}, x_{2k}, x_{3k}) = \begin{pmatrix} 4x_{1k} + 41 & 2x_{1k} & 2x_{1k} \\ 2x_{1k} + 27 & x_{1k} & x_{1k} \\ 4x_{1k} + 39 & 4x_{1k} & 0 \end{pmatrix} \quad .....(3.24)$$

$$J(x_{1,0}, x_{2,0}, x_{3,0}) = \begin{pmatrix} 4x_{1,0} + 41 & 2x_{1,0} & 2x_{1,0} \\ 2x_{1,0} + 27 & x_{1,0} & x_{1,0} \\ 4x_{1,0} + 39 & 4x_{1,0} & 0 \end{pmatrix} \quad (3.25)$$

Where $x_{1,0}$, $x_{2,0}$, $x_{3,0}$ are initial guesses given as [1,1,1].

$$J(x_{1,0}, x_{2,0}, x_{3,0}) = \begin{pmatrix} 45 & 2 & 2 \\ 29 & 1 & 1 \\ 43 & 4 & 0 \end{pmatrix} \quad (3.26)$$

$$\begin{pmatrix} 49 & 2 & 2 \\ 31 & 1 & 1 \\ 47 & 4 & 0 \end{pmatrix} \begin{pmatrix} x_{11} - x_{1,0} \\ x_{21} - x_{2,0} \\ x_{31} - x_{3,0} \end{pmatrix} = \begin{pmatrix} f_1(x_{1,0}, x_{2,0}, x_{3,0}) \\ f_2(x_{1,0}, x_{2,0}, x_{3,0}) \\ f_3(x_{1,0}, x_{2,0}, x_{3,0}) \end{pmatrix} \quad (3.27)$$

We solve the above matrix with Gaussian elimination method to reduce the above matrix to an upper triangular form.

$$\begin{pmatrix} 49 & 2 & 2 \\ 0 & -\frac{13}{49} & -\frac{13}{49} \\ 0 & 0 & \frac{196}{49} \end{pmatrix} \begin{pmatrix} x_{11} - 1 \\ x_{21} - 1 \\ x_{31} - 1 \end{pmatrix} = -\begin{pmatrix} 6 \\ \frac{13}{49} \\ \frac{56}{7} \end{pmatrix} \text{.....(3.28)}$$

Therefore, we use backward substitution to get the unknown values involved i.e

$$\frac{196}{49}(x_{31} - 1) = \frac{56}{7}$$

$$\frac{196}{49}x_{31} - \frac{196}{49} = \frac{56}{7}$$

$$\frac{196}{49}x_{31} = \frac{56}{7} + \frac{196}{49}$$

$$x_{31} = \frac{49x588}{196x49}$$

$$x_{31} = 3$$

Again

$$-\frac{13}{49}(x_{21} - 1) - \frac{13}{49}(x_{31} - 1) = -\frac{13}{49}$$

$$1(x_{21} - 1) - 1(x_{31} - 1) = -3$$

$$-x_{21} + 1 - 1(3 - 1) = -3$$

$$-x_{21} + 1 - 2 = -3$$

$$x_{21} = 2$$

And lastly

$$49x_{11} - 49 + 6 = 6$$

$$49x_{11} = 6 - 6 + 49$$

$$49x_{11} = 49$$

$$x_{11} \quad = \quad 1$$

Now that we have calculated for values of $x_{11}=x_1$, $x_{21}=x_2$, $x_{31}=x_3$, we

Therefore translated these to our original text as follows:

To decrypt the cipher text in the above example, we go through the original equations as follows:

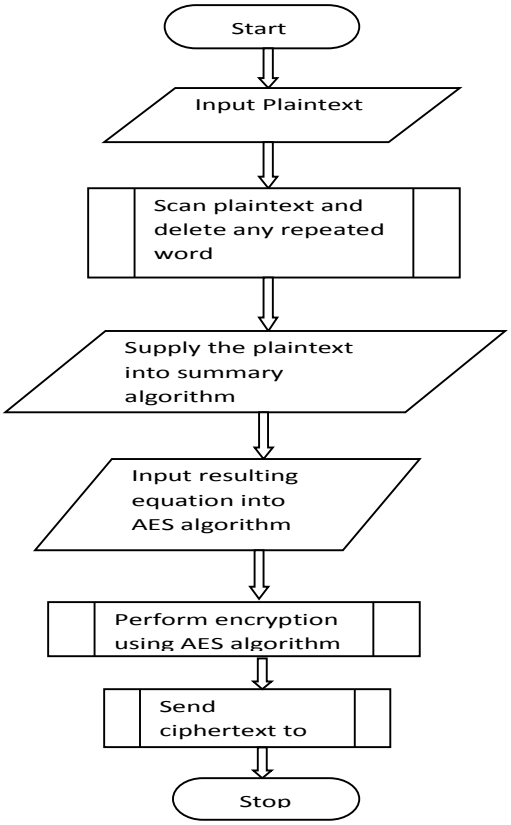
- (x_1+3) => 1+3 = 4 which is equivalent to letter **D** in the table of alphabetic
- (x_2+3) => 2+3 = 5 which is equivalent to letter **E** in the table of alphabetic
- (x_3+17) => 3+17 =20 which is equivalent to letter **T** in the table of alphabetic
- (x_1+0) => 1+0 = 1 which is equivalent to letter **A** in the table of alphabetic
- (x_2+7) => 2+7 = 9 which is equivalent to letter **I** in the table of alphabetic
- (x_3+11) => 3+11 = 14 which is equivalent to letter **N** in the table of alphabetic
- (x_3+17) => 3+17 = 20 which is equivalent to letter **T** in the table of alphabetic
- (x_1+7) => 1+7 = 8 which is equivalent to letter **H** in the table of alphabetic
- (x_2+3) => 2+3 = 5 which is equivalent to letter **E** in the table of alphabetic
- (x_1+1) => 1+1 = 2 which is equivalent to letter **B** in the table of alphabetic
- (x_2+3) => 2+3 = 5 which is equivalent to letter **E** in the table of alphabetic
- (x_1+0) => 1+0 = 1 which is equivalent to letter **A** in the table of alphabetic
- (x_2+16) =>2+16 = 8 which is equivalent to letter **R** in the table of alphabetic
- (x_2+3) => 2+3 = 5 which is equivalent to letter **E** in the table of alphabetic
- (x_2+16) => 2+16 = 18 which is equivalent to letter **R** in the table of alphabetic
- (x_1+0) => 1+0 = 1 which is equivalent to letter **A** in the table of alphabetic
- (x_2+16) =>2+16 = 8 which is equivalent to letter **R** in the table of alphabetic
- (x_2+3) => 2+3 = 5 which is equivalent to letter **E** in the table of alphabetic
- (x_2+16) => 2+16 = 18 which is equivalent to letter **R** in the table of alphabetic

Translation Method

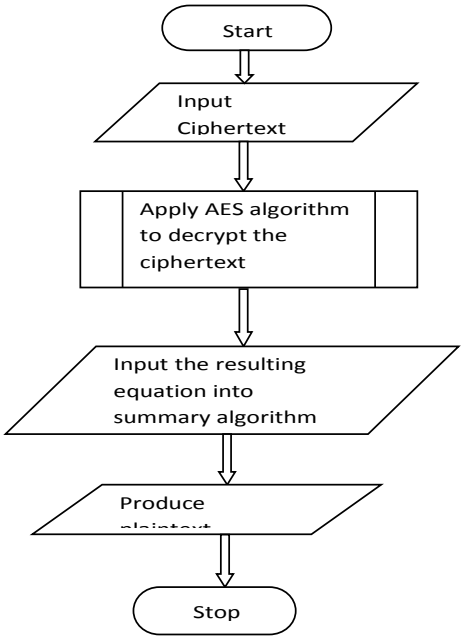
- Input: plaintext is English
- Output: plaintext in target language
- Step 1: input plaintext in English (source language)
- Step 2: Select the target language
- Step 3: perform word substitution on the plaintext.
- Step 4: produce plaintext in the target language.

Program Flowchart

Encryption



Decryption



4. Conclusion

In the world of today, where almost every aspect of our daily lives is influenced in one-way or the other by Information Technology (IT), there is a great need for us to be weary of the caliber of information we transmit over the internet. Thus, the essence of encryption of data, which is a secured and trusted method of keeping sensitive information private, is to provide adequate security abode for information against hackers and eavesdroppers.

In addition, those who are responsible for the integrity of millions of bytes of data that travel over networks, most of which are unclassified (sensitive) information, need to be security conscious about these data. This however, calls for a more secured approach to data encryption and decryption.

References

[1] A. Lee, Guideline for Implementing Cryptography in the Federal Government National Institute of Standard and Technology, Nist Special Publication, (1999), 800-821.

[2] J. Daemen and V. Rijmen, The Block Cipher Rijndeal: Smart Card Research and Application, Springer Verlag, (1998), 288-296.

[3] J. Nechvatal, M.S. Kerith and G.L. Redith, Report on the development of the advanced encryption standard (AES), *National Institute of Standards Technology*, (2002).

[4] M. Abutaha, M. Farajallah, R. Tahboub and M. Odeh, Cryptography is the science of information security, *International Journal of Computer Science and Security*, 5(2011).

[5] N. Settia, Cryptanalysis of modern cryptographic algorithms, *IJCST*, 1(2010), 166-169.

[6] P.B. Zirra and G.M. Wajiga, Cryptographic algorithms for secure data communication, *International Journal of Computer Science and Security*, 5(2011), 227-243.

[7] P.B. Zirra, G.M. Wajiga and S. Boukari, Generating cipher text using systems of equations: An asymmetric key approach, *Int. J. Pure Appl. Sci. Technol.*, 8(2012), 47-53.