J Communication, 9(1-2): 24-30 (2018)
DOI: 10.31901/24566586.2018/09.1-2.217

Encryption and Decryption of Messages in a Selected African Language Using Advanced Encryption Standard (AES) Algorithm

Tomori Rasheed Adekola[1], Olawuyi Olushola Festus[2], Adelabu Olusesan Adeyemi[3] and Oluwatosin O. Bamigboye[4*]

[1]Computer Services and Information Technology, University of Ilorin, Nigeria
[2]Centre for Open and Distance learning, University of Ilorin, Nigeria
[3]Faculty of Science and Agriculture, Department of Computer Science, University of Fort Hare, South Africa
[4]Department of Computer Science, University of Fort Hare, South Africa
E-mail: [1]<tomorirasheed@yahoo.com>, [2]festusshola@yahoo.com>, [3]<aolusesan@ufh.ac.za>, [4]<201614053@ufh.ac.za>*

KEYWORDS Data Communication. Data Integrity. Hausa Languages. Information. Security

ABSTRACT The rate of information transferred over the public network has greatly increased which has led to the challenges of data security. Information security is the process of protecting information, its availability and integrity. The objectives of this work is to design a model using mathematical approach to data encryption using Advanced Encryption Standard (AES) algorithm as well as a hybrid algorithm that employs methods of non-linear algebraic equations that will enable the intended recipient of specific message to decrypt the message in Hausa language. The system was developed using PHP as the front-end (Programming Language) and Visual Basic as the back-end (Database) running under WAMP (Window, Apache, PHP and MYSQL) Platform. When information is supply as an input, using a secret key by the user, the encrypted text is displayed on the screen for the user to see and likewise, when decrypting the already encrypted message, the secret key used for the encryption must be supplied to produce back the original message. In conclusion, the aim of the paper was to develop Encryption and decryption of messages in Hausa Language using Advanced Encryption Standard (AES) Algorithm in order to achieve maximum security level when text, file, messages and vital documents are sent across the globe.

INTRODUCTION

Cryptography involves the process of encoding of data or information before sending and decoding the data at the same time on the receiving end for the purpose of security. Many cryptographic algorithms like AES and DES are mostly used (Rani and Kaur 2017). Some vital information that is disseminated within offices, across offices, between branches of an organization and other external bodies and establishments at times gets into the hands of the unauthorized persons who tamper 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 affect the individual or organization that are concerned (AbuTaha et al. 2012).

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 in preventing interception, modifications, penetration, disclosure and enhanced data or information security are now of primary importance (Nechvatal et al. 2014). The AES algorithm used is aimed at securing the message or information that is to be transmitted across the internet.

The researchers implement Advanced Encryption Standard (AES) algorithm which replaces the data Encryption Standard (DES) that uses a 56-bit key to encrypt and decrypt information.

Literature Review

Decoding of information is the resistance of the encryption which changes the information through the process of encoding of the same information into readable form. Decode key used to reveal the encryption is called decoding key (Rashid and Rahim 2016). Encryption is devel-

oped by the governments and military establishments in providing security of private data operations (Gonsai and Raval 2014). Computer networks are primarily used by university researchers for information transfer among students, academics staff, technologies and organizations for sharing resources (Agarwal et al. 2014). Under these conditions, security is the priority of such shared information and resources so that they do not pose any security threat to sender/receiver. Nowadays, the use of computers has gone beyond their early intentions. These phenomenal changes have brought the need for tight security of data and information as they are transported across networks.

In the last five decades, as reported from the last research, computer processing speed has doubled in every one and half years (Agarwal et al. 2014). It therefore shows that codes that took a thousand years to break with the computer available in 1960 would take a year with computers available in 2001 and this calls for security consciousness on the part of the users. Encryption is a technique that transforms data from its original or unintelligent form to an intelligent cipher form so as to prevent it from Hackers.

There are few events where encryption has played important role. 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 (George and Suraj 2015). The America's success at cracking Japanese diplomatic codes was so distinguished that they actually discovered the plans for the Pearl Harbour 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 (Singh et al. 2015).

Statement of the Problem

There have been several challenges facing information sharing on a network. These include situations where the contents of the transferred documents or files on a network are hijacked by an unauthorized person due to inadequate security. Furthermore, many recipients of information are faced with the problems of adequately interpreting the content of the information that is sent to them due to language barriers.

This work addresses the problems of inadequate security in data communication. The Nigerian language that is involved in the analysis is Hausa. In order to describe some of the aspects involved, the following scenario is considered:

A situation in which the encrypted information is intercepted by unauthorized person, and subsequently, the sender is coerced to reveal the key that generated the cipher text, the result of which is that the content of the message sent is revealed. The issue is addressed by transforming the messages into nonlinear algebraic equations and a well written program in Microsoft Visual Basic. Net is implemented coupled with hybridized algorithm.

Purpose of the Study

The aim of this work is to design and implement a model for securing users information on network using Advanced Encryption Standard (AES) algorithm as well as a hybrid algorithm that employs methods of non-linear algebraic equations.

Objectives of the Study

- Introduce mathematical approach to encryption and decryption of data.
- Develop a model that will convert users' messages into a system of nonlinear equations and vice-versa using summary algorithm.
- Hybridize the summary algorithm with Advanced Encryption Standard (AES) algorithm for the purpose of data encryption and decryption.
- Implement the hybridized algorithm using appropriate tools.
- Develop a system that will enable the intended recipient of specific message to decrypt the message in Hausa language.

METHODOLOGY

Several journal articles, papers presentation and relevant past tactics work were consulted in order to have a direction for this research work.

The focus is on the algorithm and modeling formulation design of algorithm for encryption and decryption of Nigerian languages. The AES used protects privacy of email messages, documents and sensitive files by encrypting them with AES encryption algorithm as well an algorithm that employs system of nonlinear equations to provide high protection against unauthorized data access to our files and documents, while the software methodology adopted for Hausa languages is waterfall model; the system will be developed using PHP as the front-end (Programming language) and Visual Basic as the back-end (Database) running under WAMP (Window, Apache, PHP and MYSQL) Platform.

Proposed Methods

The proposed system was developed using the algorithm below. The algorithm is made up of two stages. The details of the various stages involved in this algorithm are discussed.

In protecting information within our environment using the electronic device systems such as computers, networks (for example the internet, e-commerce), mobile telephone, wireless microphone, wireless internet system, Bluetooth devices and Bank-Automatic-Teller-Machine (ATM).

To conceal the content of a message except for those intended to receive it, who knows the key that can decrypt it. Thus, it controls access to the message content making it readable to those who know the key. Without the knowledge of the key, an enemy cannot alter a message. They can alter the cipher text but when it is deciphered or decrypted, it will read as a random pattern because lack of key prevents the enemy from having control of it in the decrypted form.

The Proposed Algorithm is Shown Below:

Step 1: Let k = 1 and
Step 2: The number of word count = n
Step 3: Write the turple (w_n k)
Step 4: For k =2 to n, and
Step 5: For j =1 to i-1
Step 6: If $w_j = w_k$ then 9
Step 7: Next j
Step 8: Go to step 11 and
Step 9: Write the turple (+j, k)
Step 10: Write the turple (w_k, k)
Step 11: Next k
Step 12: Stop

Translation Method

The algorithm below was used during the translation stage:

Input:
- Encrypted text || Plain text
- D, a database

Output: Plain text in target language

```
Module Translate_Method()
 {
 Declare memory location for program elements
  inputText= get_input_text()
 If Option = Direct_Language Then
        k = input_secrete_key()
        N = Lenght(k)
        d = 32 – N
 for (i = 1; i<=d and i ≠ϕ; i ++)
          k = k & “1”
 next
 Key = byteEncoder.GetBytes(k)
 IV= byteEncoder.GetBytes (“abcdefg_ abc
 defg_” )
 Instantiate object p1 for memory data exchange
 encryption = inputText
 decryption = p1.DecryptAES(encryption, Key, IV)
 outputText = decryption
 ElseIf Option = Language_Selection Then
 inputText = get_input_text()
        strArray = Split(inputText, ” ”)
        N = UBound(strArray)
        i = 0
        ST = { w ε strArray_i }
       P = Get_Word(ST, Language_Type)
          If (P <> ” ”) Then //path to be followed if word is found
 Concat(word,P) //Perform word concatenation
    P = ” ”
    i = i + 1
  While (i <= N)
   ST = { w ε strArray_i }
 P = Get_Word(ST, Language_Type)
             If (P <> ” ”) Then
 Concat(word,P)
                P = ” ”
                i = i + 1
              Else
```

```
                P = ” ”
                J = i
                While (J <= N)
 B = J
              While (B <= N)
            If ((B <= N) And (B + 1 <= N)) Then
      ST = RightTrim(strArray_B & ” ” &
strArray_B + 1)
     P = Get_Word(ST, Language_Type)
Concat(word,P)
              B = B + 2
              J = B
              i = B
Else
P = ” ”
 ST = RightTrim(strArray_B)
 P = Get_Word(ST, Language_Type)
Concat(word,P)
        B = B + 1
        J = B
        i = B
        End If
         End While
End While
               End If
             End While
   Exit
         Else
//if not found for the first time
             i = 0
             P = ” ”
             J = i
             B = i
             While (J <= N)
  While (B <= N)
    If ((B <= N) And (B + 1 <= N + 1)) Then
                  ’’
             P = ” ”
             ST = RightTrim(strArray_B)
       P = Get_Word(ST, Language_Type)
                  If (P <> ” ”) Then
Concat(word,P)
                     B = B + 1
                     J = B
                     i = B
 Else
    ST = RightTrim(strArray_B& ” ” &
strArray_B + 1)
        P = Get_Word(ST, Language_Type)
              Concat(word,P)
              B = B + 2
              J = B
              i = B
 End If
                End If
              End While
End While
          Exit
        End If
      Else
Write “Please select language option”
End If
}
Module get_input_text()
{
return(input)
}
Module  input_secrete_key()
{
   Input “Enter your secrete key”,kl
   return kl
}
Module DecryptAES(ipt, Ky, byteEnc)
{
    Decrypt ipt with Key ‘Ky’ and byte en-
coder ‘byteEnc’ using AES algorithm
}
Module Get_Word(SText, L_Type)
{
for each SText in D using Language L_Type
{
Scan D for SText
       If ( SText ε D) then
       Fword=Equivalent_Word(SText,L_Type)
        EndIf
}
If(Fword <> “”)  Then return (Fword)
}
```

Proposed Program Flowchart

Translation

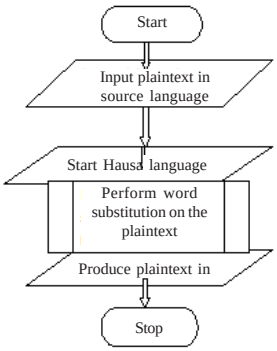

Fig. 1. Translation flowchart
Source: Author

System Design

The design phase is very important in any study for the degree of creativity and precision put into it, which determines to a large extent, the successful implementation efficiency for which the study is designed.

Any study that is not well structured in line with the proposed system would produce incorrect, misleading and perhaps disastrous output. Therefore the study must be able to take as input, comprehensible message using the secret key produced by the user. The encrypted text is likewise displayed on the screen for the user to see. Likewise, when decrypting the already encrypted message, the secret key used for the encryption must be supplied to produce back the original message.

RESULTS

The only output media for the system is the screen. The output is design to display based on the input from the users on the system. The results design proposed system is as follows:

Menu Design

The design menu of the proposed system consists of the following:

File Menu

Menu consists of the following Sub-menus: new text or file to encrypt new text or file to decrypt and exit application sub-menus.

Help Menu

Menu consists of the following sub-menus: online help and about. These are shown in Figure 1.

Input Design

The input to the proposed system is captured through a user-friendly interface shown in Figures 2 and 3. The input in Figure 2 must be a plain text to encrypt while that of Figure 3 is a cipher text. This data is converted to another form depending on the type of interface used.

New Text or File to Encrypt

The interface used allows the user to type, load text or file, or load document to encrypt. The user would then click on Encrypt button before the file, document or message is encrypted. Various options are presented on this interface for the user to make use of it. These include encrypted text, open text to encrypt and clear fields. This interface is shown in Figure 2.

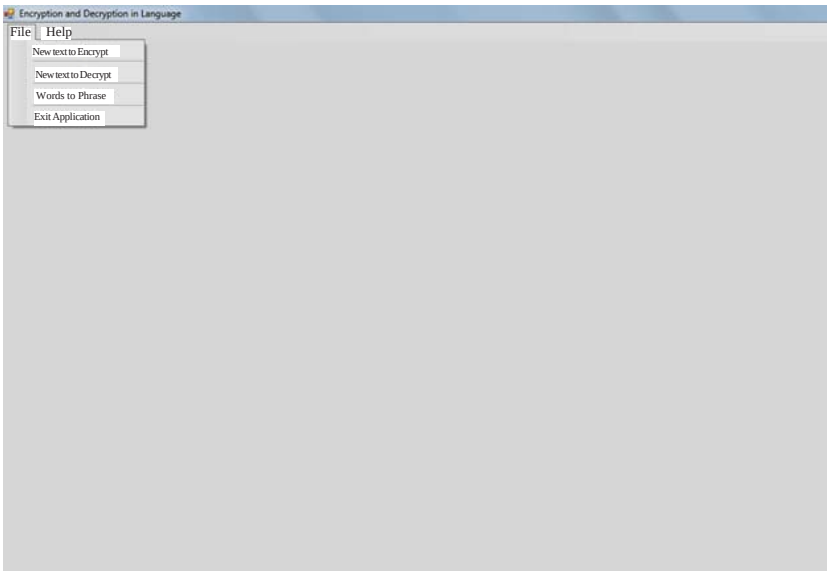

Fig. 2. Main menu screen
Source: Author

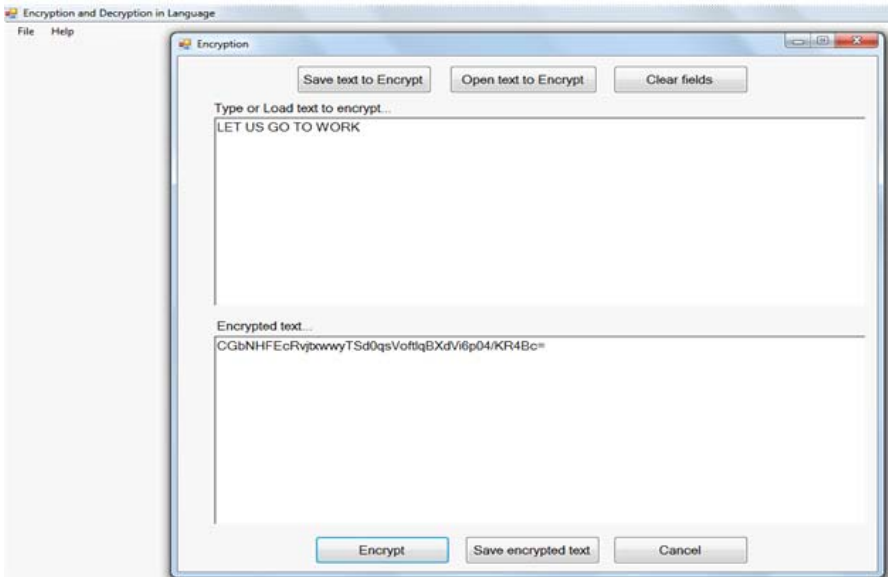

Fig. 3. New text to encrypt
Source: Author

Decryption using Hausa

Interface in Figure 3 is used to decrypt the message by selecting Hausa language from the list of language options. After choosing Hausa Language from the lists, the user will then click on decrypt button. Interface is shown in Figure 4.

DISCUSSION

System implementation is the process of making the new system operational (Wang et al. 2017). This involves design and production of necessary instruction, manuals and training materials. During the course of implementation,

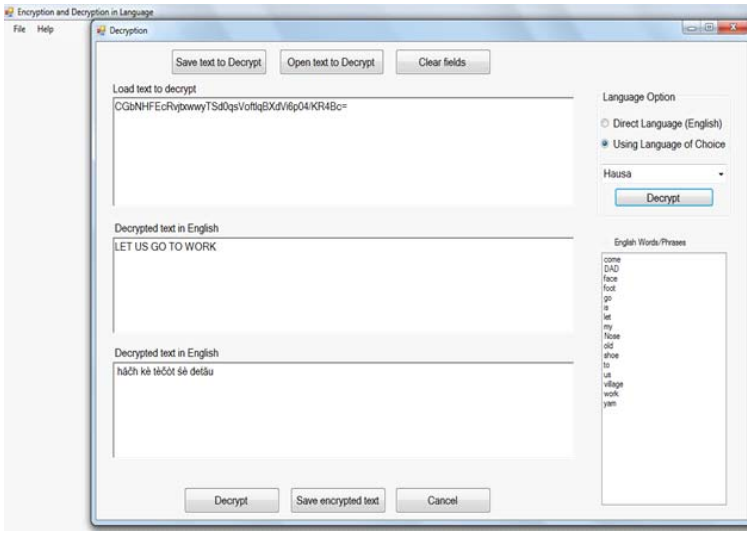

Fig. 4. Decryption
Source: Author

Microsoft Visual Basic. Net programming language was chosen simply because, it provides good facilities for modular programming techniques thus making it possible for programmers to write codes that are compact, efficient, easy to debug, modify and maintain. Also, due to the nature of the processes involved in the whole system, which include sending of data from one person to the other so as to avoid unauthorized users to have access to the documents as supported by (Wang et al. 2017). This research also supported previous research (Gonsai and Raval 2014) on the research findings.

CONCLUSION

The aim of the paper was to develop Encryption and decryption of messages in Hausa Language using Advanced Encryption Standard (AES) Algorithm in order to achieve maximum security level when text, file, messages and vital documents are sent across the globe. The proposed system hybridized known encryption and decryption algorithm called "Advanced Encryption Standard" which gives room for longer key length of 128, 192, 256 bit key and the summary algorithm. The proposed approach applied to Hausa. Microsoft Visual Basic 6.0 was implemented in order to achieve the objectives of this research work.

RECOMMENDATIONS

1. Secured hybrid algorithm should be formulated by researchers to guide against unauthorized access to sensitive information.
2. Complicated algorithm should be intensified to guide against the hackers who may want to take advantage of information.
3. Protection of information in secrete forms should be followed to guarantee the authentication of data.
4. Research work should be intensified on networks security to protect the porous posed by the users.
5. Introduction of computer securities should be in the rapid growth in the industries.
6. Computer security course syllabus should be extended in Nigeria's higher institutions of learning.

REFERENCES

AbuTaha M, Farajallah M, Tahboub R, Odeh M 2011. Survey paper: Cryptography is the science of information security. *International Journal of Computer Science and Security (IJCSS)*, 5(3): 298-309.

Agarwal V, Agarwal S, Deshmukh R 2014. Analysis and review of encryption and decryption for secure communication. *International Journal of Scientific Engineering and Research (IJSER*), 2(2): 1-3.

George SC, Suraj AA 2015. An efficient FPGA implementation of AES algorithm. *ARPN Journal of Engineering and Applied Sciences*, 10(17): 7647-7651.

Gonsai DAM, Raval LM 2014. Evaluation of common encryption algorithm and scope of advanced algorithm for simulated wireless network. *Int Journal of Computer Trends and Technology*, 11(1): 7-12.

Joan D, Rijmen V 2002. *The Design of Rijndael, AES - The Advanced Encryption Standard*. Leuven/ Belgium: Springer-Verlag.

Nechvatal J, Kerith MS, Redith GL 2012. Report on the Development of the Advanced Encryption Standard (AES). National Institute of Standards Technology. From <http://www.nist.gov/cryptoToolkit> (Retrieved on 17 August 2014).

Rani S, Kaur H 2017. Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal. *International Journal of Advanced Research in Computer Science*, 8(3): 254-258.

Rashid A, Rahim MK 2016. Critical analysis of steganography "An art of hidden writing." *International Journal of Security and Its Applications*, 10(3): 259-281.

Singh J, Lata K, Ashraf J 2015. Image encryption and decryption with symmetric key cryptography using MATLAB. *International Journal of Current Engineering and Technology*, 5(1): 448-451.

Wang M, Xing J, Wang J, Lv G 2017. Technical design and system implementation of region-line primitive association framework. *ISPRS Journal of Photogrammetry and Remote Sensing*, 130: 202-216.

Paper received for publication on August 2016
Paper accepted for publication on December 2016