World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 3, No. 3, 60-64, 2013

A Symmetric Variable–Key Stream (SVKS) Data Encryption Standard (DES) Model for Long Distance Communication

O. Osunade
Department of Computer Science,
University of Ibadan,
Ibadan, Nigeria.

Abstract— Security is very important in data transmission. Data is transmitted through unsecured paths such as the air when two devices communicate over long distances. Encryption has been adopted for securing data as it moves between the two communicating devices. Encrypted data requires a key for decrypting the message. The management and availability of the key has determined the success and adoption of encryption systems over the years. This study proposes a new key management method for the Data Encryption Standard (DES). The model developed in this research uses the DES model with modifications in the key distribution pattern. The encryption key is divided and transmitted over several media from the sender of a message to the receiver. The model also allows encryption keys of variable length as opposed to keys of fixed length in DES. This will increase the time and amount of job done for any eavesdropper to break into any encryption security thus improving the security standard of the encryption model. The model developed is secure and practicable. It is suitable for encrypting messages sent through public or social media such as email, messages, tweets and status messages.

Keywords-encryption model; key management; computer security; DES; key length; communication.

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). In implementation, key management is the hardest part of cryptography. This is because cryptanalysts often attack both symmetric and public key cryptosystem through their key management subsystem [1].

This research work improves the key distribution method in order to increase the security level provided by DES. The motivation behind this research work is to make messages that travel along pathways and reside on computer files, properly secured. This is achieved by emphasizing cryptography and improving on the key distribution aspect of the DES. The main objective is to design a mathematical model for encryption of data in long distance communication. The model developed in this research is a symmetric variable key stream encryption algorithm.

II. RESEARCH BACKGROUND

Computer communication occurs when two or more computers communicate messages over transmission media

such as twisted pair cables or airwaves. When cryptography is employed in computer communications the system shown in Figure 1 denotes the stages in the communication. In the figure Computer A is sending a message to Computer B. 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 Computer B who knows the key for decrypting the cipher text.

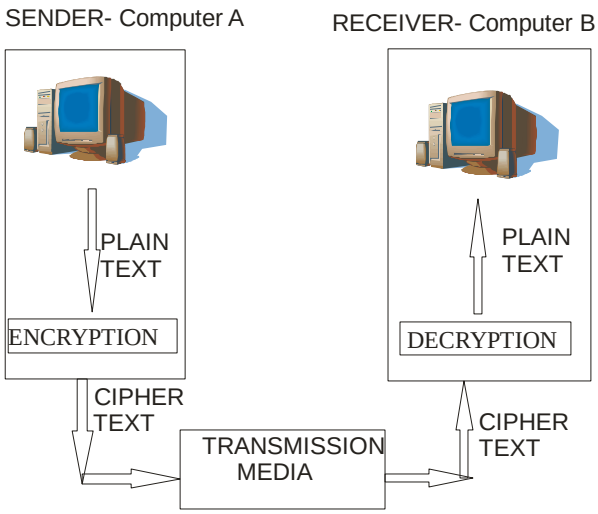

Figure 1: Communication path between two communicating devices

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 [2] 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 act can be done 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 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. 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 [3]. In the earliest and simplest ciphers, a character was the unit of data and involved either substitution or transposition.

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. 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 [3]. In the earliest and simplest ciphers, a character was the unit of data and involved either substitution or transposition.

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 [4]. 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.

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 [5]. 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 bits 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 bits key that is fixed in length. The plaintext is subjected to 19 different and complex procedures to create a 64 bits cipher text. The algorithm consists of two transposition blocks, one swapping block and 16 complex blocks called iteration blocks or Feistel cipher block [6]. 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 references [7] and [8], 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 (R1) and the second as

the left half (L1). 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)
- After the 16th round, the right and the left halves are joined and a final permutation completes the process [1].

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.

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 Twofish, 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 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.

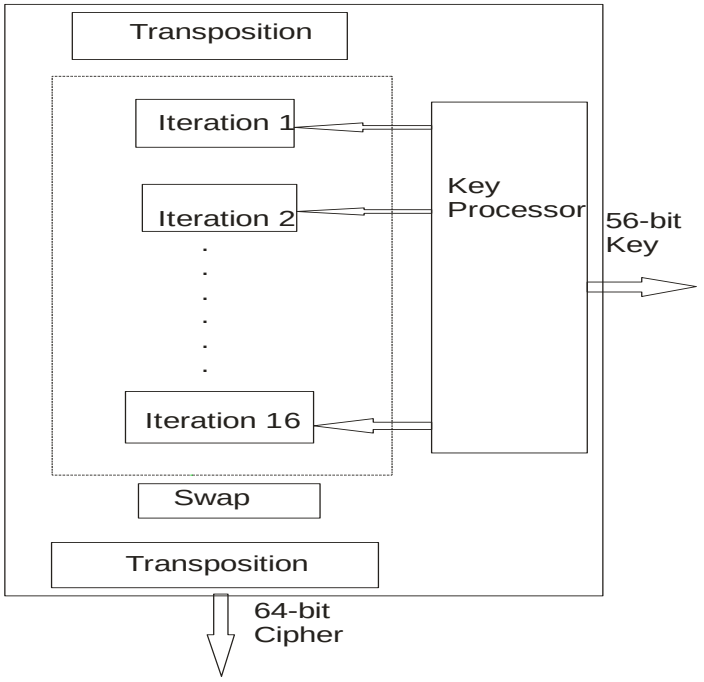

Figure 2: DES Model

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] and [12].

III. PROPOSED SOLUTION

This research work developed a mathematical model that combines existing encryption techniques. The resulting equations made provision for variable key length. The mathematical equations were then developed into a simulation program in C language.

The program consists of eleven subprograms and one main program. The subprograms helped the main program in carrying out the encryption/decryption of messages as required. The program was run using some sample data file. The program generates the output, which concealed both the organization and semantic of the sample document.

IV. THE SYMMENTRIC VARIABLE–KEY STREAM (SVKS) MODEL

The SVKS model developed in this research is a fusion of key management algorithms and modifications to the data

encryption standard (DES). The SVKS model is divided into three main modules, as shown in Figure 3 below.

- THE KEY MANAGEMENT MODULE
- THE ENCRYPTION MODULE
- THE DECRYPTION MODULE

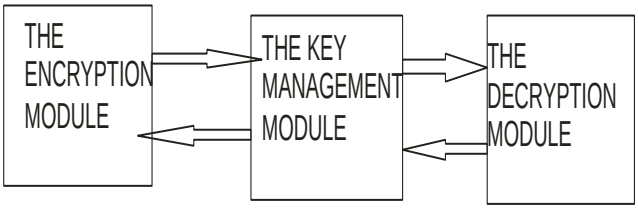

Figure 3: The block diagram of the SVKS model

A The Key Management Module

The key management module consists of five subsystems. The modules are explained briefly in the following paragraphs.

The Key Generation Subsystem: is concerned with how to generate the key to be used for the encryption/decryption process. It can be generated from a reliable random source or a pseudo-random bit generator; an acronym; a one way hash function (known as key crunching); and, specified number of character. The last option was used in this model. Any 5-letter word can be used with the last character as "E" or "D".

The Key Transfer Subsystem: is concerned with how the key components are moved from the sender to the receiver through various available media.

The Key Distribution Subsystem: is responsible for the distribution of the key used in encrypting the plaintext messages. It consists of the following functions:

The key conversion function: converts the ASCII values of the encryption key to binary numbers. It uses a function to achieve the conversion. That is, given K_x the function fc (a bijection) convert K_x to binary equivalent.

$f_c : K_x * Q_i$ {when K_x is any number to base 10 and Q is base 2 of K_x

The K_x is the domain of the function while the Q_i is the co-domain of the function. For example:

given $K_x = 12_{10}$; f_c converts K_x to $Q_i = 1100_2$.

The key dividing function: divides the bits sequence obtained from the key conversion module into "i" values. This is done if the number of bits is divisible by 4, otherwise it pads the bits with zeroes before dividing them.

Given $q = \{a_1, a_2, a_3 \text{ ------- } a_n\} \in Q, \ni F_d$ (a bijective function), such that

$$F_d : Q_iL \rightarrow Q_l^l$$

Where $Q_l^l = q_1, q_2$ ------- q_k e.g.

$$q_1 = \{a_i \, 1 \, \forall i, \, 1 \leq i \leq 4\}, \, q2$$

$$q_2 = \{ a_i \, 1 \, \forall i, \, 5 \leq i \leq 8\}$$

$$iq_k = \{ a_i \, 1 \, \forall i, \, n - 4 \leq i \leq n\}.$$

The key distribution function: is responsible for sending one set of 4 bits obtained from the key–dividing function to either the encryption module for clear text encryption or the decryption module for cipher text decryption.

$$F_{ed}: q_i \rightarrow K_i.$$

This function maps each 4-turple to key components for the intended iterations i.e. the first K_1 is equivalent to the first key component q1, the second K_2 is equal to the second key components q_2 and so on.

The function Fed is also a bijection. For instance during encryption the key components K_1, K_2, K_3 …… K_n are transferred to the computational module in this order while the reverse is the case during decryption.

B The Encryption Module

The mathematical model for encryption module is contained in the computational sub model. The computational sub-module is responsible for the splitting of the 8-bit plaintext block into two halves and subjecting these sub-blocks to a series of key independent computations. The block of data (8 bits) is split into two halves consisting of 4-bits each. Mathematically,

$$b = b^1 b^2 \qquad \text{where } b^1 = \{b^i/\forall i, \, 1 \leq i \leq 4\}$$

$$b^2 = \{b^i/\forall i, \, 5 \leq i \leq 8\}.$$

The halves are combined with the key and processed through the three steps below "i" number of times depending on the size of the key.

$$b^2{}_i = K_i \, (+) \, b^2{}_{i-1} \, (+) \, b_{i-1} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$b^1{}_i = b^1{}_{i-1} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$c = b_i \, b^2{}_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

After the final iteration, the two halves are combined together to get the 8-bits cipher text.

C The Decryption Module

The mathematical representation of the module responsible for the conversion of the cipher text to the original text or plaintext is the model used in encrypting the original message. The only difference is that if the key components are used in ascending order for encryption, they are now used in descending order when decrypting. This is the advantage of using a symmetric key algorithm.

V. CONCLUSION

In this research work, a symmetric variable-key stream (SVKS) encryption model was developed based on the DES. The model guarantees the privacy and integrity of e-mail or files transferred. The SVKS model improves on the key distribution pattern of the DES. The SVKS model offers better security than the current DES in the following way: it has a variable key length unlike the current DES with 64 bits

fixed length; the splitting of the encryption key into parts and transmitting them over different media denies single access to the key; and it also offers flexibility and ingenuity in the area of key generation and distribution over long distances.

REFERENCES

1. Schneier, C. 1996. Applied Cryptography. John Wiley & Sons, Inc., New York pp.20-250.
2. Neumann, P. 1994. Computer Security. Issues in Science and Technology, pp.50-54.
3. Cohen, F. 1995. A Short History of Cryptography. http://all.net/edu/curr/ip/Chap2-1.html. retrieved 12 February 2011
4. 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
5. U.S. Department of Commerce/National Institute of Standards and Technology. 1999. Data Encryption Standard (DES), FIPS-Pub.46. Federal Information Processing Standards Publication. Reaffirmed 1999 October 25
6. Forouzan, B.A. 2005. Data Communication and Networking. 3rd Edition Tata McGraw-Hill Publishing Company limited.
7. Whitfield, D. and Hellman, M. 1976. Privacy and Authentication: An Introduction to Cryptography. Proceedings of IEEE, Vol. 67, No 3, pp. 397-427
8. U.S. Department of Commerce/National Institute of Standards and Technology. 1980. 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
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, D.J.S.; Sicat, G.C.E.; Niguidula, J.D.; Chavez, E.P. and Hernandez, A.A. 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
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.

AUTHORS PROFILE

OSUNADE Oluwaseyitanfunmi is a member of IEEE and the Nigeria Computer Society. He has a PhD in Computer Science from University of Ibadan, Nigeria. He specializes in computer networks and data communication systems.