Volume 1, No. 3, October 2010

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

SECURE E-MESSAGING SCHEME USING SYMMETRIC KEY ENCRYPTION - EHDES

Awakash Mishra[1] and Deo Brat Ojha*[2],

[1](Research Scholar Singhania University, Jhunjhunu, Rajsthan)
Department of M.C.A, Raj Kumar Goel Engineering College, Ghaziabad, U.P., INDIA
awakashmishra@gmail.com
*[2] Deptt. Of mathematics, R. K. G. Institute of Technology, Gzb., U.P.(India),
deobratojha@rediffmail.com

Abstract: In this article, we present a secure scheme of e-messaging system for communication. It is the model of a high level secure mailing scheme for any organization. In this model, anyone can send a secret message even to any strange person in an unidentified way. The users of this model are assumed to be may or may not be the members of a closed organization. In the current era of communication, message security is too much important due to more usability of users and increases the stealing rapidly over internet.

Keywords: Message, EHDES, Stegnography, Covert Mailing System, Random Number.

INTRODUCTION

Steganography has a relatively short history; even today ordinary dictionaries do not contain the word "steganography". Books on steganography are still very few [1], [2].

The most important feature of this steganography is that it has a very large data hiding capacity [3], [4]. Steganography can be applied to variety of information systems. Some key is used in these systems when it embeds/extracts secret data. One natural application is a secret mailing system [5], [6] that uses a symmetric key. Another application pays attention to the nature of steganography whereby the external data (e.g., visible image data) and the internal data (any hidden information) cannot be separated by any means. We will term this nature as an "inseparability" of the two forms of data.

In this current paper, we will show an example of a mixed scheme of stegnography and cryptography are Secure E-Messaging Scheme Using Symmetric Key Encryption – EHDES, which are an anonymous and covert e-mailing system with complete security.

Present paper is as follows. In Section 2 describes the scheme of enhanced data encryption standard (EHDES) Section 3 we will show a secure messaging scheme using symmetric key. How we can make it a safe system in Section 4. Finally, section 5 is conclusion.

PRELIMINERIES

The amount of transfer messaging has increased rapidly on the Internet. Cryptography is a branch of applied mathematics that aims to add security in the ciphers of any kind of messages. Cryptography algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. The data integrity aims to verify the validity of data contained in a given document. [7]

Enhanced Data Encryption Standard (EHDES)

In Enhanced Data Encryption Standard (EHDES) [8], [9], [14], we use the block ciphering of data and a symmetric key. As traditional Data Encryption Standard (DES), we also break our data into 64-Bit blocks and use a symmetric key of 56-Bit.

EHDES having three phases:

1. Key Generation.
2. Encryption on Input Data.
3. Decryption on Input Cipher.

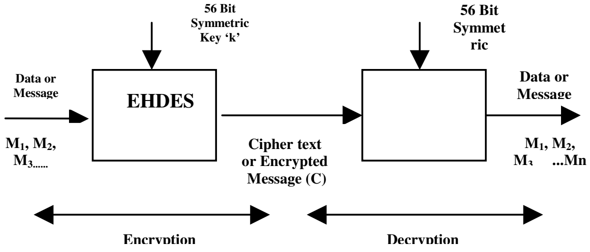

Figure 1: Encryption and Decryption process of EHDES.

Key Generation: In this phase of EHDES, We moderate the initial 56 Bit key using Random Number Generator (RNG) [10], [11], [12], [13] for every block of message (M_1, M_2, M_3 $_{...Mn}$). The new generated 56 Bit keys ($K_{new1,}$ $K_{new2,}$ $K_{new3...............}$ $K_{new\ n}$) from initial key K is used for encryption and decryption for each block of data. For new keys, we generate a random number and implement a function F on generated random number (N_{RNG}) and the initial key K.

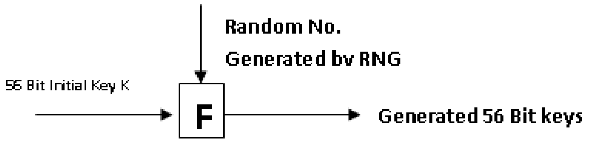

Figure 2: Process of new generated key ($K_{new\ i}$) of EHDES.

Encryption on Input Data: As we know Data Encryption Standard (DES) is based on block cipher scheme. Message breaks in 64 Bit n blocks of plain text.

$$\mathbf{M = \{M_1, M_2, M_3, \ldots\ldots, M_n\}}$$

Now, we encrypt our message $\{M_1, M_2, M_3, \ldots\ldots, M_n\}$ blocks by each new generated key

$$K_{new1}, K_{new2}, K_{new3} \ldots\ldots K_{new\ n}.$$

Decryption on Input Cipher: Decryption is the reverse process of encryption. For decryption, we also used the same key which is used in encryption. On the receiver side, the user also generate the same new key $K_{new\ i}$ for each block of cipher and generate plain text through decryption process of data encryption standard.

A MODEL OF AN E-MAILING SYSTEM

Secure E-Messaging Scheme Using Symmetric Key Encryption –EHDES (SEMSUSK-E) is a steganography application program with cryptography. In the following description, $M_{SES_{EHDES^I}}$ denotes a member $SES_{EHDES}I$, and $M_{SES_{EHDES^{II}}}$ denotes a member $SES_{EHDES}II$.

An SEMSUSK-E consists of the three following components.

1. Envelope Producer (EP).
2. Message Inserter (MI).
3. Envelope Opener (EO).

We denote $M_{SES_{EHDES^I}}$'s SEMSUSK-E as $SEMSUSK - E_I$ (i.e., customized SEMSUSK by $M_{SES_{EHDES^I}}$. So, it is described as $M_{SES_{EHDES^I}} = (EP_{SES_{EHDES^I}}, MI_{SES_{EHDES^I}}, EO_{SES_{EHDES^I}})$. $EP_{SES_{EHDES^I}}$ is a component that produces $M_{SES_{EHDES^I}}$'s envelope $(E_{SES_{EHDES^I}})\ and\ a\ f = \Sigma$. $E_{SES_{EHDES^I}}$ is the envelope (actually, an image file) which is used by all other members in the organization when they send a secret message to $M_{SES_{EHDES^I}}$. $(EO_{SES_{EHDES^I}})$ is produced from an original image (EO) . $M_{SES_{EHDES^I}}$ can select it according to his preference. $(E_{SES_{EHDES^I}})$ has both the name and e-mail address of $M_{SES_{EHDES^I}}$ on the envelope surface (actually, the name and address are "printed" on image $(E_{SES_{EHDES^I}})$. It will be placed with function f at an open site in the organization so that anyone can get it freely and use it any time. Or someone may ask $M_{SES_{EHDES^I}}$ to send it directly to him/her. $(MI_{SES_{EHDES^I}})$ is the component to insert (i.e., embed according to the steganographic scheme) $M_{SES_{EHDES^I}}$'s message into another member's (e.g., $M_{SES_{EHDES^{II}}}$)'s envelope $(E_{SES_{EHDES^{II}}})$ when $M_{SES_{EHDES^I}}$ is sending a secret message $(Mess._{SES_{EHDES^I}})$ to $(M_{SES_{EHDES^{II}}})$. One important function of $M_{SES_{EHDES^I}}$ is that it detects a key $(Key_{SES_{EHDES^I}})$ that has been hidden in the envelope$(E_{SES_{EHDES^{II}}})$, and uses it when inserting a message $(Mess._{SES_{EHDES^I}})$ in $(E_{SES_{EHDES^{II}}})$. $(EO_{SES_{EHDES^I}})$ is a component that opens (extracts) $(E_{SES_{EHDES^I}})$'s "message inserted" envelope $(E_{SES_{EHDES^I}}(Mess._{SES_{EHDES^{II}}}))$ which $M_{SES_{EHDES^I}}$ received from someone as an e-mail attachment. The sender $(M_{SES_{EHDES^{II}}})$ of the secret message $(Mess._{SES_{EHDES^{II}}})$ is not known until $M_{SES_{EHDES^I}}$ opens the envelope by using$(EO_{SES_{EHDES^I}})$.

CUSTOMIZATION OF A SEMSUSK-E

Customization of an SEMSUSK-E for member $(M_{SES_{EHDES^I}})$ takes place in the following way. $(M_{SES_{EHDES^I}})$ first decides a key $(Key_{SES_{EHDES^I}})$ with $f = \sum_{i=1}^{n} i$ where i is a positive integer, when he/she installs the SEMSUSK-E onto his computer. Let us suppose $SES_{EHDES}II$ try to communicate at any time t, then he/she picks up a number randomly form i. Now, SEMSUSK-E generates $f_t = \sum_{i=1}^{n-1} i$. Let $R = f - f_t$, SEMSUSK-E generate a key $(Key_{SES_{EHDES^I}})$ with the help of R using EHDES key generation process. Then he types in his name $(Name_{SES_{EHDES^I}})$ and e-mail address $(Email\ adr_{SES_{EHDES^I}})$. $(Key_{SES_{EHDES^I}})$ is secretly hidden (according to a steganographic procedure in his envelope $(E_{SES_{EHDES^I}})$. This $(Key_{SES_{EHDES^I}})$ is eventually transferred to a message sender's $(MI_{SES_{EHDES^{II}}})$ in an invisible way. $(Name_{SES_{EHDES^I}})$ and $(Email\ adr_{SES_{EHDES^I}})$ are printed out on the envelope surface when $(M_{SES_{EHDES^I}})$ produces $(E_{SES_{EHDES^I}})$ by using $(EP_{SES_{EHDES^I}})$. $(Key_{SES_{EHDES^I}})$ is also set to $(EO_{SES_{EHDES^I}})$, when communicators wish to start the communication. $(Name_{SES_{EHDES^I}})$ and $(Email\ adr_{SES_{EHDES^I}})$ are also inserted (actually, embedded) automatically by $(MI_{SES_{EHDES^I}})$ any time $(M_{SES_{EHDES^I}})$ inserts his message $(Mess._{SES_{EHDES^I}})$ in another member's envelope $(E_{SES_{EHDES^{II}}})$. The embedded $(Name_{SES_{EHDES^I}})$ and $(Email\ adr_{SES_{EHDES^I}})$ are extracted by a message receiver $(M_{SES_{EHDES^{II}}})$ by $(EO_{SES_{EHDES^{II}}})$.

HOW IT WORKS

When some member $(M_{SES_{EHDES^{II}}})$ wants to send a secret message $(Mess._{SES_{EHDES^{II}}})$ to another member $(M_{SES_{EHDES^{I}}})$, whether they are acquainted or not, $(M_{SES_{EHDES^{II}}})$ gets (e.g., downloads) the $(M_{SES_{EHDES^{I}}})$'s envelope $(E_{SES_{EHDES^{I}}})$, and uses it to insert his message $(Mess._{SES_{EHDES^{II}}})$ by using $(MI_{SES_{EHDES^{II}}})$. When $(M_{SES_{EHDES^{II}}})$ tries to insert a message, $(M_{SES_{EHDES^{I}}})$'s key $(Key_{SES_{EHDES^{I}}})$ is transferred to $(MI_{SES_{EHDES^{II}}})$ automatically in an invisible manner, and is actually used. $(M_{SES_{EHDES^{I}}})$ can send $(E_{SES_{EHDES^{I}}}(M_{SES_{EHDES^{II}}}))$ directly, or ask someone else to send it to $(M_{SES_{EHDES^{I}}})$ as an e-mail attachment. $(M_{SES_{EHDES^{II}}})$ can be anonymous because no sender's information is seen on $(E_{SES_{EHDES^{I}}}(M_{SES_{EHDES^{II}}}))$. $(Mess._{SES_{EHDES^{II}}})$ is hidden, and only $(M_{SES_{EHDES^{I}}})$ can see it by opening the envelope. It is not a problem for $(M_{SES_{EHDES^{II}}})$ and $(M_{SES_{EHDES^{I}}})$ to be acquainted or not because $(M_{SES_{EHDES^{II}}})$ can get anyone's envelope from an open site.

CONCLUSION

SEMSUSK-E is a very easy-to-use system because users are not bothered by any key handling, as the key is always operated automatically. As SEMSUSK-E doesn't need any authorization bureau, this system can be very low cost. All these features overcome the drawbacks of an encrypted mailing system

REFERENCES

[1] Stefan Katzenbeisser and Fabien A.P. Petitcolas (eds), "Information hiding techniques for steganography and digital watermarking", Artech House, 2000.

[2] Neil F. Johnson, Zoran Duric and Sushil Jajodia,"Information Hiding", Kluwer Academic Publishers, 2001.

[3] M. Niimi, H. Noda and E. Kawaguchi,"An image embedding in image by a complexity based region segmentation method", Proceedings of International Conf. on Image Processing'97, Vol.3, pp.74-77, Santa Barbara, Oct., 1997.

[4] E. Kawaguchi and R. O. Eason,"Principle and applications of BPCS-Steganography", Proceedings of SPIE: Multimeda Systems and Applications, Vol.3528, pp.464-463, 1998.

[5] E. Kawaguchi, et al, "A concept of digital picture envelope for Internet communication" in Information modeling and knowledge bases X, IOS Press, pp.343-349, 1999.

[6]Eiji Kawaguchi, Hideki Noda, Michiharu Niimi and Richard O. Eason, "A Model of Anonymous Covert Mailing System Using Steganographic Scheme, Information modelling and knowledge bases X",IOS Press, pp.81-85,2003.

[7] Diego F. de Carvalho, Rafael Chies, Andre P. Freire, Luciana A. F. Martimiano and Rudinei Goularte, "Video Steganography for Confidential Documents: Integrity, Privacy and Version Control" , *University of Sao Paulo – ICMC, Sao Carlos, SP, Brazil, State University of Maringa, Computing Department,* Maringa, PR, Brazil.

[8] Ramveer Singh , Awakash Mishra and D.B.Ojha "An Instinctive Approach for Secure Communication – Enhanced Data Encryption Standard (EHDES)" *International journal of computer science and Information technology,* , Vol. 1 (4) , 2010, 264-267.

[9] D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati Garg "An Innovative Approach to Enhance the Security of Data Encryption Scheme*" International Journal of Computer Theory and Engineering*, Vol. 2,No. 3, June, 2010,1793-8201.

[10] R. B. P. Dept. The Evaluation of Randomness of RPG100 by Using NIST and DIEHARD Tests. Technical report, FDK Corporation, 2003.

[11] B. Jun and P. Kocher. The Intel Random Number Generator. Cryptography Research Inc. white paper, Apr. 1999.

.[12] P. Kohlbrenner and K. Gaj. An embedded true random number generator for fpgas. In FPGA '04: Proceeding of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays, pages 71–78. ACM Press, 2004.

[13] C. Petrie and J. Connelly. A Noise-based IC Random Number Generator for Applications in Cryptography. IEEE TCAS II, 46(1):56–62, Jan. 2000.

[14] Ramveer Singh and Deo Brat Ojha," An Approach to Compress & Secure Image Communication", International Journal of Computational Intelligence and Information Security, Vol. 1 No. 7, September 2010.