International Journal of Information Sciences and Application.
ISSN 0974-2255 Volume 3, Number 1 (2011), pp. 11-17

http://www.irphouse.com

Globally Reliable E-Mail: An Application of Triple-EHDES over Teeming Channel

Ramveer Singh[1*], Awakash Mishra[2], Akshay Tyagi[3] and Deo Brat Ojha[4]

*[*1](Research Scholar Singhania University, Jhunjhunu, Rajsthan)*
Department of Information Technology,
R. K. G. Institute of Technology, Ghaziabad, U.P., India
E-mail: ramveersingh_rana@yahoo.co.in
[2](Research Scholar Singhania University, Jhunjhunu, Rajsthan)
Department of M.C.A., Raj Kumar Goel Engineering College,
Ghaziabad, U.P., India
E-mail: awakashmishra@gmail.com
[3](Research Scholar Mewar University, Chittorgarh, Rajasthan))
Gradute School of Business & Administration, Greater Noida, U.P., India
E-mail: akshaytyagi@airtelmail.in
[4]Deptt. of Mathematics, R. K. G. Institute of Technology, G, U.P.(India),
E-mail: deobratojha@rediffmail.com

Abstract

In this paper, we presented an errorless procedure of e-mailing system for Internet communication. It is the model of a real-life secure mailing system for any organization. In this model anyone can send a secret message even to any strange person in an anonymous way. The users of this model are assumed to be may or may not be the members of a closed organization. If any error occurred during the transmission due to teeming channel, it can also be determine & encountered by error correction function.Triple EHDES is used to provide supreme level of security.

Keywords: Message, EHDES, Triple EHDES, Stegnography, Covert Mailing System, Random Number, Fuzzy Error Correcting Code.

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 the power of a mixed scheme of stegnography and cryptography with error correction code, are Secure E-Messaging Scheme Using Symmetric Key Encryption –Triple EHDES, which are an anonymous and covert e-mailing system with complete security [15].

Present paper is as follows. Section 2, describes the scheme of Triple enhanced data encryption standard (T-EHDES) and method of error correction code.In 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.

Preliminaries

Now the use of internet is increasing rapidly. The amount of transfer messaging has increased rapidly on the Internet. The pivotal role of cryptography is, it provides the process of encryption and decryption. Cryptography algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. [7], [9], [14].

Triple EHDES

Triple EHDES uses the cascading or chain of Enhanced DataEncryption Standard (EHDES) [7, 8].

Let EK(P.T.) and DK(P.T.) represent the EHDES encryption and decryption of P.T. using EHDES key K respectively. Each EHDES encryption/decryption operation is a compound operation of EHDES encryption and decryption operations.

The standard specifies the following keying options for bundle (K1, K2, and K3)

1. Keying Option 1: K1, K2 and K3 are independent keys.
2. Keying Option 2: K1 and K2 are independent keys and K3 = K1.
3. Keying Option 3: K1 = K2 = K3.

Key Generation

Message breaks in 64 Bit n blocks of plain text.

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

Now, we encrypt our message $\{M_1, M_2, M_3, \ldots\ldots, M_n\}$ blocks by each new generated key $K_{new1}, K_{new2}, K_{new3} \ldots\ldots K_{new\ n}$. with the help of F and random number.[10, 11, 12. 13]

Encryption on Input Data

The transformation of a 64-bit block P.T. into a 64-bit block C.T. that is defined as follows:

C.T = EK3 (DK2 (EK1 (P.T.))).

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. the transformation of a 64-bit block P.T into a 64-bit block C.T. that is defined as follows:

P.T. = DK1 (EK2 (DK3 (C.T.))).

Error Correction Code

A metric space is a set C with a distance function dist : $C \times C \rightarrow R^{+} = [0, \infty)$, which obeys the usual properties(symmetric, triangle inequalities, zero distance between equal points)[16,17].

Definition: Let $C\{0,1\}^{n}$ be a code set which consists of a set of code words c_i of length n. The distance metric between any two code words c_i and c_j in C is defined by $$dist(c_i, c_j) = \sum_{r=1}^{n} \left| c_{ir} - c_{jr} \right| \qquad c_i, c_j \in C$$

This is known as Hamming distance [18].

Definition: An error correction function f for a code C is defined as $f(c_i) = \{c_j / dist(c_i, c_j) \text{ is the minimum, over } C - \{c_i\}\}$. Here, $c_j = f(c_i)$ is called the nearest neighbor of c_i [16].

Definition: The measurement of nearness between two code words c and c' is defined by $\text{nearness}\ (c, c') = dist(c, c') / n$, it is obvious that $0 \le \text{nearness}\ (c, c') \le 1$ [18].

Definition: The fuzzy membership function for a codeword c' to be equal to a given c is defined as[13]

$$FUZZ(c') = 0 \qquad \text{if nearness}(c, c') = z \le z_0 < 1$$
$$= z \qquad \text{otherwise}$$

A model ofGlobally Reliable E-Mail: An Approach of Triple EHDES (GREAT-E).

Globally Reliable E-Mail: An Application of Triple-EHDES (GREAT-E) is a stegnography application program with cryptography. In the following description,$M_{GREAT-E}1$, denotes a member *of*GREAT-E I, and $M_{GREAT-E}2$,denotes a member of GREAT-E 2.

AGREAT-E consists of the three following components.

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

We denote$M_{GREAT-E}1$'s GREAT-E as GREAT-E1 (i.e., customized GREAT-E by$M_{GREAT-E}1$. So, it is described as$M_{GREAT-E}1 = (EP_{GREAT-E}1, MI_{GREAT-E}1, EO_{GREAT-E}1)$. $EP_{GREAT-E}1$is a component that produces $M_{GREAT-E}1$'s envelope $(E_{GREAT-E}1.)\ and a f = \sum_{i=1}^{n} i$. $E_{GREAT-E}1$is the envelope (actually, an image file) which is used by all other members in the organization when they send a secret message to $M_{GREAT-E}1$. $(EO_{GREAT-E}1)$is produced from an original image$(EO\ \ )$. $M_{GREAT-E}1$can select it according to his preference. $(E_{GREAT-E}1)$has both the name and e-mail address of $M_{GREAT-E}1$on the envelope surface (actually, the name and address are "printed" on image $(E_{GREAT-E}1)$. 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 $M_{GREAT-E}1$to send it directly to him/her. $(MI_{GREAT-E}1)$is the component to insert (i.e., embed according to the stegnographic scheme) $M_{GREAT-E}1$'s message into another member's (e.g., $M_{GREAT-E}2$)'s envelope $(E_{GREAT-E}2)$ when $M_{GREAT-E}1$is sending a secret message ($Mess._{GREAT-E}\ 1$) to ($M_{GREAT-E}1$). One important function of $M_{GREAT-E}1$is that it detects a key $(Key_{GREAT-E}1)$ that has been hidden in the envelope$(E_{GREAT-E}2)$and uses it when inserting a message ($Mess._{GREAT-E}\ 1$)in$(E_{GREAT-E}2)$. $(EO_{GREAT-E}1)$is a component that opens (extracts)$(E_{GREAT-E}1)$'s "message inserted" envelope $(E_{GREAT-E}1(\ Mess._{GREAT-E}\ 2))$which $M_{GREAT-E}1$received from someone as an e-mail attachment. The sender ($M_{GREAT-E}2$) of the secret message ($Mess._{GREAT-E}\ 2$)is not known until $M_{GREAT-E}1$opens the envelope by using$(EO_{GREAT-E}1)$.

Customization of Great-E

Customization of a GREAT-E for a member ($M_{GREAT-E}1$)takes place in the following way. ($M_{GREAT-E}1$), first decides a key $(Key_{GREAT-E}1)$with $f = \sum_{i=1}^{n} i$ where i is a positive integer, when he/she installs the GREAT-E onto his computer. Let us suppose $E_{GREAT-E}2$ try to communicate at any time t, then he/she picks up a number randomly form i. Now, GREAT-E generates$f_t = \sum_{i=1}^{n-1} i$. Let $R = f - f_t$, GREAT-E generate a key $(Key_{GREAT-E}1)$with the help of R using Triple EHDES key generation process. Then he types in his name $Name_{GREAT-E}1$and e-mail address

$(Emailadr_{GREAT-E}1)$. $(Key_{GREAT-E}1)$is secretly hidden (according to a steganographic procedure in his envelope $(E_{GREAT-E}1)$.This$(Key_{GREAT-E}1)$is eventually transferred to a message sender's $(MI_{GREAT-E}2)$in an invisible way.$(Name_{GREAT-E}1)$ and$(Emailadr_{GREAT-E}1)$are printed out on the envelope surface when $(M_{GREAT-E}1)$produces $(E_{GREAT-E}1)$by using $(EP_{GREAT-E}1)$. $(Key_{GREAT-E}1)$is also set to $(EO_{GREAT-E}1)$. When communicators wishto start the communication.$(Name_{GREAT-E}1)$and$(Emailadr_{GREAT-E}1)$are also inserted (actually, embedded) automatically by $(MI_{GREAT-E}1)$any time $(M_{GREAT-E}1)$inserts his message ($Mess._{GREAT-E}1$)in another member's envelope $(E_{GREAT-E}2)$. The embedded $(Name_{GREAT-E}1)$and $(Emailadr_{GREAT-E}1)$are extracted by a message receiver $(M_{GREAT-E}2)$by$(EO_{GREAT-E}2)$.

How it works

When some member $(M_{GREAT-E}2)$wants to send a secret message ($Mess._{GREAT-E}2$)to another member $(M_{GREAT-E}1)$, whether they are acquainted or not, $(M_{GREAT-E}2)$gets (e.g., downloads) the $(M_{GREAT-E}1)$'s envelope $(E_{GREAT-E}1)$, and uses it to insert his message ($Mess._{GREAT-E}2$)by using $(MI_{GREAT-E}2)$. When $(M_{GREAT-E}2)$tries to insert a message,$(M_{GREAT-E}1)$'s key $(Key_{GREAT-E}1)$is transferred to $(MI_{GREAT-E}2)$automatically in an invisible manner, and is actually used. $(M_{GREAT-E}2)$can send $(E_{GREAT-E}1(M_{GREAT-E}2))$directly, or ask someone else to send, it to $(M_{GREAT-E}1)$as an e-mail attachment with using encryption process of Triple EHDES on $(E_{GREAT-E}1(M_{GREAT-E}2))$. $(M_{GREAT-E}2)$can be anonymous because no sender's information is seen on$(E_{GREAT-E}1(M_{GREAT-E}2))$.($Mess._{GREAT-E}2$)is hidden, and only $(M_{GREAT-E}1)$can see it by opening the envelope. It is not a problem for $(M_{GREAT-E}2)$and $(M_{GREAT-E}1)$to be acquainted or not because $(M_{GREAT-E}2)$can get anyone's envelope from an open site.

Error Correction

Receiver check that $dist(t(c)c') > 0$, he will realize that there is an error occur during the transmission. Receiver apply the error correction function f to $c' : f(c)$.

Then receiver will compute nearness $(t(c), f(c')) = dist(t(c) f(c')) / n$

$$FUZZ(c') = 0 \quad \text{if nearness}(c, c') = z \le z_0 < 1$$
$$= z \quad \text{otherwise}$$

Conclusion

Section 3 and 4 itself shows the strength and security of Globally Reliable E-Mail: An Application of Triple-EHDES over Teeming Channel. The attraction and usability of this application is, it's also having the feature of error detection and correction using error correction code.

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, ZoranDuric and SushilJajodia,"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, MichiharuNiimi 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 RudineiGoularte, "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.

[15] G. Lo-varco,W. Puech, and M. Dumas. “Dct-based watermarking method using error correction codes”, In ICAPR’03, International Conference on Advances inPattern Recognition, Calcutta, India, pages 347–350, 2003.

[16] J.P.Pandey, D.B.Ojha, Ajay Sharma, “Enhance Fuzzy Commitment Scheme: An Approach For Post Quantum Cryptosystem”, in Journal of Applied and Theoretical Information Technology, (pp 16-19) Vol. 9, No. 1, Nov. 2009.

[17] V.Pless, “ Introduction to theory of Error Correcting Codes”, Wiley , New York 1982.

[18] A.A.Al-saggaf,H.S.Acharya,“A Fuzzy Commitment Scheme”IEEE International Conference on Advances in Computer Vision and Information Technology 28-30November 2007 – India

Authors Bibliography

Ramveer Singh, Bachelor of Engineering from Dr. B.R. Ambedkaruniversity, Agra (U.P.), INDIA in 2003. Master of Technology from V.M.R.F. Deemed University, Salem (T.N.), INDIA in 2007. PersuingPh.D from Singhania University, Jhunjhunu, Rajsthan, INDIA. The major field of study is Cryptography and network security. He has more than eight year experience in teaching and research as ASSOCIATE PROFESSOR. He is working at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. The current research area is Cryptography and Network security. Mr. Singh is the member of LMCSI, LMIAENG, LMIACSIT, LMCSTA. He is the author/co-author of more than 17 publications in International/National journals and conferences.

Awakash Mishra, Master of Computer Application from Uttar Pradesh Technical University, Lucknow (U.P.), INDIA in 2007. PersuingPh.D from Singhania University, Jhunjhunu, Rajsthan, INDIA. He has more than four year experience in teaching and research as LECTURER. He is working at Raj Kumar Goel Engineering College, Ghaziabad (U.P.), INDIA. The current research area is Symmetric Key Cryptography.

AkshayTyagi, PersuingPh.D from MewarUniversity, Chittorgarh, Rajsthan, INDIA. He has more than five year experience in teaching and research as LECTURER. He is working at Gradute School of Business & Administration, Greater Noida, U.P., INDIA. The current research area is Cryptography& fuzzy commitment scheme.

Dr. Deo Brat Ojha, Ph.D from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varansi (U.P.), INDIA in 2004. His research field is Optimization Techniques, Functional Analysis & Cryptography. He has more than Six year teaching & more than eight year research experience. He is working as a Professor at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA.Dr. Ojha is the member of Mathematical Society Banaras Hindu University, LMIAENG, LMIACSIT. He is the author/co-author of more than 50 publications in International/National journals and conferences.