iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VIII **Month of publication:** August 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

A Dual Text Encryption Model using Hyper Encryption and Geometric Cryptography

Ms. Ritu Malik, Ms. Sunita

Ritu- Department of CSE & IT B.P.S.M.V., Sunita-Department of CSE& IT B.P.S.M.V.

***Abstract*—the security of cryptosystem has always been a problem. There are number of protocols that provide the attainable security. Hyper Encryption is one of the Encryption protocols that provide the everlasting security. But in today's era where with the maximum use of technology the eavesdropper power has been increased really very much. So there is a need of increased security. But the security of text based encryption scheme is always at risk. If we use graphical shape for the encryption with the text based encryption we can provide a better security layer. In this paper we are going to propose a hybrid encryption approach with the Hyper Encryption and Geometric Cryptography in this we will use the two layer security and try to make a protocol that provide a better security with a reliable approach**

***Keywords*— Hyper Encryption, Geometric cryptography, PSN, OTP, Fingerprinting**

I. INTRODUCTION

As the Internet becomes an increasingly important means of conducting transactions and the volume of e-business grows exponentially, a secure infrastructure is needed to provide authentication, confidentiality and access control. Security has evolved from a basic password scheme to a complex key infrastructure. Initially, shared secret keys were exchanged and maintained between pairs of correspondents. However, as the Internet expanded, this method became impractical. So to deal with this situation we have to develop a practical cryptographic system to keep our data secret. One Time Pad is a provable secure cryptosystem that is developed by Gilbert Vernam in 1918. It use the truly random series of bits as the secret key (Pad) as the same length as the plaintext. Simple Modular or XOR operation is performed between the plaintext and the secret key to encrypt it.. But practical implementation put some limitation on One Time Pad.

As advancement Rabin described the scheme of Hyper Encryption that provide benefits over the limitation of One Time and provide the everlasting security to the user data .In its basic scheme it takes many PSN servers from which anybody can request a page of random bits. Each page is served only twice then it was destroyed. So the two users who want to transfer data can agree on the same page of random bits and can take this page as a onetime pad. After the initial shared secret key it also allows the user to create the new secret pad to make the communication indefinitely

II. HYPER ENCRYPTION

Hyper Encryption is a form of encryption invented by Michael O.Rabin. Hyper Encryption is a shared secret key block cipher scheme. Block size is taken usually of m=32/64.Hyper Encryption is the first encryption scheme provably providing the everlasting secrecy against the computationally unbounded Adversary. To make the system everlasting secret the system use the assumption of Bounded Storage Model introduced by Maurer. Hyper Encryption uses the shared secret key together with the public random bits. Although anyone can see the data but the decryption by the Adversary without knowing the secret key is not feasible because of the limited storage space available to the Adversary as the assumption of BSM. It use the random key bit as secret pad as in OTP but if the secret key is compromised even then the message encrypted before the key compromise will be perfectly secure. Hyper Encryption work with the multiple servers known as the Page Server Node (PSN) . From which any user can request the random bits page with the help of a secret key. A single page can be given only to the two users having the same shared secret key. After that the page was destroyed completely by the PSN. This page of random bits is further used as the shared secret pad b/w the user as in the OTP encryption scheme. After sharing the initial secret key through a secure way that used to take the random

IJRASET: ISSN: 2321-9653 Volume II, Issue VIII, August 2014

bits page from the PSN all other transaction like making the secret pad and doing the message transaction can be done on the public network. It also allows creating the new One Time Pad to make the continuity of communication. It allows both the user to send the exponential number of message by using the initial shared secret key. Hyper Encryption use the Fingerprinting scheme to share the OTP on the network and to authenticate the data

III. Operation Scheme of Hyper Encryption

Hyper Encryption is a system that allows the two parties to transfer the secure data starting with an initial secret key and to make use of the publically available computer for random data.

Hyper encryption initially starts with the sharing of a secret key.

Then this shared secret key is used to request the Random bits pages from the **PSN** (Page Server Node).PSN gives random bits page to the requesting user. User access the random page with the help of the shared secret key. PSN gives the random bit page to the user who requested it with the secret key. The single page is given to only two users with the same secret key

After downloading the page from the PSN the both users A and B make sure that they have downloaded the same page of Random bits that they are going to use as OTP by using the method of **Page Reconciliation**. Basically the page reconciliation protocol used here use the **Fingerprinting** method for reconciliation.

In this the User A and User B computes the Fingerprints of the pages they have downloaded and then user A send its fingerprint to user B and user B compare these fingerprint with its own. In this way both determine the common pages they have downloaded. These pages work as the One Time Pad for the data encryption.

In this way the Hyper Encryption provide everlasting security with assumption of Bounded Storage Model (BSM). In BSM this is assume that the Adversary has the unbounded computational power but he has the limited storage capacity. If there is the case that Adversary will be able to access the user transaction but he can't be able to store the whole message transaction at the same time If by some how the Adversary will be able to access the user's secret key but his storage capacity is limited so at the time when he will be able to use the secret key for adversary the secret key will no longer be in use for the user, may be the user have already access the PSN random page. SO if the Adversary tries to access the PSN page he will get the different page. Or somehow if the Adversary became able to access the PSN page same as the User then at the time of page reconciliation the different page of the users will be discarded to make OTP. And it will be impossible or having a very low probability that the Adversary can generate a page whose fingerprint is same as of as the user random page fingerprint.

IV. LIMITATION OF HYPER ENCRYPTION

[1] The initial shared secret key length is very large.

[2] Choosing of PSN for downloading the random page

[3] Reconciliation protocol can create problem if the Reconciliation message lost or processed as unordered way

[4] It is a complex method that can't be implemented simply on paper

[5] As all the encryption and Decryption operation are performed purely on the text based so the Security is always at risk

V. PROPOSED A DUAL TEXT ENCRYPTION MODEL USING HYPER ENCRYPTION AND GEOMETRIC CRYPTOGRAPHY

Cryptography is the one of the key approach for information security used to encode the information and convert it to some normalized. In the traditional cryptography approaches, the text information is encoded using some text oriented mathematical operations. In this work, a hybrid cryptographic approach is suggested that will combine the hyper encryption along with geometric key cryptography. At the earlier stage of this work, the text data will be taken as input and the hyper encryption will be performed over it. This encoded data will be then used for geometric cryptography. In this approach, the circle is been used as the base geometric shape to perform the cryptographic operation. In this present approach, the complete surface will be covered by small circles with equal radius r. These circles are placed horizontally and vertically so that complete geometric area will be covered. Now, the input text is converted to the data bits and placed over these circle boundaries sequentially. Once the placement is done, the geometric transformation is applied

I.J.R.A.S.E.T.: ISSN: 2321-9653 Volume II, Issue VIII, August 2014

ISSN: 2321-9653

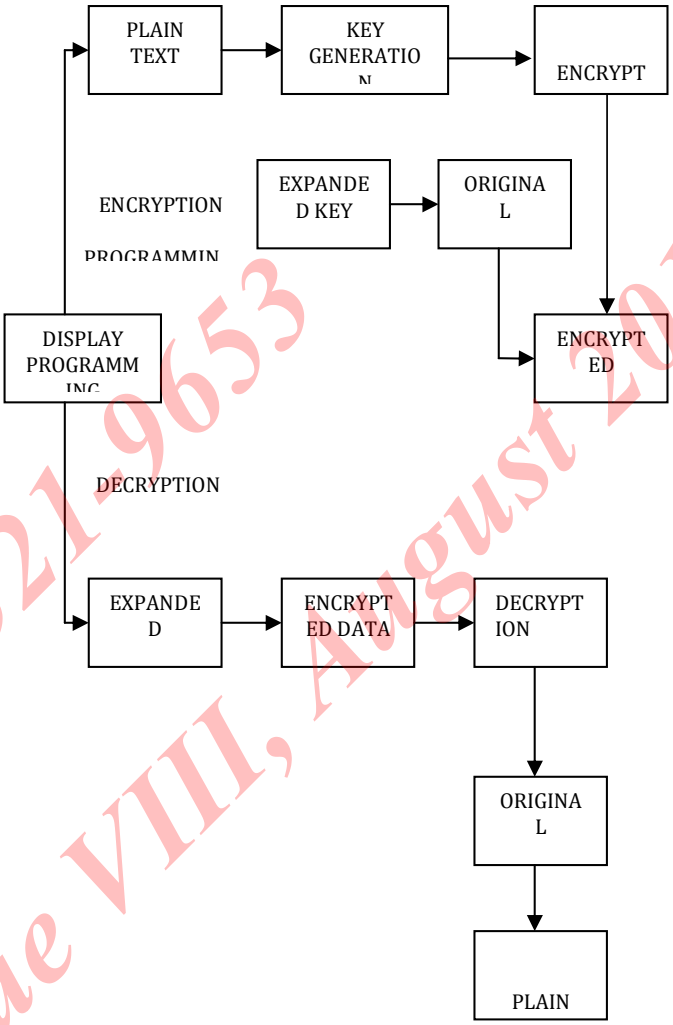
over the surface. In this presented approach, a hybrid transformation will be applied in terms of displacement, scaling and rotation operation. After these operations, the data will be captured back from each circle in same way and convert back to the encoded form. While performing the retrieval, same operation will be performed in reverse order. The presented work will improve the existing work in terms of hybrid transformation approach so that the encoding strength will be improved and it will be difficult to crack the cryptographic contents.

SIGNIFICANCE OF WORK:-

The advantages of the proposed work are defined as under The presented work will be effective in terms of security as the work will use the hybrid cryptographic. As the work is based on block level analysis, the work will provide the efficiency in cryptography process.

The presented expanded model is shown here in figure. The model begins with the acceptance of the input text. The text can be input directly in the form of a string or can be taken in the form of a file. Once the text is obtained, The proposed algorithmic approach will be implemented on it to encode the data. At the earlier stage, the hyper encryption is performed by performing the block level transformation and merging. At second stage the geometric structure will be obtained on which the text will be placed in the form of bits. The geometric area will be defined along with physical size specifications and the radian parameters of the geometric object used. Here we have taken the eclipse as the geometric object. The next step is to generate the key over it. To generate the key the radius of the eclipse along with geometric definition is been used.

Once the key is generated. The next process is to write the data over this geometric object boundaries bit by bit. To perform this, the circumference of all available graphical objects is taken and data is write on the boundaries. As the data is written over there, the next process is to perform the basic transformation. The geometric transformation is here performed to encode the data. Once the transformation, the data is taken back bit by bit. In same way as the storage is performed. Finally the encoded text will be obtained.



VI. ANALYSIS OF PROPOSED WORK

The analysis of work is here defined in terms of time taken by the work for different cryptography operations on different input text of different length. The results are here shown in the table

Table : Analysis Result

IJRASET: ISSN: 2321-9653 Volume II, Issue VIII, August 2014

ISSN: 2321-9653

Input Length	*Encryption Time*	*Decryption Time*
100	*234*	*152*
200	*316*	*263*
300	*435*	*321*
400	*863*	*436*
500	*1636*	*963*

The results are here analysed respective to different length inputs. The results are shown in the form of graph

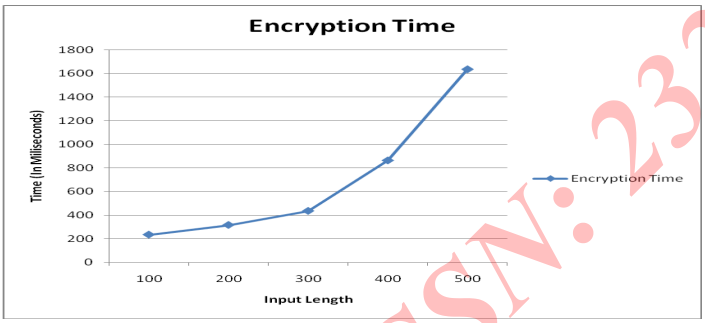


Figure : Encryption Time Analysis

Here figure is showing the time taken to encrypt the input text. Here x axis showing the size of input text and y axis shows the time in milliseconds.

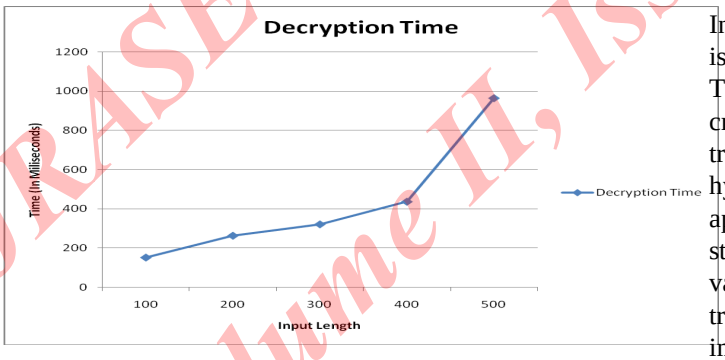


Figure : Decryption Time Analysis

Here figure is showing the time taken to decrypt the input text. Here x axis showing the size of encrypt text and y axis shows the time in milliseconds.

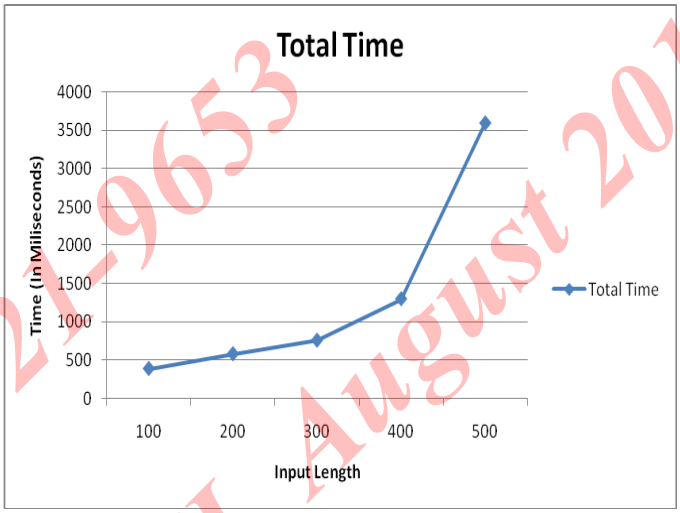


Figure : Total Time Analysis

Here figure is showing the time taken to encrypt and decrypt the input text. Here x axis showing the size of encrypt text and y axis shows the time in milliseconds.

VII. CONCLUSION

In this present work, an effective hybrid cryptography scheme is defined by combining two symmetric key based approaches. These approaches are hyper encryption scheme and geometric cryptography. The hyper encryption scheme is a block transformation scheme that encodes the text data. Once the hyper encryption is performed, the geometric cryptography is applied over it. The geometric cryptography is a geometric structure transformed approach. This approach places the data values on the boundary of the geometric circle and then transformation is applied over it. This dual approach is implemented in java environment. The results obtained from the system the effective encoding and decoding in effective time.

VIII. ACKNOWLEDGEMENT

IJRASET: ISSN: 2321-9653 Volume II, Issue VIII, August 2014

I would like to express my deep gratitude to Assistant Professor Ms. Sunita, my research work supervisor, for her valuable and constructive suggestions during the planning and development of this research work. Her willingness to give her time so generously has been very much appreciated.

REFERENCES

[1] http://www.articsoft.com/encryption.htm

[2] Ramel Levin, "Finding a better approach to PKI-based Digital Signatures", June 2006.

[3] www.arx.com"Introduction to PKI - Public Key Infrastructure", European Master in Multimedia Projects 2002 Jean Carlo Binder

[4] http://www.seminarsonly.com/IT/Public-Key-Infrastructure.php

[5] YounSun Cho, "Secure Access Control for Location-Based Applications in WLAN Systems", Nov 2005, pp 11

[6] Győző Gódor, "Novel Authentication Algorithm – Public Key Based Cryptography in Mobile Phone Systems", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006, pp 126-134

[7] Hatem Hamad, "Data encryption using the dynamic location and speed of mobile node", Journal of Media and Communication Studies Vol. 2 (3), pp.067–075, March 2010

[8] Hassan Elkamchouchi," A New Blind Identity-Based Signature Scheme with Message Recovery". The Online Journal on Electronics and Electrical Engineering (OJEEE) Vol 2, pp 200-205, 2009

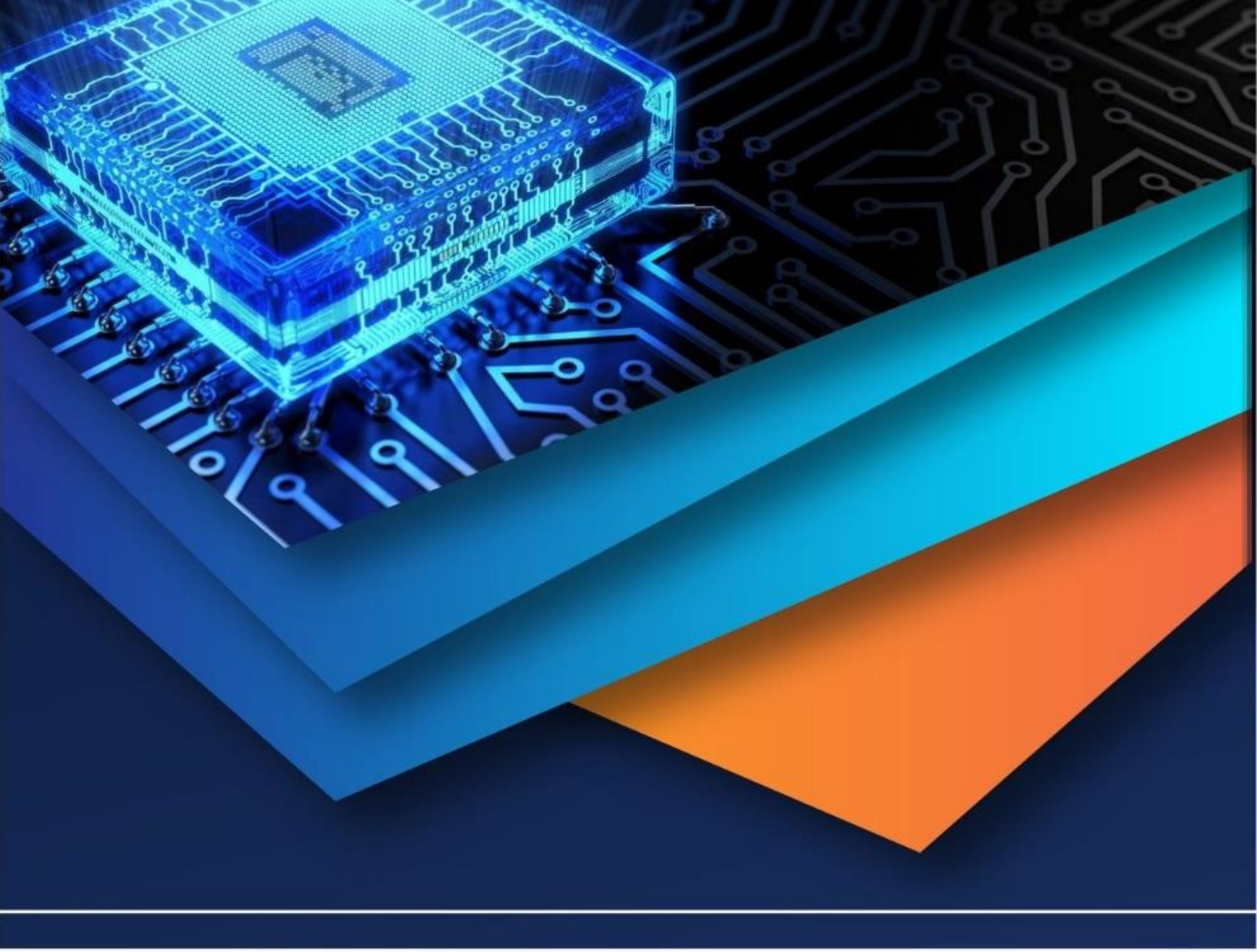
[9] Seny Kamara," Dynamic Searchable Symmetric Encryption", CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10 (pp 965-976)

[10] Parisa Kaghazgaran," Secure Two Party Comparison over Encrypted Data", 2011 World Congress on Information and Communication Technologies 978-1-4673-0125-1@ 2011 IEEE (pp 1127-1130)

[11] Trisha Chatterjee," Symmetric key Cryptosystem using combined Cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm", 978-1-4673-0125-1@ 2011 IEEE (pp 1179)

[12] Chao-Wen Chan," A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008 (pp 128-132)

IJRASET: ISSN: 2321-9653 Volume 1, Issue VIII, August 2014



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)