Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Design and Development of New symmetric Cryptography Protocol to Improve Text Security

Prof.Gajendra Singh*
C.S (Department) Sssist Shehore
(M.P) &R.G.P.V, India

Preeti Shukla
M.Tech. Scholar, Sssist Shehore
(M.P) &R.G.P.V, India

Abstract: ***Internet is easiest communication channel between two parties. During communication between parties' lots of text information's is transmitted from one system to another system. This is a immense thing at sending end but at receiving end it comes with immense risk. Chances of hacking of information during the transmission process are always there. We cannot control this hacking of information 100 % that's why there are different-different technique are available in the markets which convert this readable information in to unreadable information before sending on communication channel. Such type techniques are called encryption/decryption technique. There are so many different encryption/decryption technique each has their own trade-offs between time and security complexity. The focus of this work is confidentiality of text information in a public domain. Databases are used to accumulate a wide variety of confidential text information, including personally exclusive information and other records. The quantity and value of confidential text information is constantly rising, and this text information must be protected from attackers or unauthorized modification. This proposed work aims to provide confidentiality of text information through proposed cryptography technique based on the private key value. The proposed cryptograph technique implemented in this research work extends and improves the earlier presented cryptography technique like AES, DES, and IDEA. Presented research work is the study of cryptography and difficulties associating with existing technique. Furthermore this is proposing encryption technique. This encryption technique is based on the block cipher concept which is a type of symmetric cryptography technique where it will be encrypt and decrypt any type of text information in block of bit wise way. The primary purpose of this proposed research work is to enhance the security level. The proposed encryption technique is analysed by using a parameter known avalanche effect.***

Keywords: Symmetric Cryptography, Encryption, Decryption, Security, Key, Asymmetric Cryptography

I. PROPOSED WORK

A network of computer is any set of computing system which has the capability of exchanging information by interacting with each other significantly, allowing resource distribution in a proper way. The group of computers is interrelated by communication channels, which require being secured information exchange in batter way. This field of networking consists of professional field of network safety adopted by administrator of network to stop and monitor illegal access, denial of computer network and modification [10]. To battle the growing difficulty, security professionals are in look for of better protection. Security trouble compromises the security and therefore various Symmetric cryptographic algorithms have been presented to achieve the higher security service in the proper way, such as Integrity, Non-Repudiation, Authentication, Confidentiality, and Availability. These algorithms are needed to provide users authenticity and data security. In this research work purpose of the proposed concept is the security with efficiency. Concept of the proposed concept is based on symmetric key with block cipher. As we know that symmetric key cryptography provide higher efficiency in terms of execution and block cipher give the strength to encrypt a block of text at a time**.**

Whenever a person wants access(write or Read) information from internet or public domain then it read or write all the content in readable form. For example user want send personal information through this site/system in public network. First of all user will fill up all the necessary confidential information in the site/system at user end and then send to other end but these confidential information should not go directly to other end but it will pass through cryptography system. For this proposed system using security features like cryptography, with the help of cryptography it will encrypt confidential information into cipher text and this cipher text will transmit to other end via public network. It is preferred to communicate information with high security. At present, different types of symmetric cryptographic technique provide high security but low efficiency to information on proscribed networks. These algorithms are needed to provide information security with high efficiency. This new security concept has been designed for better security using symmetric cryptographic techniques. Figure 1 is showing the general block diagram of proposed concept, here secrete message pass to proposed encryption algorithm and finally it will convert from readable form to unreadable form known as cipher text. During whole encryption process number of step are executing and they are using number of various operation like XOR and circular shifting. All these operation are performing along with symmetric key value because encryption are not possible a key value and it already known the importance of private key value during encryption and decryption. Length of the key value is also play important role because higher key length causes of higher security but

too much higher is also a cause of poor performance, so it is very important that key length should high but it also efficient. In the proposed concept 128 bits of key length are using which provide too much security with effectiveness.

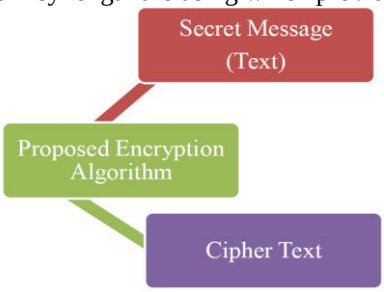


Figure 1: Block Diagram of Proposed Encryption Concept

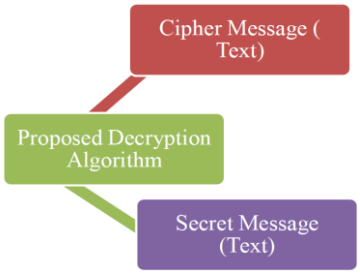


Figure 2: Block Diagram of Proposed Decryption Concept

Figure 2 is showing the block diagram of proposed concept during decryption. In this cipher text message pass through proposed decryption algorithm and finally it converting unreadable text into readable text known as plain text. During decryption number of steps is executing using some operation like XOR and circular shifting operation but in reveres order like encryption. All these operation are working with private key value.

Proposed Encryption Architecture:

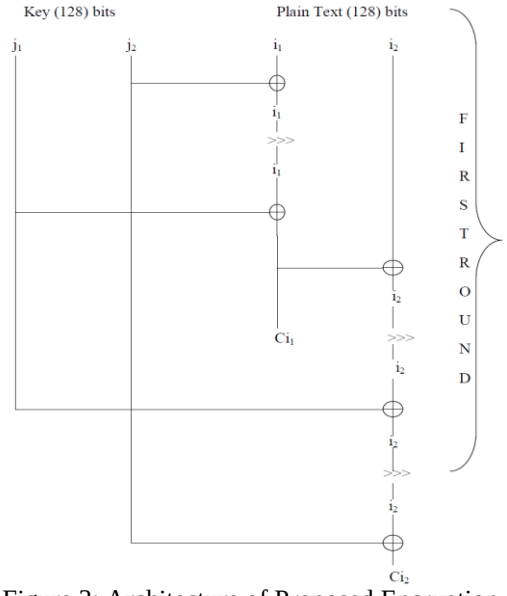


Figure 3: Architecture of Proposed Encryption

Proposed Encryption Algorithm Step

1. Input text of i bits i = 1 to N
2. Read text block of 128 bits at a time.
3. Input Key of j bits j = 128 bit
4. Apply division function on i of equal bits
   Div (i/2) = (i_1, i_2)
5. Similarly Apply Division function on j
   Div (j/2) = (j_1, j_2)
6. Perform XOR between j_2 and i_1 and resultant i_1.
7. Perform 3 bits right circular shift on i_1
8. Perform XOR between j_1 and i_1 and resultant i_1
9. Perform XOR between i_1 and i_2 and resultant i_2

10. Perform 3 bits right circular shift on i_2
11. Perform XOR between j_1 and i_2 and resultant i_2
12. Perform 3 bits right circular shift on i_2
13. Perform XOR between j_2 and i_2 and resultant i_2
14. Combine i_1 and i_2 to produced Cipher Text CI
15. Repeat above process 10 times.
16. Exit

Proposed Decryption Architecture:

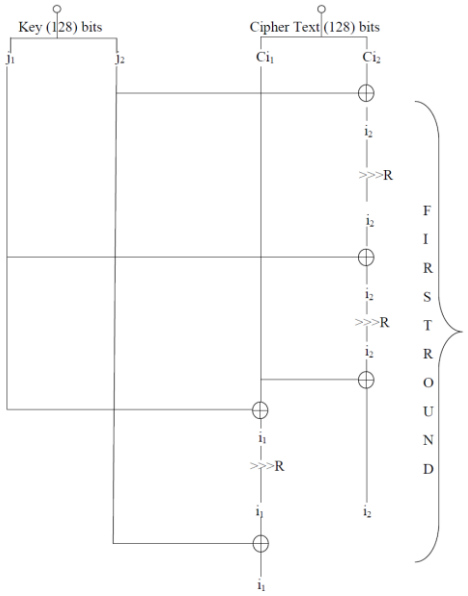


Figure 4: Architecture of Proposed Decryption

Proposed Decryption Algorithm

1. Input cipher text (Ci) of i bits i = 1 to N
2. Read cipher text (Ci) block of 128 bits at a time.
3. Input Key of j bits j = 128 bit
4. Apply division function on Ci of equal bits
   Div (Ci/2) = (Ci_1,C i_2)
5. Similarly Apply Division function on j
   Div (j/2) = (j_1, j_2)
6. Perform XOR between j_2 and Ci_2 and resultant i_2.
7. Perform 3 bits right circular shift reversely on i_2
8. Perform XOR between j_1 and i_2 and resultant i_2
9. Perform 3 bits right circular shift reversely on i_2
10. Perform XOR between Ci_1 and i_2 and resultant i_2
11. Perform XOR between j_1 and Ci_1 and resultant i_1
12. Perform 3 bits right circular shift reversely on i_1
13. Perform XOR between j_2 and i and resultant i_1
14. Combine i_1 and i_2 to produced Secret Text I
15. Repeat above process 10 times.
16. Exit

Example 1: In this example proposed algorithm taking one secrete message and displaying cipher text with showing all intermediate value in the form of binary.

PLAINTEXT**:** Understanding semiconductor diode application through MAT lab simulink IEEE technology and engineering education (ITEE) Applying Itelligent controller for speed regulation of DC moto Journal Efficiency optimization of three phase induction motor by slip compension Journal Understanding semiconductor diode application through MAT lab simulink IEEE technology and engineering education (ITEE)

KEY: “asdfghjklzxcvbnm”

CIPHERTEXT :

-pMhP,,³,Ê"˜Ã/iñtEˆ L0

Tš -6ž › eÑ

E©h8xëý• öˆ ìpá” ÍôTh$sµãÕ

G8¾iÌ„ íˆ <b¬.ã€ ‡ c@M„ M„ T

/£Ýk~Öiü]¨|tÅ8OU€ ×©×Åtü½H˜ e
H\ª..ñZ%´EÑm¡h˜ h‹ â1øPŽªaõiIì ĀÕ4ÒTž ÐMµM-ht,N=1¯w~m±,å
<Œe¥<" í©`à• á

<éö|ýh§ft4|

4T*ƒ* ¾-
åódHápi€ Q<

}ÕD½ÔH!Aµ,©hĀù□ ½rĀ$□ ÑQ-mõh4]~□ ù°H□ B¹PD!IðLĀ□ l[³?¶Ä,äIôqôP8G½Ý□gõ]m˜P!8Éå×•R-@mñ5Iõh,ý³H¶
C(%öÁhu˜T8□ ˆ†Ä¢.ÅŒl58U]ÖŽ • ÀC]Áu)hl,û½AStEuÙ4\¼|

$þ‡ãú-NgmØ!i°ll_«ˆ0Ÿ“¶m

Brute force attack**:** With a key of length n bits, there are 2^n possible keys. An algorithm with a security level of x bits is stronger than one of y bits if x > y. If an algorithm has a security level of x bits, the relative effort it would take to "beat" the algorithm is of the same magnitude of breaking a secure x-bit symmetric key algorithm (without reduction or other attacks). The 128-bit security level is for sensitive information, and the 192-bit level is for information of higher importance [16]. Here proposed algorithm having 128 bits key length so there are 2^{128} possible keys. The larger number of operation (2^{128}) required to try all possible 128-bit keys is widely considered to be out of reach for conventional digital computing techniques for the future.
Characteristics of the Proposed System**:**

- Reliability and Fault Tolerance:
- Availability:
- Security:
- Adaptability and Availability:
- Correctness and consistency:
- Portability:
- Performance:

II. RESULTS

Performance Analysis**:** This section presents the performance of the existing and proposed technique that is based on selected parameters. Selected parameter is avalanche effect which is described below.

Avalanche Effect: In cryptography, the avalanche effect refers to an attractive property of block ciphers and cryptographic hash functions algorithms.
The avalanche effect is satisfied if:

- If the output changes significantly (e.g., half the output bits flip) cause of a slight change in input (e.g., flipping a single bit)
- In "quality" block ciphers, such a small change in either the key or the plaintext should cause a strong change in the cipher text.

Both of above features allow small changes to propagate rapidly through iterations of the algorithm, in such a way that every bit of the output should depend on every bit of the input before the algorithm terminates. Avalanche Effect Formula is given below

$$\text{Avalanche Effect} = \frac{\text{Number of change bit in cipher text}}{\text{Number of bit in cipher text}}$$

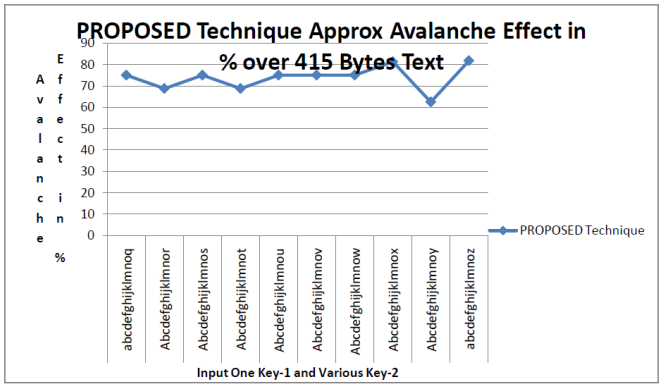
In the results comparisons, encrypts various size of text file and calculates avalanche effect and execution time. Here proposed system are comparing existing technique with proposed technique on predefined parameters like avalanche effect approximately 100 times run to the proposed system, after that noted down performance parameters (Avalanche affect) which is shown in table 1, 2, 3 and 4 and graph 1, 2, 3 and 4. During Results evaluation, proposed system has change key value corresponding to plain text value to perform encrypted/decrypted and generated cipher data by existing and proposed technique. Size of the selected key was same in each time. Finally, the outputs of the comparison system are avalanche effect which is noted in numeric form.

In this proposed research work has define total four test case where Test Case. In test case I the avalanche effect by changes in key value on 415 bytes and noted down the bit differences in percentage which is shown in table 1. In test case II is also evaluating the avalanche effect between existing and proposed by changing in key value on 830 byte text data and noted down the bit differences in percentage which is shown in table 2.

In test case III is also evaluating the avalanche effect between existing and proposed by changing in key value on 1245 byte text data and noted down the bit differences in percentage which is shown in table 3.
In test case IV is also evaluating the avalanche effect between existing and proposed by changing in key value on 1660 byte text data and noted down the bit differences in percentage which is shown in table 4.
Test Case 1: In test case 1 avalanche effect are calculating between, existing and proposed cryptography technique through key value., this is shown in table 1 and the graphical analysis is shown in graph 1. In this test case key-1 are fixed where minor changes occurring in key-2 and observing the avalanche effect.

Table 4.1 Comparative Avalanche effects in percentage (%) of between Existing and Proposed Technique

Key		PROPOSED Technique
Key 1	Key 2	Approx Avalanche Effect in %
abcdefghijklmnop	abcdefghijklmnoq	75
abcdefghijklmnop	Abcdefghijklmnor	68.75
abcdefghijklmnop	Abcdefghijklmnos	75
abcdefghijklmnop	Abcdefghijklmnot	68.75
abcdefghijklmnop	Abcdefghijklmnou	75
abcdefghijklmnop	Abcdefghijklmnov	75
abcdefghijklmnop	Abcdefghijklmnow	75
abcdefghijklmnop	Abcdefghijklmnox	81.25
abcdefghijklmnop	Abcdefghijklmnoy	62.5
abcdefghijklmnop	abcdefghijklmnoz	81.75

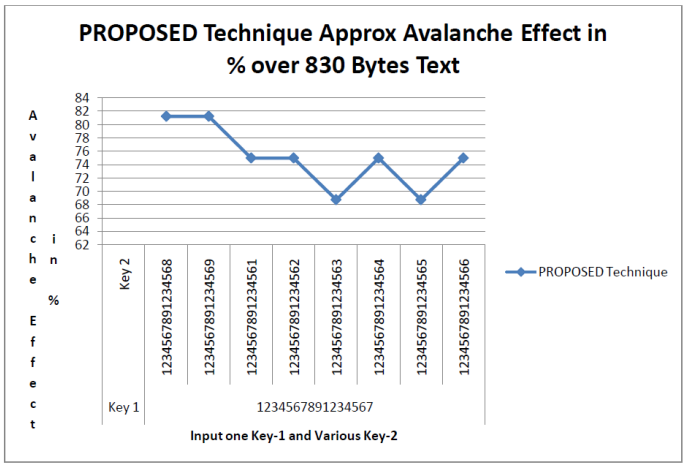


Graph 1: Avalanche effects in percentage (%) on 415 bytes of text through various Key-2

Test Case 2: In test case 1 avalanche effect is calculating between, existing and proposed cryptography technique through key value. This is shown in table 2 and the graphical analysis is shown in graph 2. In this test case key-1 are fixed where minor changes occurring in key-2 and observing the avalanche effect

Table 2 Avalanche effects in percentage (%) of between Existing and Proposed Technique

Key		PROPOSED Technique
Key 1	Key 2	Approx Avalanche Effect in %
12345678912345672	12345678912345682	81.25
1234567891234567	1234567891234569	81.25
1234567891234567	1234567891234561	75
1234567891234567	1234567891234562	75
1234567891234567	1234567891234563	68.75
1234567891234567	1234567891234564	75
1234567891234567	1234567891234565	68.75
1234567891234567	1234567891234566	75

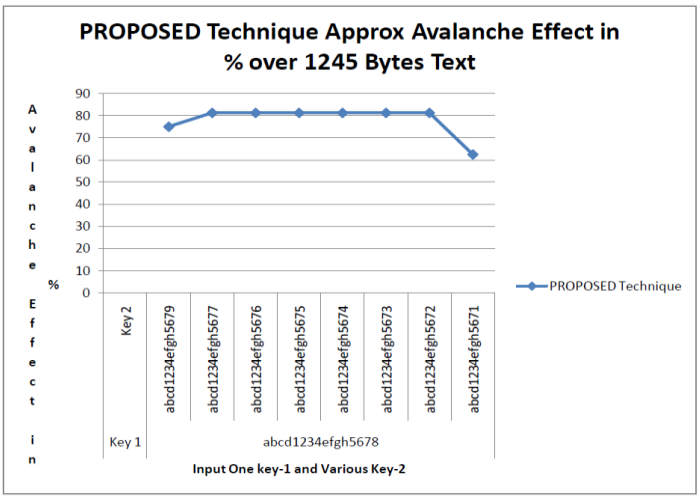


Graph 2: Avalanche effects in percentage (%) on 830 bytes of text through various Key-2

Test Case 3: In test case 1 avalanche effect are calculating between, existing and hybrid cryptography technique through key value. This is shown in table 3 and the graphical analysis is shown in graph 3. In this test case key-1 are fixed where minor changes occurring in key-2 and observing the avalanche effect

Table 3 Avalanche effects in percentage (%) of Proposed Technique

Key		PROPOSED Technique
Key 1	Key 2	Approx Avalanche Effect
abcd1234efgh5678	abcd1234efgh5679	75
abcd1234efgh5678	abcd1234efgh5677	81.25
abcd1234efgh5678	abcd1234efgh5676	81.25
abcd1234efgh5678	abcd1234efgh5675	81.25
abcd1234efgh5678	abcd1234efgh5674	81.25
abcd1234efgh5678	abcd1234efgh5673	81.25
abcd1234efgh5678	abcd1234efgh5672	81.25
abcd1234efgh5678	abcd1234efgh5671	62.5

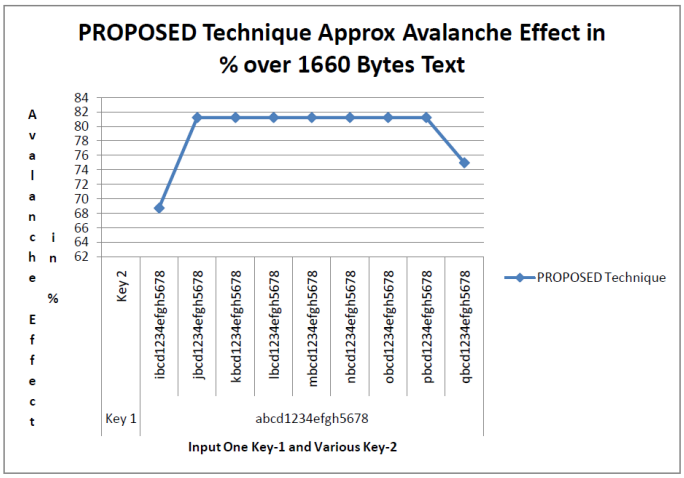


Graph 3: Avalanche effects in percentage (%) on 1245 bytes of text through various Key-2

Test Case 4: In test case 1 avalanche effect is calculating of proposed technique through key value. This is shown in table 4 and the graphical analysis is shown in graph 4. In this test case key-1 are fixed where minor changes occurring in key-2 and observing the avalanche effect.

Table 4: Avalanche effects in percentage (%) of Proposed Technique

Key		PROPOSED Technique
Key 1	Key 2	Approx Avalanche Effect
abcd1234efgh5678	ibcd1234efgh5678	68.75
abcd1234efgh5678	jbcd1234efgh5678	81.25
abcd1234efgh5678	kbcd1234efgh5678	81.25
abcd1234efgh5678	lbcd1234efgh5678	81.25
abcd1234efgh5678	mbcd1234efgh5678	81.25
abcd1234efgh5678	nbcd1234efgh5678	81.25
abcd1234efgh5678	obcd1234efgh5678	81.25
abcd1234efgh5678	pbcd1234efgh5678	81.25
abcd1234efgh5678	qbcd1234efgh5678	75



Graph 4: Avalanche effects in percentage (%) on 1660 bytes of text through various Key-2

Results Analysis:

From table 1 to 4 it's observed that avalanche effect are calculating between key values on different size of plain text, in all four case proposed technique producing higher avalanche effect. In Case-1, key-1 "abcdefghijklmnop" and key-2 "abcdefghijklmnoq" in table 1 producing 75% avalanche effect producing through proposed technique and similarly key-1 "abcdefghijklmnop" and key-2 "abcdefghijklmnor" producing 68.75% avalanche effect through proposed technique.

In Case-2 key-1 "1234567891234567" and key-2 "1234567891234568" in table 2 producing 81.25% avalanche effect through proposed technique and similarly key-1 "1234567891234567" and key-2 "1234567891234569" producing 81.25% avalanche effect through proposed technique.

In Case-3, key-1 "abcd1234efgh5678" and key-2 "abcd1234efgh5679" in table 3 producing 75% avalanche effect through proposed technique and similarly key-1 "abcd1234efgh5678" and key-2 "abcd1234efgh5677" producing 81.25 % avalanche effect through proposed technique.

In Case-4 key-1 "abcd1234efgh5678" and key-2 "ibcd1234efgh5678" in table 4 producing 68.75 % avalanche effect through proposed technique and similarly key-1 "abcd1234efgh5678" and key-2 "jbcd1234efgh5678" producing 81.25 % avalanche effect through proposed technique. From the analysis of produced avalanche effect it's easy observed that proposed technique is batter.

III. CONCLUSIONS

In this dessertation work perused the concept of symmetric cryptography including the different type of logical operation on the special kind of private key and an algorithms like "Proposed Encryption". The proposed concept provides a architecture for confidentiality of text data in public domain that can be useful in various software applications like banking, medical, government organization, defense and many more. Benefits to the proposed symmetric cryptography concept include the confidentiality with simplicity. Drawbacks to the proposed symmetric cryptography concept include ineffective encryption/decryption speed in huge amount of text information due to more number of steps

in proposed algorithm as compare existing algorithm but the important factor of this is higher security in terms of avalanche effect. The security analysis presents that the symmetric cryptographic strength of proposed concept is based on the "proposed encryption algorithm". Recent work suggests that proposed concept is not affected by any type of losses of information. The proposed concept is distinguished by plaintext decomposition into multiple sub blocks during processing of "proposed encryption algorithm" and secret key value. The multiple sub block solution makes decryption feasible for large text information during decryption process, and key value increase security through layering and provide higher confidentiality.

REFERENCES

[1] Aasifhasan, Neeraj Sharma "A New Method Towards Encryption Schemes (N Ame-Based-Encryption Algorithm)" Published In IEEE International Conference On Reliability, Optimization And Information Technology -ICROIT 2014, India, PP 310-313 Feb 6-8 2014

[2] Xinqiang Li, Lili Yu, Lihuan Wei "The Application Of Hybrid Encryption Algorithm In Software Security" Published In IEEE International Conference PP 669-672, 2013

[3] Hanan A. Al-Souly, Abeer S. Al-Sheddi, Heba A. Kurdi "Enhanced TSFS Algorithm For Secure Database Encryption" Published In IEEE Science And Information Conference October 7-9, 2013 | London, UK PP 328-334

[4] Yash Bharadwaj, Shampa Chakraverty "A Design Pattern For Symmetric Encryption" Published In IEEE International Conference On Control, Computing, Communication And Materials (ICCCCM)2013 Pp 1-6

[5] A.Ramesh, Dr.A.Suruliandi "Performance Analysis Of Encryption Algorithms For Information Security" Published In IEEE International Conference On Circuits, Power And Computing Technologies [ICCPCT-2013] Pp 840-844

[6] Rahul Deep Sircar, Gunjan Sekhon, Asoke Nath "Modern Ecryption Standard (MES) : Version-II" IEEE International Conference on Communication Systems and Network Technologies 2013PP 506-511

[7] Gurpreet Singh, Supriya "Modified Vigenere Encryption Algorithm and its Hybrid Implementation with Base64 and AES" published in Second IEEE International Conference on Advanced Computing, Networking and Security 2013 PP 232-237

[8] Mr. Ramesh Shahabadkar, Dr. Ramachandra V. Pujeri "Optimization of Encryption Technique using Evolutionary Algorithm for Protecting Multimedia Contents in P2P System. published in 4th IEEE ICCCNT - July 4-6, 2013, Tiruchengode, India PP 256-261

[9] Songsheng Tang, Fuqiang Liu Nath "A one-time pad encryption algorithm based on oneway hash and conventional block cipher" published IEEE, June 2012.

[10] Chandra Prakash, Dewangan, Shashikant Agrawal "A Novel Approach to Improve Avalanche Effect of AES Algorithm" International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 8, October 2012 ISSN: 2278 – 1323

[11] Irfan.Landge, Burhanuddin Contractor, Aamna Patel and Rozina Choudhary " Image encryption and decryption using blowfish algorithm" World Journal of Science and Technology 2012, 2(3):151-156 ISSN: 2231 – 2587

[12] An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm : Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Choudhary, Asoke Nath: Communicated for publication in IEEE International conference WICT 2011 to be held at Mumbai Dec 11-14, 2011.

[13] Symmetric Key Cryptography using Random Key generator : Asoke Nath, Saima Ghosh, Meheboob Alam Mallik: "Proceedings of International conference on security and management(SAM'10" held at Las Vegas, USA Jul 12-15, 2010), P-Vol-2, 239-244(2010).

[14] David Kahn, "The Code Breakers: The Story of Secret Writing," Simon & Schuster, 1996

[15] Simon Singh, "The Code Book," Anchor Books, 1999

[16] Robert Reynard "Secret Code Breaker II: A Cryptanalyst's Handbook." , 1997

[17] David Mertz, "Introduction to cryptology, Part 1:" 2001

[18] Shivangi Goyal "A Survey on the Applications of Cryptography" published in International Journal of Science and Technology Volume 1 No. 3, March , 2012 PP 137-140 available at http://www.journalofsciences-technology.org/archive/2012/march_vol_1_no_3/9685431326187 843.pdf

[19] Saranya K, Mohanapriya R, Udhayan J "A Review on Symmetric Key Encryption Techniques in Cryptography" published in International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014 539 ISSN: 2278 – 7798 PP 539-544 available at http://ijsetr.org/wp-content/uploads/2014/03/IJSETR-VOL-3-ISSUE-3-539-544.pdf

