A Hybrid Cryptography Technique for Improving Network Security

V. Kapoor
Dept. Of Information Technology, IET DAVV
Indore (MP) India

Rahul Yadav
Dept. Of Information Technology, IET DAVV
Indore (MP) India

ABSTRACT
The security of network and the network data is primary aspect of the network providers and service providers. Therefore during the data exchange the cryptographic techniques are utilized for securing the data during various communications. On the other hand the traditional cryptographic techniques are well known and the attackers are known about the solution. Therefore new kind of cryptographic technique is required which improve the security and complexity of data cipher. In this paper a hybrid cryptographic technique for improving data security during network transmission is proposed and their implementation and results are reported. The proposed secure cryptographic technique promises to provide the highly secure cipher generation technique using the RSA, DES and SHA1 technique. The implementation of the proposed technique is provided using the JAVA technology and their performance in terms of space and time complexity is estimated and compared with the traditional RSA cryptography. The proposed cryptographic technique found the efficient and improved cipher text during comparative performance analysis.

Keywords
Data security, Network transmission, Cryptographic security, Data exchange, Hybrid cryptography, RSA, DES and SHA1.

1. INTRODUCTION
The art of preserving information by transforming it (encrypting it) into an unreadable format (for human eyes), called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking, although modern cryptography techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important [1]. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is Pretty Good Privacy because it's effective and free. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and

public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses [2].There are a number of applications available now in these days by which the private and sensitive data is transmitted using untrusted network. Basically most of the time user sends the data from a trusted network to a trusted network. But between source and target host the network remains unsecure. Therefore, Most of the applications are consumes the cryptographic techniques for providing the security and confidentiality in data [3]. In this presented work the main aim is to find the efficient and optimum solution for color image cryptography [4]. Efficiency concerned with the minimizing the computational resources in terms of memory consumption and execution time and the solution optimization is leads to modifying the cryptographic technique using hybrid approach with their integrity check. Thus the desired cryptographic system required to work in less time and less memory consumption. In order to develop such approach simple mathematical techniques and lightweight cryptographic standards are required to employ with the system.

The proposed work is intended to provide an efficient and a complex cipher generation technique using the hybridization of different techniques. For successfully achieve the desired goal following tasks are included in the study.

1.1 Study of different image and visual cryptographic scheme
In this phase of study various cryptographic approaches are explored in order to find the appropriate solution.

1.2 Design and implementation of the new enhanced algorithm:
Form the previous studies a new cryptographic technique is recovered and the enhancement on the existing technique is proposed. The proposed technique is further implemented using the suitable programming language in this module.

1.3 Performance analysis
In this phase the performance of the system is evaluated and the comparative study among traditional algorithm and presented improved technique is performed for finding the computational and storage complexity.

2. LITERATURE AND SURVEY
In the current years, there is an explosion in the amount of information being exchanged over Network; therefore it becomes very essential to provide proper security measures. In order to provide a secure environment to send data over network, a proper analysis of present security mechanism needs to be done. Recently one of the existing system uses compression based mechanism along with RSA algorithm for light weighted devices such as mobile phones and pda's [10]. This system provides a secure way to send message over the network [8]. This system uses compresses technique to reduce the length of message, then encrypt it by using RSA algorithm. RSA algorithm is an asymmetric algorithm which uses Public Key Encryption method. One of limitation of using asymmetric cryptography is time and space complexity. This system is also known as Hybrid Compression Encryption system (HCE). One another method uses compression based cryptography to transmit medical related information. It uses

compression methods like Sequitur for reducing the size of data being sent. The combination of McEliece public-key cryptosystem with compression provides confidentiality in the transmission [9].This system has a drawback as its efficiency drops with increase in data. The proposed system uses symmetric key cryptography hence it is faster than asymmetric key cryptography and uses compression technique to reduce the size of cipher text.

3. PROPOSED SYSTEM

The information technology is growing frequently using the internet and communication technologies. The internet is a huge source of communication and data transmission; therefore a significant amount of applications and their users are getting the services of the internet and their networks. The network is secured using various techniques such as the firewall and other anti-virus techniques. But among the two private networks the data is traverse through the public network and the public network is not much secure due to the different kinds of attacks and their security issues. Therefore the cryptographic techniques are utilized for improving the security of data during their transmission in the public networks.

On the other hand the different traditional cryptographic solution for network data transmission is well known and different techniques that are breakable by hackers. Thus new kinds of techniques for improving the network data security is required to investigated and developed. In this presented work a hybrid technique is developed using two different cryptographic approaches. These techniques are modified for improving the key generation and integrity checks by which the security is assured at both the end of network.

The proposed techniques are able to secure the data when the data is transmitted on the public and unauthorized data networks. And during different kinds of outsider attacks are identified is data altered during transmission or not. Thus the presented technique is an effective and essential for the network data security where the two users are communicating in unknown networks.

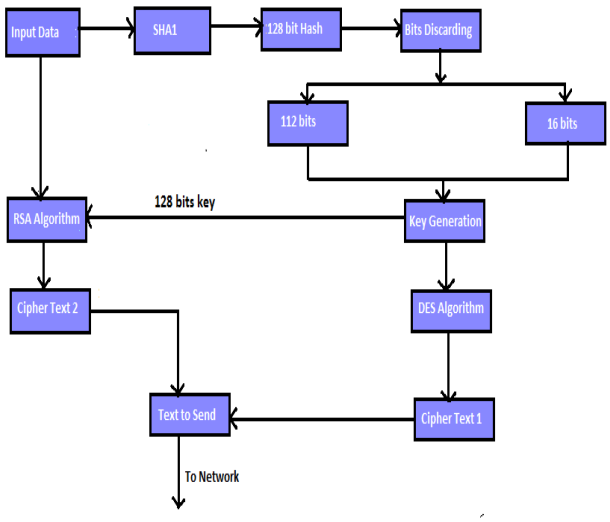

Figure 1: Encryption process

The proposed working hybrid model for data cryptography is given using figure 1 and figure 2. In figure 1 the encryption process of the system is described and the figure 2 reports the decryption process of the system. During the encryption process user need to encrypt the file using the hybrid cryptographic model, thus a input file is first produced to the system. The input file is first processed using SHA1[5] hash generation algorithm, the SHA1 algorithm generates the 128 bit hash code for the input data.

Over the produced 128 bit hash key the bit discarding process is taken place, in this process the 128 bit hash code is converted into 16 blocks of the 8 bit data. In each block of data the first bit is removed and placed separately for further processing. Thus the 128 bit hash code is converted into 112 bit of code and 16 bit of separated code. Both the bits 112 and 16 bit data is produced into a key generator where the 16 bit data is divided into 2 blocks of 8 bit and 112 bit of data converted into 14 blocks of data both the newly generated blocks are combined to generate the complete 128 bit of key. For securing the key more the DES algorithm [7] is used to encrypt the key which generates the cipher 1 which the encrypted key for decryption process. On the other hand the input original data is produced over the RSA algorithm [6] with a 128 bit key generated by the key generator. This process generates the cipher 2. In further steps the cipher text 1 and cipher text 2 is combined and ready to prepare the text for transmission.

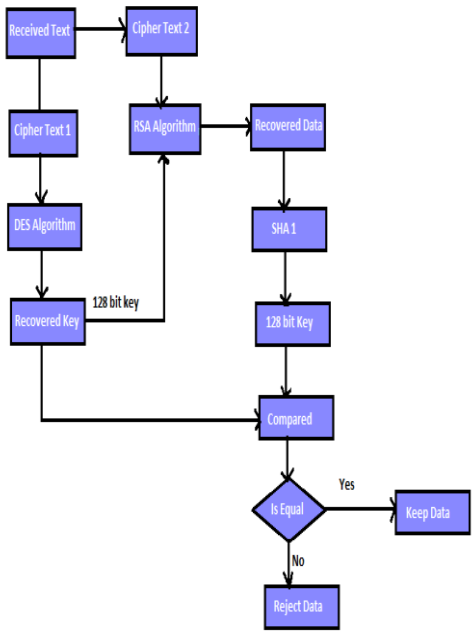

Figure 2: Decryption process

The transmitted text to the network is received by the end user, this text is termed here as the received text. In first process the received text is divided into two different ciphers, cipher 1 which is outcome of key data and seconds the cipher 2 that contains the encrypted data for security. The cipher 1 is treated first to generate the key for data recovery, therefore first the cipher text 1 is produced to DES algorithm for the recovering the original key by which the data is recovered. After recovering key using decipher of cipher text 1 the key is produced to RSA algorithm with the cipher text 2. The RSA algorithm decipher the original text and can be used with the other application but for authenticating the recovered data on

receiver end the integrity check is applied for the data. Therefore first the recovered data is processed through the SHA1 hash key and 128 bit obtained from the data. In further the comparer is implemented, the comparer has two functionalities first using the SHA1 128 bit, regenerate the original key by which the encryption performed. Thus the same operation is performed over the 128 bit to generate key and second the comparison among generated key and the obtained key from network. In further is both the keys are found similar the data is accepted by the system else the data can be rejected.

4. RESULTS ANALYSIS

The experimental evaluation and performance is computed and compared with RSA algorithm as described in [11]. The comparison is performed with the help of some performance factors. This section provides discussion about the obtained results.

4.1 Encryption time

The time required to encrypt data is termed as encryption time of the cryptographic system. The encryption time of the proposed technique and RSA algorithm is given using figure 3 and table 3.

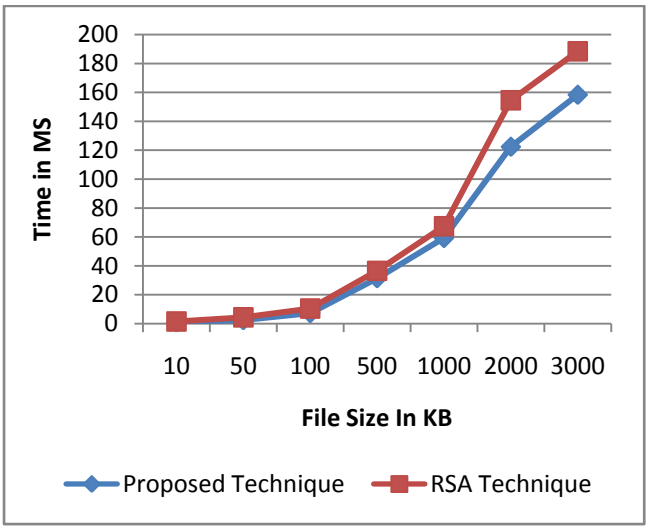

Figure 3: Encryption time

Table 3. Encryption time

File size	Proposed system	Traditional RSA system
10	0.93	1.47
50	2.47	4.38
100	7.29	10.47
500	31.42	36.53
1000	59.22	67.41
2000	122.39	154.53
3000	158.35	188.44

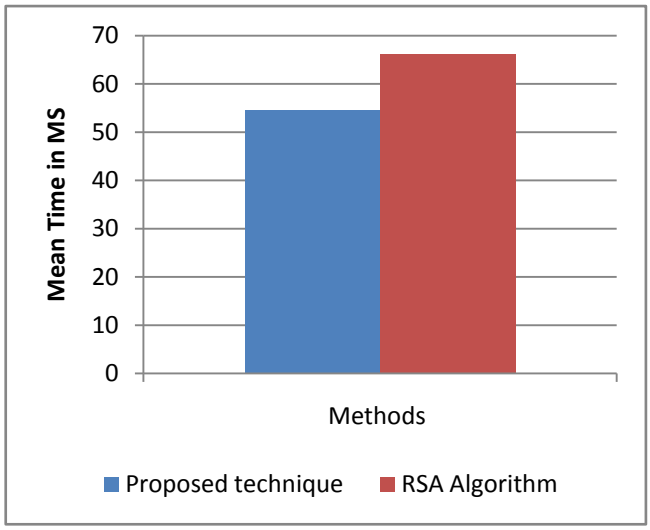

Figure 4: Mean encryption time

The diagram contains data of different file size in X axis by which experiments are conducted. Similarly Y axis contains amount of time in milliseconds. The blue line shows the performance of proposed technique and RSA algorithm is denoted by red line. The results show proposed algorithm consumes less time as compared to RSA algorithm. The amount of time depends on data. To approximate comparative performance figure 4 provides mean performance of algorithms. According to mean performance proposed technique consumes less amount of time with respect to RSA algorithm.

4.2 Decryption time

The time to recover original data from cipher is known as decryption time. Figure 5 shows comparative performance of RSA and proposed algorithm. In this figure X-axis contains file of different size for experiments and Y axis contains time required. The decryption time of the proposed algorithm is efficient as compared to RSA algorithm.

Table 4. Decryption time

File size	Proposed algorithm	Traditional RSA system
10	0.673	0.947
50	2.92	3.98
100	5.89	7.16
500	21.46	27.81
1000	39.87	47.88
2000	74.56	92.53
3000	125.94	147.22

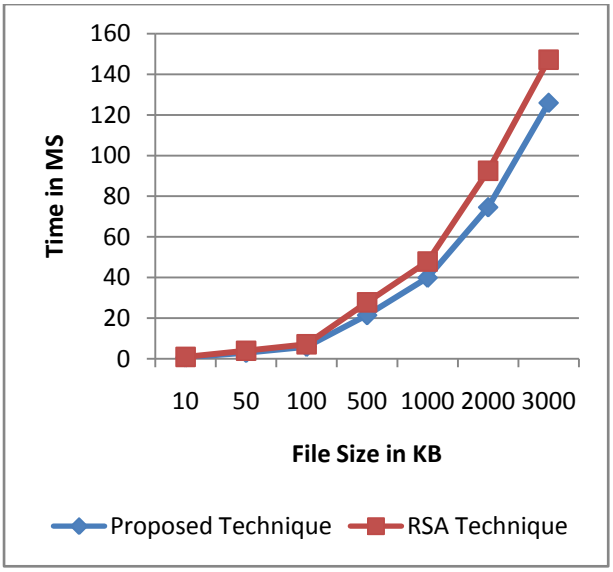

Figure 5: Decryption time

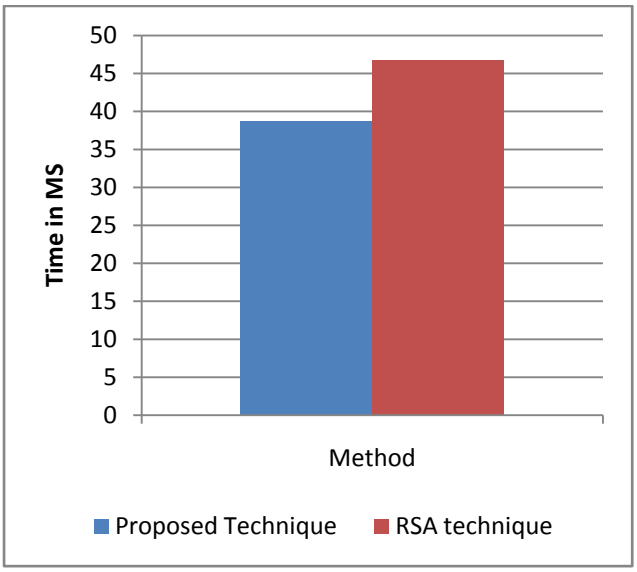

Figure 6: Mean decryption time

The results as defined in figure 5 shows, the proposed technique is efficient as compared to RSA algorithm. To differentiate among both the performance mean decryption time is also estimated and given using figure 6. The results shows proposed technique provides advantage over RSA algorithm. Thus proposed technique reduces the time consumption about 6-10 MS as compared to RSA algorithm.

4.3 Encryption memory

The amount of main memory required to execute algorithm is known as encryption memory. The figure 7 shows comparative memory consumed of implemented algorithm. In figure 7 shows the main memory consumed in terms of kilobytes in Y axis and file size used are given at X axis. The obtained results of proposed algorithm consume less memory with respect to RSA algorithm.

Table 5. Memory consumption

File size	Proposed technique	Traditional RSA technique
10	28038	28842
50	29114	30488
100	29437	31847
500	31864	32435
1000	32108	34722
2000	33148	35519
3000	34127	36254

The memory consumption of proposed and RSA algorithm is demonstrated in figure 7. To show advantage of proposed algorithm over RSA algorithm mean space complexity is computed and given using figure 8. The diagram includes memory consumption in kilobytes in Y axis and methods are given in X axis. The performance of proposed technique is efficient as compared to RSA algorithm.

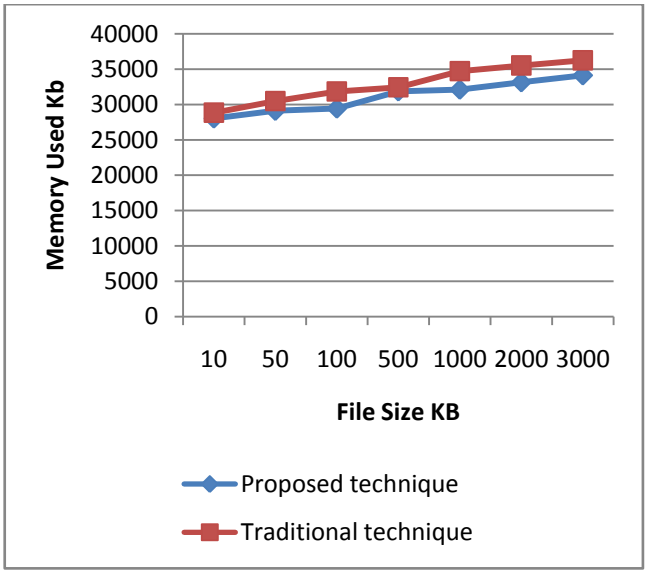

Figure 7: Encryption memory

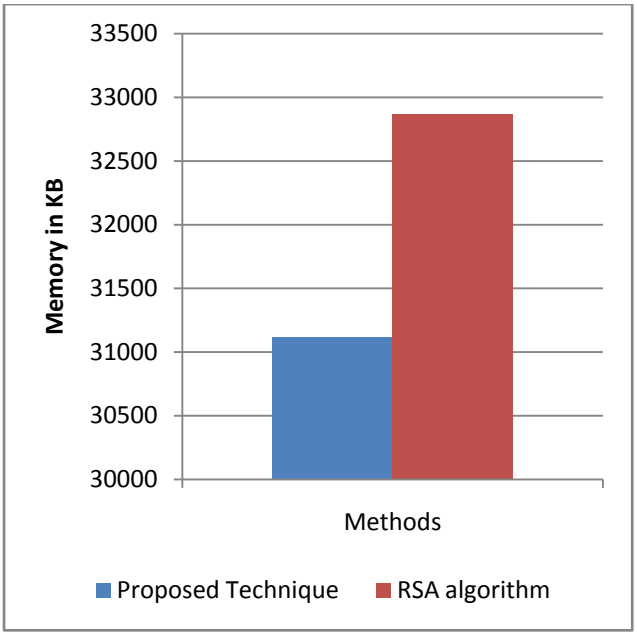

Figure 8: Mean encryption memory

4.4 Decryption memory

The amount of main memory required to recover encrypted data is known as the decryption space complexity. The figure 9 shows main memory required for data decryption.

Table 6. Decryption memory used

File size	Proposed technique	Traditional RSA technique
10	29472	29729
50	29187	30018
100	31383	31948
500	31284	32857
1000	34221	35268
2000	35633	36773
3000	36335	38826

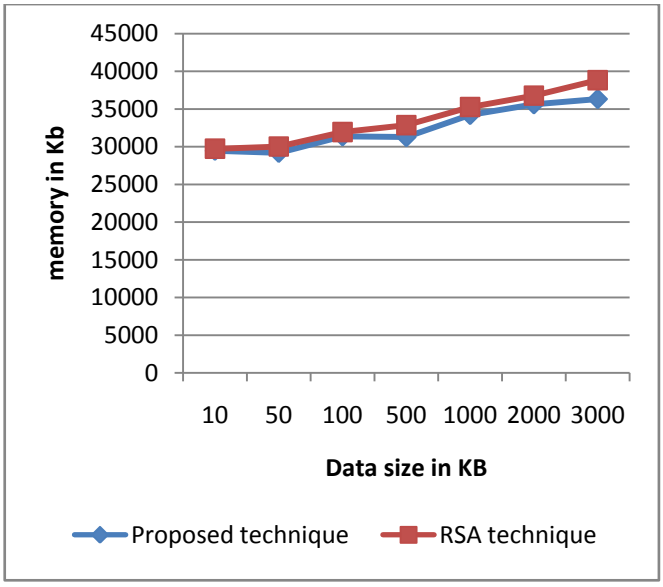

Figure 9: Decryption memory

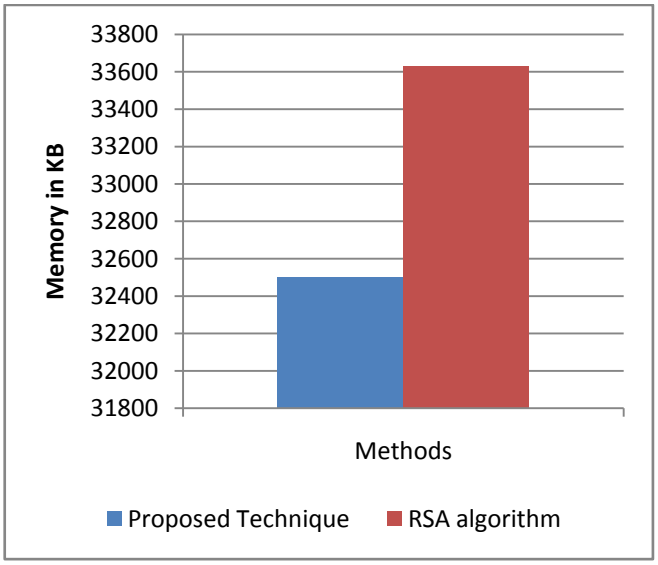

Figure 10: Mean decryption time

The X axis of diagram shows file size and Y axis contains main memory consumed in kilobytes. The obtained results shows space complexity of proposed technique is effective as compared to RSA algorithm. The difference between both techniques is also given by mean decryption time and given figure 10. The mean memory consumption of the proposed technique is efficient as compared to RSA algorithm.

5. CONCLUSIONS

The experimental results shows that the performance of the proposed cryptographic solution. The comparative performance of the proposed technique is summarized in the below given table 7. The key of the proposed work and this paper is to find a strong encryption algorithm. That can be efficiently works on the different kinds of data and produces the complex cipher text. Therefore a hybrid cryptographic technique using RSA, DES and SHA1 is prepared. In order to enhance the encryption process and the secure key generation a bit discarding process is also implemented. This process reduces the key size and improving the complexity of the key generation process. The implementation of the proposed hybrid encryption technique performed using the JAVA

technology. Additionally their performance is estimated in terms of encryption time, decryption time and the space complexity. Additionally the obtained performance of the proposed cryptographic solution is compared with the traditional RSA algorithm for similar size of file.

Table 7. Performance summary

S. No.	Parameters	Proposed	RSA
1	Encryption time	Low	High
2	Decryption time	Low	High
3	Encryption memory	Low	High
4	Decryption memory	Low	High

According to the obtained results the proposed technique is producing efficient and complex cipher with less resource consumption. In near future the approach is improved more for implementing the technique for security using cloud security and other different sensitive area of information security.

6. REFERENCES

[1] Dr. Vivek Kapoor, Rahul Yadav, "A Hybrid Cryptography Technique to Support Cyber Security Infrastructure", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 11, November 2015

[2] V Gampala, S Inuganti, S Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231- 2307, Volume-2, Issue-3, July 2012

[3] Akanksha Samadhiya, Trapti ozha, "Secure Mobile Cloud Storage and Data Transmission", Int.J.Computer Technology & Applications,Vol 6 (4),567-570

[4] Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", & 2011 Elsevier B.V. All rights reserved.

[5] Sun-Jung Kim, Young Jun Yoo, Jungmin So, Jeong Gun Lee, Jin Kim and Young Woong Ko, "Design and Implementation of Binary File Similarity Evaluation System", International Journal of Multimedia and Ubiquitous Engineering Vol.9, No.1 (2014), pp.1-10

[6] Mykola Karpinskyy, Yaroslav Kinakh, "RELIABILITY OF RSA ALGORITHM AND ITS COMPUTATIONAL COMPLEXITY", Computing, 2003, Vol. 2, Issue 3, 119-122

[7] Ashita Sharma, Navroz Kaur, "Implementation of DES (Data Encryption Standard) Algorithm", International Journal for Multi Disciplinary Engineering and Business Management, Volume-2, Issue-3, July-September, 2014

[8] Hybrid Compression Encryption Technique for Securing SMS Tarek M Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed & Ahmed M Mahfouz

[9] HexiMcEliece Public Key Cryptosystem K. Ilanthenral∗ and K. S. Easwarakumar Department of Computer Science and Engineering, Anna University, Chennai 600 025, India

[10] Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 21, April 2015 34.

[11] Sonal Modh, DR. M. K. Rawat, "Mobile Data Security using TPA Initiated Token Based Cryptography", IJSETR, Vol.05,Issue.06, March-2016, Pages:1140-1146