Performance Analysis of Multiple Keys used for Data Security

Hitesh Mittal
Research Scholar
ECED
Thapar University, India

Ajay Kakkar
Assistant Professor
ECED
Thapar University, India

ABSTRACT
Data security is an essential component of an organization in order to keep the information safe from various competitors. It helps to ensure the privacy of a user from others. Secured and timely transmission of data is always an important aspect for an organization. The use of strong encryption algorithms almost make it impossible for a hacker to get access of node which is being protected by multiple keys. Keeping in view the importance of dynamic keys for secure data transmission this work focused on the use of dynamic keys for data security.

Keywords
Encryption, Plain Text, Cipher Text, Key, Decryption, Security

1. INTRODUCTION
Cryptography is a technique used to avoid unauthorized access of data. It has two main problems a) Encryption algorithm and b) Key. Numbers of cryptographic algorithms are available in market such as DES, AES, TDES and RSA[11]. The strength of these encryption algorithms depends upon their key strength. Strong encryption algorithms and optimized key management techniques always help in achieving confidentiality, authentication and integrity of data and educe the overheads of the system. The long key length takes more computing time to crack the code. Plain text is the original message which is converted into cipher text. Cipher text is the encrypted text done with the help of key. Key is a word or value which is used for encryption/decryption. Cryptography is basically divided into two categories that are a) symmetric and b) asymmetric. Asymmetric algorithms are little bit slower than symmetric algorithms but provide a good level of security.

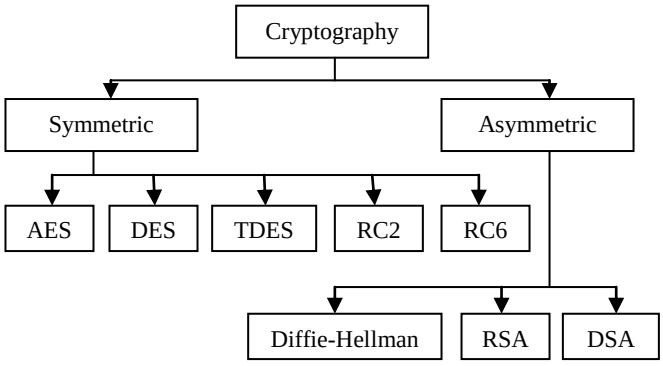


Fig 1: Types of Cryptography

2. LITESRATURE SURVEY
This section involves the work done by the various researchers in the field of cryptographic algorithm for data security. From this survey various gaps have also been drawn and stated in section 3.

Adam J. Elbirt [1] *et al.* evaluated the AES block cipher algorithm using FPGA based kit. They proposed that reprogrammable devices such as field-programmable gate arrays were highly attractive option for hardware implementations for encryption algorithms. The main limitation was that when the size of implementation increases then the number of rounds unrolled or pipelined was increased and this increase was partially offset by the packing of the round keys within the round structure.

Hua Li [2] *et al*. worked on new compact dual-core architecture used in AES. They presented a new compact architecture that consists of two independent cores that practice encryption and decryption simultaneously. Proposed key generation unit with 32-bit data path was explored in order to provide round keys for encryption and decryption. A novel way to implement shift rows was one of the key designs in the compact 32-bit architecture proposed in order to increase encryption time. The major limitation was that this design also requires fewer more hardware resources in comparison to the designs.

Jason H. Li [3] *et al.* worked on scalable key management and clustering scheme for secure group communication in *Adhoc* and WSN. They describe scalable key management and clustering to achieve more secured system. The scalability problem was solved by partitioning communicating devices into subgroups with a leader in each subgroup. The Distributed Efficient Clustering Approach (DECA) provided robust clustering to form subgroups. Analytical and simulation results demonstrate that DECA was energy efficient and resilient against node mobility. This scheme was not suitable for large cluster size.

Elisa Bertino [4] worked on the concepts, approaches, and challenges of database security. Relevant concepts underlying the notion of database security were summarized and the most well-known techniques were also discussed which were focused on access control system. He describe the key access control models which were mandatory access control models and the role-based access control (RBAC) model. He also discussed security for advanced data management systems. The major limitation was that when an individual user wants to change the subscription a new device needs to be issued.

Hung-Yu Chien [5] presented an efficient time bound hierarchical key assignment scheme. They proposed a tamper resistant device that has a new time bound key assignment scheme. It significantly improves the computational performance and reduces the implementation cost.

H. C. Williams [6] modified the RSA public-key encryption algorithm. He suggested that if the encryption procedure was broken into a certain number of operations than remainder used as modulus could be factored after few more operations. This technique was in similar appearance to RSA so as produce

digital signatures. The main limitation of this scheme was that very large prime numbers were used and generated mathematical errors were observed.

Martin E. Hellman [7] extended the shannon theory approach to cryptography. He discussed about Shannon's random cipher model which was conservative than in such case when a randomly chosen cipher was considered, the security falls significantly. The concept of matching a cipher to a language and the trade-off between local and global uncertainty were also developed. The limitation of this approach is that it is not directly applicable to designing practical cryptographic systems.

Taher Elgamal [8] proposed a signature scheme based on discrete logarithms and implemented Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. The security of both systems relies on the difficulty of computing discrete logarithms over finite fields.

Mao-Yin Wang [9] *et al.* configured single and multi-core AES architectures for flexible security. According to them the major building blocks for the architecture of AES was a group of AES processors. Each AES processor provides a block cipher scheme with a novel key expansion design approach for the original AES algorithm. In this multi core architecture the memory controller of each AES processor was designed for the maximum overlapping between data transfer and encryption and thus reducing interrupt handling load of the host processor.

Hung-Min Sun [10] *et al.* proposed dual RSA algorithm and also analyzed the security of the algorithm. Dual RSA was a variant of RSA which could be used in situations that require two instances of RSA with the advantage of reducing the storage requirements for the keys. Two applications for dual RSA were blind signatures and authentication. The security of dual RSA was raised in comparison to RSA when there were small values of e and d. The main disadvantage of using dual RSA was that the computational complexity of the key generation algorithms was also increased.

3. GAP IN STUDY

The following observations have been drawn from the literature survey and are stated below:
a) Single key of short length is not capable to provide secured cryptographic model. b) Long length key can be able to provide secured cryptographic model. c) In order to keep all the primitives in limit optimized hardware is required. d) Use of dynamic keys are preferred for encryption process and e) There is a need to optimize the key arrangement in order to achieve secured cryptographic model.

4. RESULTS AND DISCUSSION

Problem Formulation: There are several problems with RSA. One of the problem with RSA is factoring because if N is factored then it is very easy to find private key. So, keeping in mind we proposed modified RSA.

Proposed work is stated below.

1. Select four prime numbers p, q, r and s at random.
2. Multiply p, q, r and s which come up with N.
3. Choose a number relatively prime to z and call it d.
 Where z = (p-1)(q-1)(r-1)(s-1).
4. Find e such that e*d = 1 mod z.
5. Public Key is (n, e).
6. Private Key is (n, d).
7. Cipher Text = power (PT, e) mod (n).
8. Plain Text =power (CT, d) mod n.

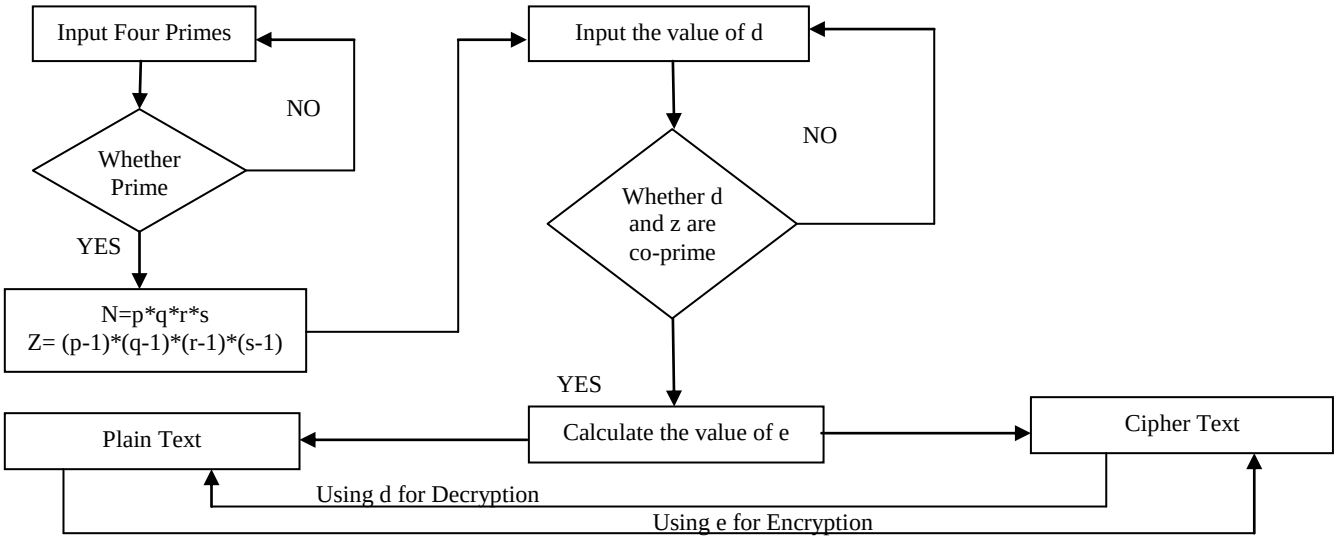


Fig 2: Flowchart of Proposed Algorithm

5. COMPARATIVE ANALYSIS

Performance measurement criteria are time taken by the algorithms to perform the encryption and decryption of the input text file that is encryption throughput and decryption throughput. Throughput(kb/msec) =ΣInput File Size(kb)/Σ Execution Time(msec)

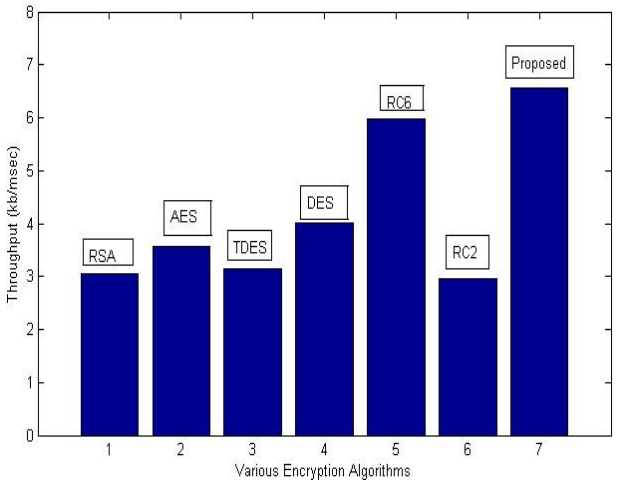
5.1 Encryption Throughput

The encryption throughput is the time taken to encrypt 1kb file in 1msec. Encryption throughput for RSA, AES, TDES, DES, RC6, RC2 and proposed algorithm are 3.06, , 3.56, 3.14, 4.01, 5.97, 2.97 and 6.57 (kb/msec) respectively. Since it is shown that proposed algorithm consumes less time for all types of file sizes and has greater throughput.

Table 1: Encryption Throughput

Input File Size(kb)	Encryption Execution Time(msec)						
	RSA	AES	TDES	DES	RC6	RC2	Proposed
49	49	38	48	33	24	57	27
59	60	56	54	29	41	60	30
100	93	90	81	49	60	91	42
247	125	112	111	47	77	121	45
321	158	164	167	82	109	168	75
694	222	210	226	144	123	262	135
899	369	258	299	240	162	268	160
5345.28	1441	1237	1466	1296	695	1570	660
Throughput(kb/msec)	3.06	3.56	3.14	4.01	5.97	2.97	6.57

From the above calculated values of throughput we are able to plot the bar graph of various encryption algorithms. It is clear from the bar graph that proposed algorithm is best and RC2 is worst among other encryption algorithms.



Graph 1: Encryption Throughput

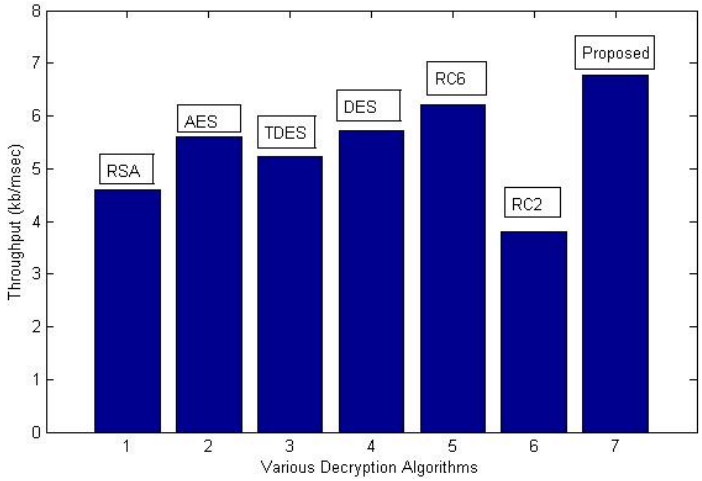
5.2 Decryption Throuhput

The decryption throughput is the time taken to decrypt 1kb file in 1msec. Decryption throughput for RSA, AES, TDES, DES, RC6, RC2 and proposed algorithm are 4.59, 5.61, 5.22, 5.71, 6.22, 3.79 and 6.77 (kb/msec) respectively. Since it is shown that proposed algorithm consumes less time for all types of file sizes and has greater throughput.

Table 2: Decryption Throughput

Input File Size(kb)	Decryption Execution Time(msec)						
	RSA	AES	TDES	DES	RC6	RC2	Proposed
49	51	58	51	42	28	59	25
59	60	63	53	50	35	65	32
100	76	60	57	57	58	90	53
247	110	76	77	72	66	95	59
321	158	149	87	74	100	161	71
694	171	142	147	120	119	165	134
899	173	171	171	152	150	183	145
5345.28	880	655	835	783	684	1216	619
Throughput (kb/msec)	4.59	5.61	5.22	5.71	6.22	3.79	6.77

From the above calculated values of throughput we are able to plot the bar graph of various decryption algorithms. It is clear from the bar graph that proposed algorithm is best and RC2 is worst among other decryption algorithms.



Graph 2: Decryption Throughput

6. CONCLUSION AND FUTURE SCOPE

After studying various encryption algorithms it is found that the strength of the algorithm depends on the length of the key. As the key length is increased the security of algorithm is also increased but performance degrades and vice-versa. To avoid this we have to optimize the key length. After critically analyzing RSA it is found that there are some flaws in it and to overcome these flaws a new algorithm has been proposed. The proposed algorithm increases the security of the system and also reduces the computation time. When proposed algorithm is compared with other algorithms it is found that throughput of proposed algorithm is greater than other encryption algorithms. In future work can be carried out to decrease the complexity of the algorithm.

7. REFERENCES

[1] A.J. Elbirt, W. Yip, B. Chetwynd and C. Paar, "An FPGA Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 9, No. 4, pp. 545-557, 2001.

[2] Hua Li and J. Li, "A New Compact Dual-Core Architecture for AES Encryption and Decryption", IEEE Canadian Journal of Electrical and Computer Engineering, Vol. 33, No. 3, pp. 209-213, 2008.

[3] Jason H. Li, B. Bhattacharjee, M. Yu and Levy, "A Scalable Key Management and Clustering Scheme for Wireless Adhoc and Sensor Networks", Journal of Future

Generation Computer Systems, Elsevier Science Publishers, Vol. 24, pp. 860-869, 2008.

[4] E. Bertino, N. Shang and S. S. Wagstaff, "An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 2, pp. 65-70, 2008.

[5] H. Chien, "Efficient Time-Bound Hierarchical Key Assignment Scheme", IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 10, pp. 1301-1304, 2004.

[6] H. C. Williams, "A Modification of the RSA Public-Key Encryption Procedure", IEEE Transactions on Information Theory, Vol. 26, No. 6, pp. 726-729, 1980.

[7] M. E. Hellman, "An Extension of the Shannon Theory Approach to Cryptography", IEEE Transactions on Information Theory, Vol. 23, No. 3, pp. 289-294, 1977.

[8] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, Vol. 31, No. 4, pp. 469-472, 1985.

[9] M. Y. Wang, C. P. Su, C. L. Horng, C.W. Wu and C. T. Huang, "Single and Multi-core Configurable AES Architectures for Flexible Security", IEEE Transactions on Very Large Scale Integration Systems, Vol. 18, No. 4, pp. 541-552, 2010.

[10] K. Bhatele, A. Sinhal and M. Pathak, "A Novel Approach to the Design of a New Hybrid Security Protocol Architecture", IEEE International Conference on Advanced Communication Control and Computing Technologies, pp.429-433, 2012.

[11] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM Magazine, Vol. 21, No. 2, pp. 120-126, 1978.