Improved DSA Cryptographic protocol and its comparative study with RSA protocol

Dhananjaya Singh, Assistant Professor, Computer Science Department, AIACT&R, Delhi-110031,India. dhananjaya1987@gmail.com

Parma Nand Professor,Computer Science Department, Galgotias University, Gr. Noida-201306,India parmaastya@gmail.com

Rani Astya Assistant Professor, Computer Science Department, IILM, Gr. Noida-201306, India astyarani@gmail.com

Payal Dixit, Assistant Professor, Computer Science Department, SIET, Gr. Noida-201306,India. payaldixit16@gmail.com

Abstract: Security is gratifying day after day alarm for a extensive sort of communication over the internet that operate, exchange a few words, and amass susceptible data. Data encryption is the alteration of data into the form called ciphertext which is not straightforwardly read by unintended or unwanted people. Decryption is the method of converting encrypted data back into its unique form, so that it is effortlessly tacit by the anticipated recipient. The DSA (Digital Signature Algorithm) protocol which is being commonly used for encryption and decryption is modified in this paper. The performance of this modified cryptographic technique is compared with existing RSA (Rivest Shamir and Aldemann) protocol in terms of time and security. The results achieved in the form of tables and graphs in support of this reveal significant improvement in security and time.

Keywords- Cryptograpic Algorithms, Encryption Technique, Security, RSA Algorithm, DSA Algorithm, Security Protocol, Decryption Technique.

I. INTRODUCTION

In the modern time, when the Internet provides indispensable communication [11] between millions of people and it is also being ever more used as a means for commerce hence security becomes a extremely important issue to deal with while sharing of information over the internet. Now a days, since the role of internet in every field has become utmost important hence people must be careful with the communication carried on over the internet for commercial, banking or for any other reasons so that untrusted[17] parties can't reach to them. Hence one essential feature for secure communications is the use of cryptography. Cryptography[13] is the discipline of science to write the information in secret code and this is also a prehistoric art since it has been used before hundred or thousands of year ago. Cryptographic algorithms are divided in two pars i.e. Symmetric (private key or secret key) algorithms and Asymmetric (public key) algorithms.

The classification of the cryptographic algorithm is illustrated as follows:

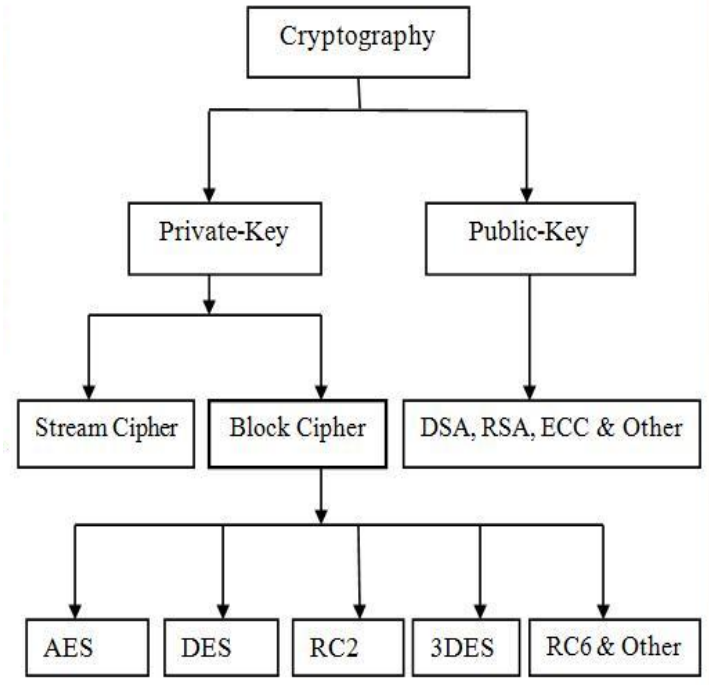


Figure1: Classification of the Cryptographic Algorithms

II. METHODOLOGY

The overall focus in this paper is to proof that our algorithm is much better on two parameters (security and time) as compared to other algorithms. The figure below shows the methodology used in this paper to accomplish the particular task. The figure is:

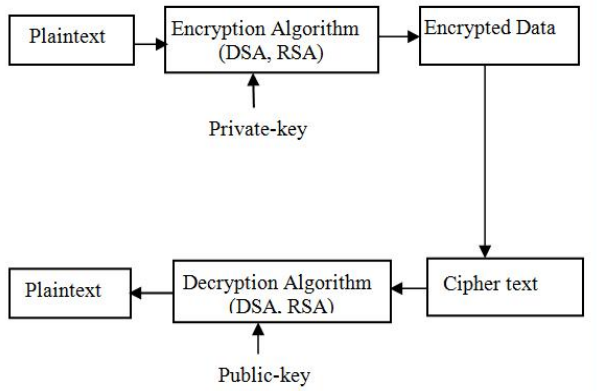


Figure 2: Technique used in the paper

The technique used to bring about this task involves the notion of cryptographic algorithms. We have shown that the work carried out in this paper gives best result based on parameters like security since we have shuffled the binary values many fold and encryption and decryption time. This technique can be applied on a various grid size for example; we can say grid can be of size 128, 64 and 32.

We have implemented our technique in this paper on grid size 32. How we have applied grid reading technique is shown below.

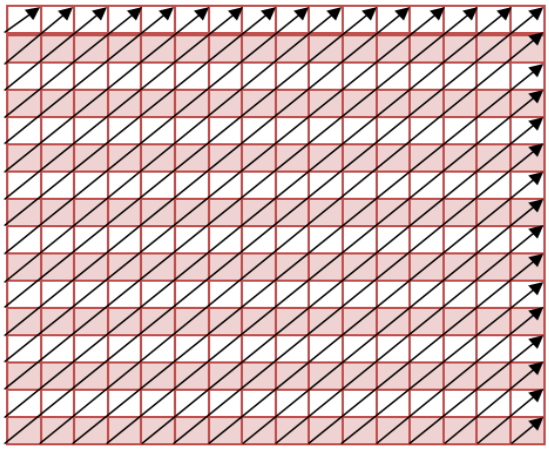


Figure 3: Technique of Grid Reading on gridsize16X16

The grid reading has been shown here on grid size 16X16 but it is implemented efficiently on grid size 32X32 which correspond to .txt file in the form of ASCII values of every character from the source file, if grid is undersized (i.e. grid is not completely full from the certain source file), then padding is made with 0's so that grid is totally fulfilled.

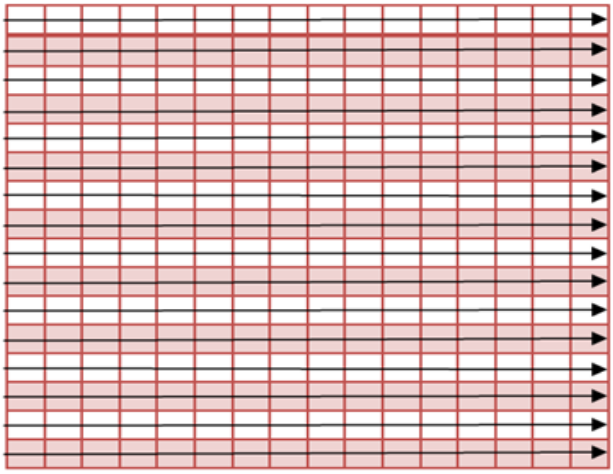
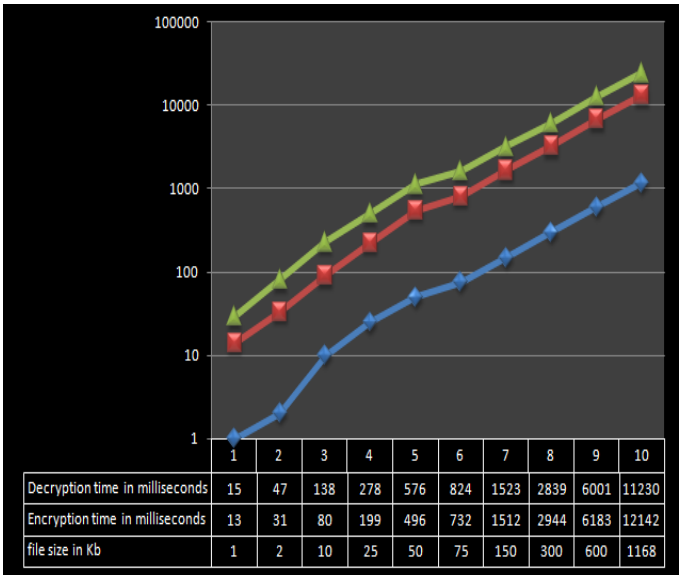


Figure 4: Technique of Grid Writing on grid size 16X16

III. RESULT ANALYSIS

The outcomes which are shown below in the form of graphs and tables are generated effectively in JAVA programming language.



	1	2	3	4	5	6	7	8	9	10
Decryption time in milliseconds	15	47	138	278	576	824	1523	2839	6001	11230
Encryption time in milliseconds	13	31	80	199	496	732	1512	2944	6183	12142
file size in Kb	1	2	10	25	50	75	150	300	600	1168

Figure 5: Implementation of RSA encryption and decryption time v/s source file on grid 32

The above graph in fig 5 is generated from table-I which is tested for various input file of different size to result encryption and decryption time.

Table I: Tested source file v/s RSA decryption and encryption time on grid size 32

Source file name	File size before encryption(in KB)	File size after encryption (in KB)	Encryption time (in millisec)	Decryption time (in millisec)
test01.txt	1	1	13	15
test02.txt	2	2.08	31	47
test03.txt	10	10	80	138
test04.txt	25	25	199	278
test05.txt	50	50	496	576
test06.txt	75	75.1	732	824
test07.txt	150	150	1512	1523
test08.txt	300	300	2944	2839
test09.txt	600	600	6183	6001
test10.txt	1168	1169	12142	11230

The graph for DSA algorithm is shown in figure 6 from table-II also implemented for source file of varying sizes which is shown below.

Table II: Tested source file v/s DSA decryption and encryption time on grid size 32

File name	File size before encryption(in KB)	File size after encryption (in KB)	Encryption time (in millisec)	Decryption time (in millisec)
File01.txt	1	1	47	31
File02.txt	2	2	31	31
File03.txt	4.01	4.01	31	16
File04.txt	6	6	47	32
File05.txt	10	10	31	16
File06.txt	25	25	109	47
File07.txt	50	50	125	47
File08.txt	75	75	172	31
File09.txt	150	150	62	15

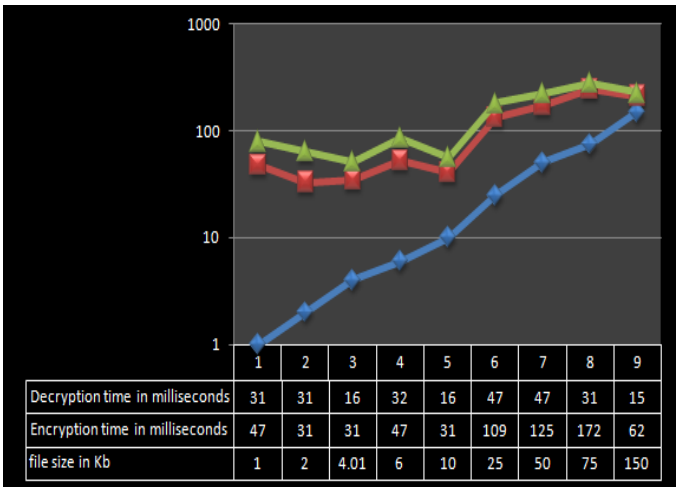
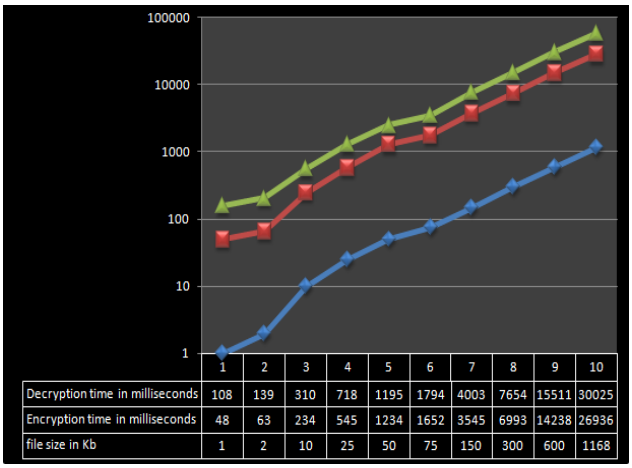


Figure 6: Implementation of DSA encryption and decryption time v/s source file on grid 32

From figure 6 it is concluded that the decryption time for DSA algorithm is very less in comparison to all the other algorithms of varying grid size i.e for RSA (graph shown in fig 5, 7 and table I, III). We found that as we enlarge the length of the source file, the decryption time for DSA algorithm keep on decrementing as the graph shows (fig 6). Hence we can say our algorithm is more efficient in terms of security and time as have shown that result of our algorithm is much better as compared to the existing work done so far on varying grid size. Now the table-III for RSA algorithm [21] on grid size 64 for different source file is given as follows:

Table III: Tested source file v/s RSA decryption and encryption time on grid size 64

Source file name	File size before encryption(in KB)	File size after encryption (in KB)	Encryption time (in millisec)	Decryption time (in millisec)
test01.txt	1	1	48	108
test02.txt	2	2.08	63	139
test03.txt	10	10	234	310
test04.txt	25	25	545	718
test05.txt	50	50	1234	1195
test06.txt	75	75.1	1652	1794
test07.txt	150	150	3545	4003
test08.txt	300	300	6993	7654
test09.txt	600	600	14238	15511
test10.txt	1168	1169	26936	30025



	1	2	3	4	5	6	7	8	9	10
Decryption time in milliseconds	108	139	310	718	1195	1794	4003	7654	15511	30025
Encryption time in milliseconds	48	63	234	545	1234	1652	3545	6993	14238	26936
file size in Kb	1	2	10	25	50	75	150	300	600	1168

Figure 7: Implementation of RSA encryption and decryption time v/s source file on grid 64

IV. CONCLUSION

In this paper, we have implemented the .txt file of various sizes on varying grid of size say 32 and 64 to find the encryption and decryption time. We have also shown (in result section in the form of table and graphs) that encryption and decryption time by using our technique is best as compared to existing work say RSA algorithm on grid size 32 and 64. Hence we say that this work is best on two parameters say security and time.

V. FUTURE ENHANCEMENTS

The graphs and tables generated in this paper are successfully implemented to encrypt and decrypt the plaintext (.txt files) in JAVA programming language on grid size 32 and 64. The future enhancements for this work is that others cryptographic algorithms like ECC[15] (Elliptic Curve Cryptography), Diffie-Hellman algorithm[16], AES algorithm[8] can be used to encrypt and decrypt on word file or pdf file or image or video on grid size of variable size say 32, 64 and 128.
Security [11] can also be enhanced it its future work by changing the techniques and algorithms used in this work.

REFERENCES

[1] Alaa A, Khaled A., Waiel F., Mohamed A., 2010,"Attack and construction of simulator for some of cipher systems using neuro-identifier," International arab journal of information technology, vol. 7, No. 4, pp. 365-372.

[2] S.A.Aljunid,S.M.Asi,S.Z.S.Idrus, January 2008 "Performance analysis of encryption algorithms text length size on web browsers," International journal of computer science and network security", vol. 8, No.1, pp. 20-25.

[3] Jawahar Thakur, Nagesh Kumar, "DES, AES and blowfish: symmetric key cryptography algorithms simulation based performance analysis", "International journal of emerging technology and advanced engineering", December 2011, vol.1, No. 2, pp. 6-12.

[4] D S Abd Elminaam,Kader H M Abdual and Hadhoud,M Mohamed, "Evaluating the performance of sysmmetric encryption algorithms", International journal of network security, May 2010, vol. 10, No. 3, pp. 216-222.

[5] Bashir Alam, Musheer Ahmad, and Omar Farooq, "Chaos based mixed keystream generation for voice data encryption","International journal on cryptography and information security", March 2012, vol. 2, No.1, pp. 39-48.

[6] Raman Maini and S Preet Singh, "Comparison of data encryption algorithms", "International journal of computer science and communication", January-June 2011, vol. 2, pp. 125-127.

[7] J.Saigeetha and V.Selvi, 2010 "Speed and security enhancement through public key cryptography", "International journal of engineering science and technology", vol.2(8), pp.3551-3556.

[8] Penchalaiah, N. and Seshadri, R., 2010. "Effective comparison and evaluation of DES and rijndael algorithm (AES)", International journal of computer science and engineering, vol. 02, No. 05, pp. 1641-1645.

[9] Schaefer F., 1996. A simplified data encryption standard algorithm, "Computer journal of cryptology", vol. 20, No. 1, pp. 77-84.

[10] Coppersmith, D, May 1994. "data encryption standard and its strength against attacks."IBM journal of research and development", pp. 243 -250.

[11] Mary Agoyi, Devrim Seral, "Sms security: an asymmetric encryption approach", sixth international conference on wireless and mobile communications, 2010 IEEE, pp 448-452.

[12] Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, 1977.

[13] J. Daemen and V. Rijmen, "Rijndael, the advanced encryption standard", Dr. Dobb's Journal, Vol. 26, No. 3, March 2001, pp. 137-139.

[14] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, vol. 21, No. 2, pp. 120 - 126, 1978.

[15] Neal Koblitz, "Elliptic curve cryptosystems", Mathematics of computation,vol. 48, 1987, pp.203-209.

[16] P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", proceedings, 35th annual symposium on the foundations of computer science, 1994, pp. 124.

[17] Dan Boneh, "Twenty years of attacks on the RSA cryptosystem", Notices of the AMS, vol. 46, No. 2, Feb. 1999, pp. 203-213.

[18] M. Wiener, "Cryptanalysis of short RSA secret exponents",IEEE transactions on information theory, vol.36,1990, pp.553-558.

[19] D.Boneh, G.Durfee, "Cryptanalysis of RSA with private key d<N.292", proceedings of eurocrypt'98, 1998, pp. 1-11.
[20] D. Coppersmith, "Small solutions to polynomial equations and low exponent RSA vulnerabilities", Journal of cryptology, vol. 10, 1997, pp.233-260.
[21] D. Boneh, G. Durfee, and Y. Frankel, "An attack on RSA given a fraction of the private key bits", proceedings, Asia Crypt '98, vol. 1514, 1998, pp. 25-34.
[22] Dhananjaya Singh and Parma Nand, **"**Data encryption using square grid transposition with cryptography DSA technique**"**,International journal of emerging technology and advanced engineering, Vol. 2, Issue 6, June 2012, ISSN 2250–2459, pp: 393-398.