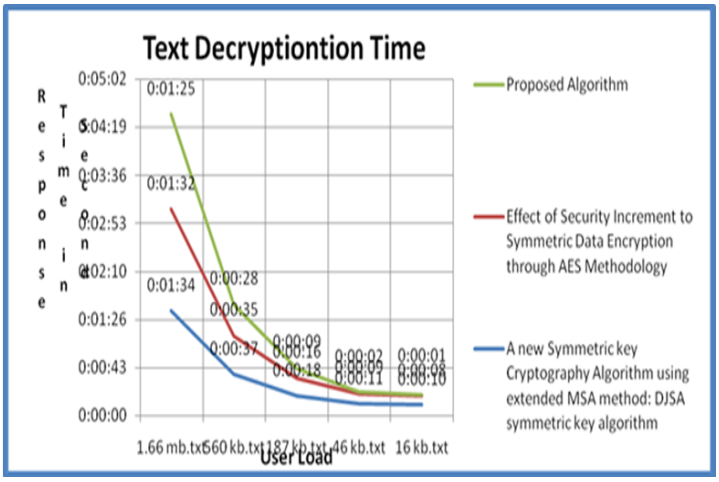

Figure 10: Decryption time comparison of text files between various algorithms with proposed algorithm

Characteristic of Proposed Technique:

Simplicity: Our proposed algorithm is very simple. Each trading partner can use the same encryption algorithm no need to develop and exchange secret algorithms.

Security: Due to the length of the key our proposed technique is very much secured.

Throughput: Due to its simplicity we can encrypt data with high rates. Proposed Keys for symmetric-key ciphers are relatively short.

Efficiency: Due to simplicity our proposed technique is high efficient. To produce stronger ciphers our proposed symmetric key can be a good choice. Symmetric-key encryption is perceived to have an extensive history.

Robustness: With the advances in technology it is of vital importance that our encryption system is robust enough to withstand the advances in technology. The more an encryption technique relies on mathematics, the less the robustness.

Availability: Some of the encryption techniques discussed have been around for years, but not all are fully functional yet. Those that have been around for some time may have the advantage of being "tried-and-tested", while some organizations are not familiar with others.

Integration: The integration level of our encryption system will depend on how easily it can be integrated at the application level. The proposed encryption technique must be able to be implemented on software and hardware.

Distribution: With present day technology evolving around the Internet and networks, it is important that our proposed encryption techniques work on an entire network, not only on a point-to-point basis. When one broadcast a message through a network all the intended recipients should get the same encrypted, secure message.

Time efficiency: Users expect encryption to be immediate, otherwise the process is cumbersome. The time efficiency of our proposed encryption technique measures in second to encrypt and decrypt information and it's very good.

Flexibility: The flexibility issues of our proposed encryption technique are very high which is referring to the use of keys and whether the key lengths are set, or whether different key lengths can be used.

Reliance on users: our proposed encryption techniques support this features. If a user has chosen a "bad" password or key encryption and decryption will not proceed for further action.

Conclusion and Future Enhancement: From the result its is clear that our "proposed technique" is batter result producing as compared "DJSA symmetric key algorithm" and "Effect of Security Increment to Symmetric Data Encryption through AES Methodology". If any user emphasis on security then he can use our proposed algorithm. Our method is essentially block cipher method and it will take less time if the file size is large. The important thing of our proposed method is that it is almost impossible to break the encryption algorithm without knowing the exact key value. We propose that this encryption method can be applied for data encryption and decryption in any type of public application for sending confidential data.

References

[1] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[2] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms "2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 $26.00 © 2009 IEEE DOI 10.1109/CIS.2009.81.

[3] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.

[4] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[5] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag.

[6] By Klaus Felten "An Algorithm for Symmetric Cryptography with a wide range of scalability" published by 2nd International Workshop on Embedded Systems, Internet Programming and Industial IT.

[7] Majdi Al-qdah & Lin Yi Hui "Simple Encryption/Decryption Application" published in International Journal of Computer Science and Security, Volume (1) : Issue (1).

[8] T Morkel, JHP Eloff " ENCRYPTION TECHNIQUES: A TIMELINE APPROACH" published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[9] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[10] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 978-0-7695-3263-9/08 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[11] [Rijn99]Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999.