A REVIEW OF SYMMETRIC KEY AND ASYMMETRIC KEY ENCRYPTION ALGORITHMS

Deepika Rani Bansal
M.Tech student, Department Of Computer Science & Engineering
Apex Institute Of Engineering & Technology
Jaipur, India
eng.deepika87@gmail.com

Preeti Thakur
Professor , Department Of Computer Science & Engineering
Apex Institute Of Engineering & Technology
Jaipur, India
preeti_thakur3@yahoo.com

Abstract— This review paper concentrates on the comparison of symmetric key algorithms and to find the best symmetric key algorithm among others . Many authors performed comparative analysis of symmetric key and asymmetric key algorithms using different performance parameters . As security is important to protect private information , then we need to know which algorithm is best to us .

Keywords—Encryption , performance ,attacks, security .

I. INTRODUCTION

This review paper concentrates on the comparison of symmetric key algorithms and to find the best symmetric key algorithm among others . Many authors performed comparative analysis of symmetric key and asymmetric key algorithms using different performance parameters . As security is important to protect private information , then we need to know which algorithm is best to us .

II. LITERATURE REVIEW

Abdul Karem in [1] compared DES , TDES , AES and BLOWFISH on .NET framework . He found that BLOWFISH is best . After BLOWFISH , AES performed better . AES performed better than DES . He found that TDES is the slowest algorithm (2008).

In [2] authors compared symmetric key algorithms like AES , DES , RC2,RC6,3DES for power consumption in wireless devices . Experiments are performed on .NET environment . Experiment proves that Blowfish is best among others , followed by RC6 . Text files and video files are used to check the performance of algorithms (2009) .

Authors in [3] presented performance evaluation of selected symmetric key algorithms . The selected algorithms were AES, DES, and 3DES, RC6, Blowfish and RC2. In the case of changing packet size, it was concluded that Blowfish has better performance than other popular encryption algorithms used , followed by RC6. DES has proved better than 3DES (2010) .

In [4] authors compared AES , DES and BLOWFISH . Java security and cryptography classes are used for experiment . BLOWFISH performed best in this experiment .

Authors in [5] compared BLOWFISH , AES , DES and 3DES . Experiment shows that BLOWFISH performed best , while performance of AES and DES is almost equal . AES performed little better than DES . DES has performed better than 3DES (2011) .

In [6] authors performed comparative performance analysis of different symmetric key algorithms like BLOWFISH , DES ,3DES , AES . Experiments are performed on a simulation software . Results shows that BLOWFISH performed best followed by AES . DES performed better than 3DES . AES performed better than DES (2011) .

According to [7] BLOWFISH is the most secure among TDES , AES , DES . DES is prone to brute force attack , it has only 2^{56} key combinations , which are easy to break . For hacker it is easy to break DES (2012).

In [8] authors performed comparative analysis of DES , 3DES , AES , BLOWFISH . Experiments are performed on simulation software . Experiments shows that BLOWFISH performed best . AES and DES performed almost equal .AES performed little better than DES (2012).

In [9] authors studied different cryptographic algorithms and compare the performance of BLOWFISH and AES . Experiments are performed using different audio files . Results proved that BLOWFISH is performed better than AES (2012).

In [10] authors compared the symmetric key algorithms . Experiment is done on visual studio .NET framework . Comparison is done on AES , TWOFISH , BLOWFISH , CAST -256 . BLOWFISH performed best among all algorithms (2013) .

Authors in [11] compared the various algorithms DES , IDEA , BLOWFISH , CAST 128 , RC6 . These algorithms are implemented in java using IAIK-JCE library in NetBeans IDE 7.0.1 . Algorithms are compared on the basis of execution time . Experiment shows that RC6 has minimum execution time .Throughput of RC6 and BLOWFISH is almost equal . BLOWFISH performed better than IDEA . IDEA has better throughput than DES for decryption but for encryption DES has better performance . CAST 128 and IDEA has almost same throughput (2013) .

In [12] authors compared various symmetric key algorithms like DES , 3DES , IDEA , MARS , CAST 128 , BLOWFISH , AES , RC6 . Again BLOWFISH performed best . Memory usage of AES and DES is equal , but performance of AES is better than DES . CAST and DES performed equal . IDEA , MARS , 3DES require same amount of memory and little difference in performance (2014) .

In [13] authors studied different encryption algorithms like DES , 3DES , AES , BLOWFISH , RSA , DIFFIE-HELLMAN . BLOWFISH is reviewed as best in terms of power consumption , security , encryption ratio , throughput , speed .After BLOWFISH , AES performed better . After AES , performance of DES was good .Authors also introduced attacks for every algorithms , for DES , brute force attack is powerful (2014).

Authors in [14] compared and reviewed different symmetric key and asymmetric key algorithms like DES ,3DES, AES, RSA ,BLOWFISH , TWOFISH , THREEFISH , RC5 , ECC , IDEA. They found BLOWFISH fastest and 3DES slowest . They also listed the all possible attacks on these algorithms like for DES , exhaustive key search attack , differential cryptanalysis attack , linear cryptanalysis attack (2015).

In [15] authors did performance evaluation of selected symmetric key algorithms . The selected algorithms were AES , DES and BLOWFISH . Performance is evaluated in terms of throughput and power consumption for wireless devices . Experiments are performed on .NET 2010 . Different size text files , audio files and image files are used for performance evaluation . Results proved that performance of BLOWFISH is better than AES and DES . (2015).

III. CONCLUSION

We reviewed different existing symmetric key and asymmetric key algorithms . We can see that in our literature survey it is proved by authors that symmetric key algorithms are faster than asymmetric key algorithms . As in survey , different researchers proved BLOWFISH performed best among other symmetric key algorithms . Performance of BLOWFISH is measured on various types of file like image file , text file , video file etc. with different loads under different operating system and various web browsers .

ACKNOWLEDGMENT

I want to give my sincere thanks to Ms. Preeti Thakur , for her guidance throughout my research . Her deep knowledge and diligence helped me a lot. I also want to express my profound gratitude for my family and friends for their unfailing support and encouragement .

REFERENCES

[1] Tamimi, A. Al. "Performance analysis of data encryption algorithms." Retrieved October 1 (2008).
[2] Elminaam, Diaa Salama Abdul, Hatem M. Abdul Kader, and Mohie M. Hadhoud. "Performance evaluation of symmetric encryption algorithms on power consumption for wireless devices." International Journal of Computer Theory and Engineering 1, no. 4 (2009): 343
[3] Minaam, D. S. A., Abdual-Kader, H. M., & Hadhoud, M. M. (2010). Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types. IJ Network Security, 11(2), 78-87.
[4] Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis.International journal of emerging technology and advanced engineering, 1(2), 6-12.
[5] Singh, Simar Preet, and Raman Maini. "Comparison of data encryption algorithms." International Journal of Computer Science and Communication 2.1 (2011): 125-127.
[6] Singh, Gurjeevan, Ashwani Kumar Singla, and K. S. Sandha. "Through Put Analysis of Various Encryption Algorithms." IJCST 2.3 (2011).
[7] Agrawal, M., & Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. International Journal on Computer Science and Engineering, 4(5), 877.
[8] Mandal, P. C. (2012). Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish. Journal of Global Research in Computer Science, 3(8), 67-70.
[9] Pavithra, S., & Ramadevi, M. E. (2012). STUDY AND PERFORMANCE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),1(5), pp-82.
[10] Apoorva, Y. K. (2013). Comparative study of different symmetric key cryptography algorithms. International Journal of Application or Innovation in Engineering and Management, 2(7), 204-6.

[11] Aggarwal, K., Saini, J. K., & Verma, H. K. (2013). Performance Evaluation of RC6, Blowfish, DES, IDEA, CAST-128 Block Ciphers. International Journal of Computer Applications, 68(25).
[12] Mushtaque, M. A. (2014). Comparative Analysis on Different parameters of Encryption Algorithms for Information Security. JCSE International Journal of Computer Science, 2(4).
[13] Tripathi, R., & Agrawal, S. (2014). Comparative Study of Symmetric and Asymmetric Cryptography Techniques. International Journal of Advance Foundation and Research in Computer (IJAFRC), ISSN, 2348-4853.
[14] Bhanot, R., & Hans, R. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. International Journal of Security and Its Applications, 9(4), 289-306.
[15] Adekanmbi, O. O., Omitola, O. O., Oyedare, T. R., & Olatinwo, S. O. Performance Evaluation of Common Encryption Algorithms for Throughput and Energy Consumption of a Wireless System.