Abstract

Key Generation is a technique to provide a secure and efficient generation of Key Pairs so that the keys can't be attacked by the external or unauthorized users. Since there are various techniques implemented for the generation of keys such as based on Graphical Methods [1]. Here in this paper a review of all the existing techniques implemented for the generation of Key Pairs is analyzed and discuss their various advantages and limitations, so that on the basis of various issues in the existing Key Pairs Generation Techniques a new and efficient technique is implemented in future.n this paper, we describe the formatting guidelines for IJCA Journal Submission.

References

2. Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, and Gene Tsudik. On the performance of
Pairwise Independent Key Generation Algorithm: A Survey

4. Jose A. Onieva, Jianying Zhou, and Javier Lopez “Analysis of an Asynchronous Multi
5. Giuseppe Ateniese, “Efficient Verifiable Encryption (and Fair Exchange) of Digital
Signatures”, Proceedings of the 6th ACM conference on Computer and communications
6. F. Bao, R. H. Deng, and W. Mao, “Efficient and practical fair exchange protocols with
8. G. Wang, “Generic non-repudiation protocols supporting transparent off-line TTP,”
9. Vinod Moreshwar Vaze, “Digital Signature on-line, One Time Private Key [OTPK]”,
International Journal of Scientific & Engineering Research, ISSN:2229-5518, Volume 3, Issue 3,
March -2012.
Signature”, IEEE Transactions On Information Forensics And Security, Vol. 5, No. 1, March
2010.
TTPs”, IJCA Special Issue on “Computational Science – New Dimensions & Perspectives”
NCCSE, 2011.
Signatures”, Proceedings of the 6th ACM conference on Computer and communications
13. Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Provably authenticated
group Diffie-Hellman key exchange - The dynamic case. In Proceedings of the 7th International
Conference on the Theory and Application of Cryptology and Information Security: Advances in
79, 87
contract signing protocol,” in Proc. ACISP’04, vol. 3108, LNCS, pp. 176–187, Springer-Verlag,
2004.
17. K. Kalaivani, K. Renugadevi, Nithya, “Pairwise Independent Network using Key
18. Sirin Nitinawarat, Chunxuan Ye, Alexander Barg, “Secrete Key Generation for a
19. Peng Xu, Zhinguo Ding, Xuchu Dai,” The private Key Capacity of a Cooperative


Index Terms

Computer Science  Algorithms

Keywords