Table 9: Effect of Key search space with size of Ciphertexts

Number of Ciphertexts	Average Key Search Space				
	GSO $h_{coeff}(k)=1$ (GA)	GSO $h_{coeff}(k)=0$ (PSO)	GSO $h_{coeff}(k)=0.2$	GSO $h_{coeff}(k)= 0.3$	GSO $h_{coeff}(k)=rand(k)$
100	272	258	242	235	221
500	265	232	228	205	197
1000	240	210	201	191	182

5. Conclusion

In this paper, a novel approach GSO by combining the effectiveness of GA and PSO is proposed to attack Simplified-DES. From the results and analysis, it is observed that GSO reduces the key search space by the factor of 5.6 and runs through less time. Implementing our approach in high speed computers further reduces the time consumption. This shows that the GSO can be effectively used in the field of cryptanalysis and this approach has been reported for the first time to attack the ciphers. Though SDES is simpler than DES, this gives a better idea to attack DES and other complex block ciphers like AES .

References:

[1] Neal Koblitz, A course in Number Theory and Cryptography, Springer International Edition, 2008.

[2] William Stallings, Cryptography and Network Security Principles and Practices, Pearson Education, 2004.

[3] Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw hill Education, 2nd edition 2008.

[4] Nadia Nedjah, Ajith Abraham, Luzia de Macedo Mourelle, Swarm Intelligent systems, Studies in Computational Intelligence, Vol.26,2006.

[5] Nadia Nedjah, Ajith Abraham, Luzia de Macedo Mourelle, Computational Intelligence in Information Assurance and Security, Studies in Computational Intellige nce, Vol. 57,2007.

[6] Spillman R,Janssen M, Nelson B and Kepner N, "Use of Genetic Algorithm in Cryptanalysis of Simple Substitution Cipher" Cryptologia, Vol.17, No.4, pp. 367-377, 1993.

[7] Garg Poonam, A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm, International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April 2009 pp-34-42.

[8] Garg Poonam , Cryptanalysis of SDES via Evolutionary Computation Techniques, International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009. Pp 117-123.

[9] Nalini, Attacks of simple block ciphers via efficient heuristics, Information Sciences, pp 2553-2569.

[10] Nalini, Cryptanalysis of Simplified data encryption standard via Optimization heuristics, International Journal of Computer Sciences and network security, vol 6, No 1B, Jan 2006.

[11] Vimalathithan.R, M.L.Valarmathi, "Cryptanalysis of S-DES Using Genetic Algorithm", International Journal of Recent Trends in Engineering, Vol2, No.4, November 2009, pp.76-79.

[12] Vimalathithan.R, M.L.Valarmathi, "Cryptanalysis of S-DES Using Particle Swarm Optimization", 10th National Workshop on Cryptology, Coimbatore, India, Sep 2010.

[13] A. Gandelli, F. Grimaccia, M. Mussetta, P. Pirinoli, R.E. Zich, "Development and Validation of Different Hybridization Strategies between GA and PSO", Proc. of the 2007 IEEE Congress on Evolutionary Computation, Sept. 2007, Singapore, pp. 2782–2787.

[14] A Menezes,P.Vanoorschoot,S.Vanstone Handbook of Applied Cryptography,CRC Press,1996.

[15] J,kennedy, R.Eberhart, "A discrete Binary version of the Particle Swarm Algorithm," International Conference on Neural network, Vol. IV,pp:4104-4108, Australia,1997.

[16] J,kennedy, R.Eberhart, "Particle Swarm Optimization," IEEE international Conference on Neural Networks,pp:1942-1948,Australia,1995

[17] Collin R.Reeves, J,E Rowe, Genetic Algorithms-Principles and Perspectives, A guide to GA theory, Kluwer Academic Publishers.

[18] Haupt R.L, Haupt S.E. , Practical Genetic Algorithms, 2nd ed., Wiley, 2004.

[19] M.Mitchell, An Introduction to Genetic Algorithms, First MIT press paperback edition, 1998.

[20] Goldberg D.E., "Genetic Algorithm in Search, Optimization and Machine Learning", Boston, Addison-Wesley, 1999.