International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Multilevel Approach for Cryptography using Genetic Algorithms with Existing S-DES Key Generation Method

Dr. Pooja Bagane*[1], Dr. Deepak Dharrao[2], Dr. S. Kotrappa[3]

Submitted: 10/09/2022 **Accepted:** 20/12/2022

Abstract: Cryptography is the art of writing secret codes. Cryptographers try to write secret codes. Cryptanalysts will break secret codes. Cryptographers and cryptanalysts always try to be ahead of each other. Genetic algorithms (GA) are structured yet randomized search algorithm invented by Darwinian's evolutionary ideas about natural selection and genetics. The field of security is colossal and vast. Many researchers are working in this field to achieve security and privacy. Researchers tried different evolutionary algorithms for cryptography. This paper discussed the multilevel approach for Cryptography using the S-DES Key Generation method and genetic algorithm. Convergence of S-DES and Genetic Algorithm is more secure and unbreakable than traditional cryptosystem.

Keywords: *Cipher, Cryptography, Genetic Algorithm, Key Size, SDES*

1. Introduction

Cryptography came from a Greek word called "krypto's" which defines "Hidden Secrets". Cryptography is the exercise and theory of beating information. It is the skill/discipline of transforming plain/original data into coded data and again reconverting that plain text into its original data.

Figure 1 shows the cryptography process, which involves two methods: Encryption and Decryption. The plaintext is the original information or message, and the ciphertext is the coded one. Cipher is an algorithm for converting original text to coded text. Key is the information used in cipher known only to sender/recipient to encode or decode the data. Encryption which is also known as Encipherment, is a process of converting original data into coded one. Decryption which is also known as decipherment, is a process of recovering ciphertext from plaintext. We can summarize that cryptography is learning of encryption theory or techniques.

Cryptanalysis (codebreaking) is the survey of theory/techniques of decrypting coded data without knowing a key. Cryptology is a combination of cryptography and cryptanalysis.

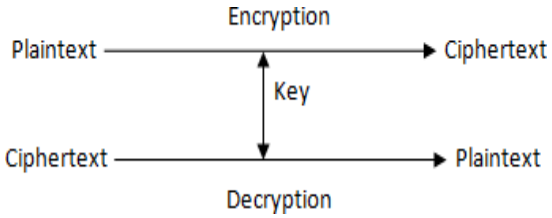


Figure 1. Cryptography Process

[1, 2] *Department of Computer Science, Symbiosis Institute of Technology, (SIT) affiliated to Symbiosis International (Deemed University), Pune, India*
[3] *Department of Computer Science & Engineering, KLE Dr. MSSCET, Belgaum, Karnataka- India.*
** Corresponding Author Email: poojabagane@email.com*

1.1. Types of Ciphers

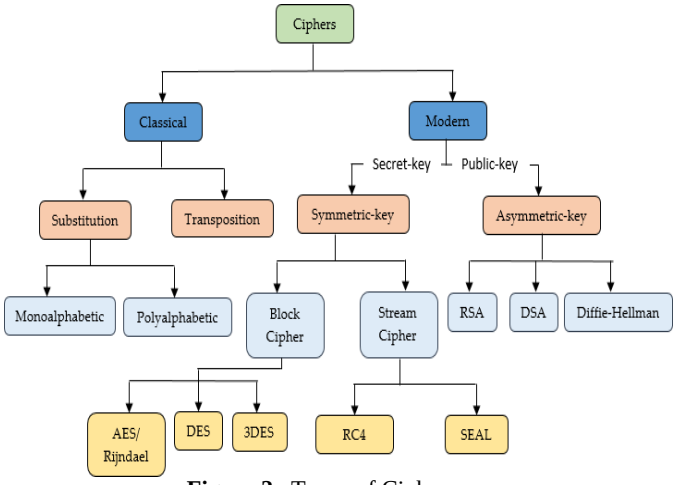


Figure 2. Types of Ciphers

Figure 2 represents types of ciphers. There are two types of ciphers: Classical (Traditional) and Modern Ciphers. Traditional cipher is used authoritatively but, for the most part, has fallen into disuse. Most classical or traditional ciphers can be reasonably computed and solved by hand in contrast with modern cryptosystems. However, they are also usually easy to decode by using recent technology. Traditional Ciphers are subdivided into two parts: Substitutions Ciphers and Transposition Ciphers. Bits are substituted all over the data for other bits in a substitution cipher. In a transposition cipher, the order of bits is rearranged with definite techniques, the original value of the bit remains the same. Binary strings will be transformed into another binary string using modern cryptographic algorithms. Based on the type of key used, there are two types in modern ciphers: Symmetric and Asymmetric. Further, based on the processing of binary strings, symmetric encryption schemes can be classified into Block Cipher and Stream Cipher. In block cipher, the plain binary text is refined

in chunks of bits at a time. In a stream cipher, bit by bit refinement of plain text. AES, DES, 3DES is the types of block cipher. RC4, SEAL is the type of stream cipher. Asymmetric encryption uses a public key. RSA, DSA, Diffie-Hellman are types of asymmetric key encryption.

1.2. S-DES

Simplified Data Encryption Standard (S-DES) is a straightforward model of the DES Algorithm. However, it is just like the DES set of rules; however, it is a smaller group of regulations and has fewer parameters than DES. It became made for instructional functions so that information DES could end up simpler. It is a block cipher that takes a block of undeniable textual content and converts it into ciphertext. It takes a block of eight-bit. It is a symmetric key cipher, i.e., they use the equal key for each encryption and decryption. In this article, we will exhibit the key era for s-des encryption and decryption set of rules. We take a random 10-bit key and bring eight-bit keys to be used for encryption and decryption.

1.3. Genetic Algorithms

Genetic algorithms (GA) are structured yet randomized search algorithm invented by Darwinian's evolutionary ideas about natural selection and genetics. Simulation of fitness of all individuals above all successive generations to work out the problem. The population of individuals has consisted of each generation. Each individual represents a point in a search space and a possible solution. Every individual needs to be processed by different genetic operations like a crossover, mutation, etc. The genetic algorithm has the following essential functions:

- Initialization: Initial population is generated randomly as stated into a uniform distribution over all possible solutions by Genetic algorithms.
- Selection: Survival of the fittest identified by the Selection operator using a fitness function.
- Variation: After selecting a promising solution using the fitness function, deviations are performed to create new solutions using Crossover (Recombination) and mutation operation. Copulating between individuals is performed by a crossover operation. Random modification in solutions will be done by Mutation operation.
- Replacement: The population of new candidate solutions substitutes the original one or its part after applying crossover and mutation to the set of promising solutions, and the next iteration is executed (starting with selection) unless termination criteria are met.

This paper includes the related works in section 2, proposed method in section 3, imple- mentation details in section 4, Results and discussion in section 5, and conclusion in section 6.

2. Related Work

The field of security is enormous and vast. Many researchers are working in this field to achieve security and privacy. Researchers tried different evolutionary algorithms for cryptography.

Rahman Dalimunthe et al. [2] used a genetic algorithm for encryption and decryption of vernam cipher with a combination of complement methods. The result shows that the proposed system provides an improved level of security. The complexity of an algorithm is more due to 2's complement method.

Pujari, S.K., Bhattacharjee, G., Bhoi, S. [3] proposed a hybridized method, a combination of DNA Sequence and Genetic Algorithm used for image encryption. The experiment proved the robustness of the DNA Sequence and GA-based method. This paper only focused on image encryption.

A stream cipher is a bit-level symmetric key cryptography algorithm. Sen, A., Ghosh, A., Nath, A. [4] used the genetic algorithm for encryption and decryption of stream cipher. A GA-based stream cipher is an unbreakable cipher; therefore, security is soaring.

Bethany Delman [7] compared traditional methods and genetic algorithms for crypt- analysis of all classical ciphers. Experimental result shows that conventional approaches are easier to implement and works better than Genetic Algorithm for cryptanalysis.

A Genetic algorithm is used by Ragheb Toemeh and Subbanagounder Arumugam [8] for cryptanalysis of polyalphabetic substitution ciphers. The result shows that successfully searched key size.

Poornima G. Naik, Girish R. Naik [9] proposed a genetic algorithm for Asymmetric key encryption and decryption. The genetic algorithm proved highly secure and unbreakable for the Asymmetric key encryption and decryption process.

3. Materials and Methods

A Genetic Algorithm can be used for encryption and decryption as it is a randomized yet structured search algorithm. Figure 3 shows Multilevel Approach for Cryptography using Genetic Algorithms, which involves encryption and decryption process using Genetic Algorithm. S-DES Block Cipher is considered here. As shown in the figure, we have taken the 10-bit key for SDES key generation and plain text from the user as input. The standard keys (i.e., two) are generated from the user-provided 10-bit key; as stated by Cesar, the smallest one is used for encryption and decryption. After key generation, the system will calculate the ciphertext, which will be the intermediate cipher. Left shift will be applied before genetic operations. Now we will use the genetic algorithm on the intermediate cipher, which includes different genetic operations like selection, crossover, and mutation. This process gives us actual ciphertext, which will be difficult to break for an unauthorized person. GA Inverse operation is used for decryption which consists of the inverse of mutation, crossover. Inversing GA, we will get intermediate data. After that, the right shift will be performed. Plain text will be calculated using the key.

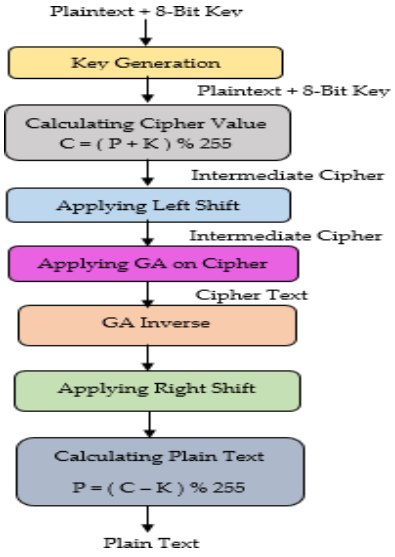


Figure 3. Multilevel Approach for Cryptography using Genetic Algorithms

4. Methodology

Encryption Process: The minor key generated, say K, is used for further operations. Using the key and user input plain text, the cipher value is calculated using the following formula,

C = (P + K) % 255

Where P is the plain text value, and K is the key generated using SDES key generation. C is the respective cipher value. For further procedure, the circular left shift is applied on intermediate cipher value, i.e., C

Example: Suppose C=11001011 After Circular shift, C=11110010

For encrypting the intermediate C value GA is applied, the following figure 4 shows how GA is used:

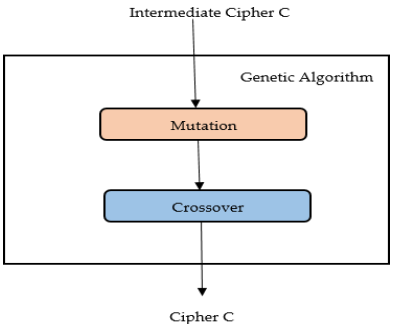


Figure 4. GA on Intermediate Cipher

Following two operations of GA are applied on input cipher value.

Mutation :

In this proposed system, single point mutation is used. The mutation is used for changing one of the characters of the parent to generate new offspring. For this, the binary equivalent of respective cipher value is obtained, and its one of the bit is changed to create new offspring. Figure 5 shows the mutation operation.

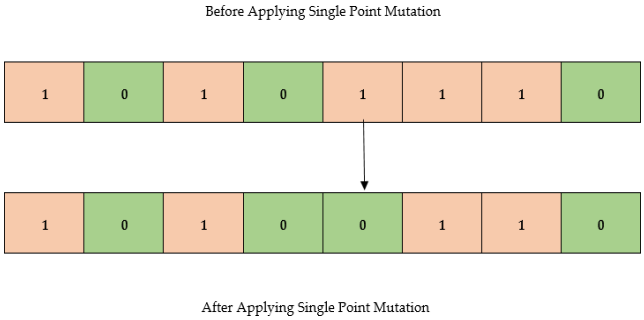


Figure 5. Mutation

Crossover :

In the crossover, the single-point crossover is used. The intermediate cipher is reversed from the middle point. Figure 6 shows the crossover operation.

After this stage, the ciphertext is produced, which is generated by using SDES key generation and genetic algorithm.

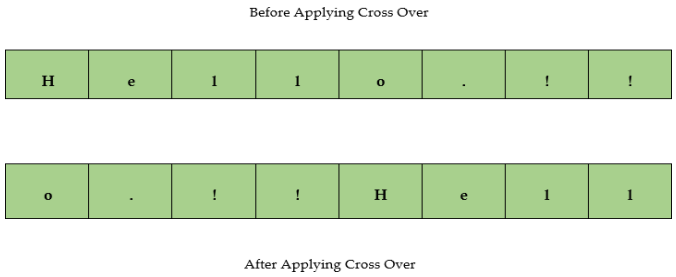
Decryption Process: In the decryption process, the exact reverse rotation of the encryption is followed, and those steps are as follows,

- Genetic Algorithm Inverse
- Circular Shift Operation
- Calculation of Plain Text

The GA Inverse is performed as follows:

First, Crossover is performed and, then Mutation.

Figure 6. Mutation



The figure 7 shows how the crossover and mutation are performed in the decryption process.

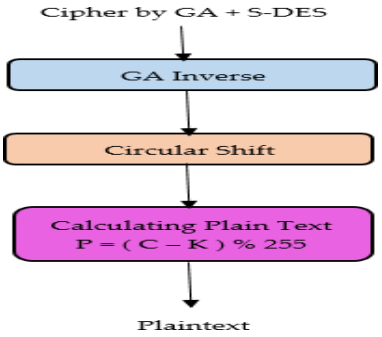


Figure 7. Decryption Process

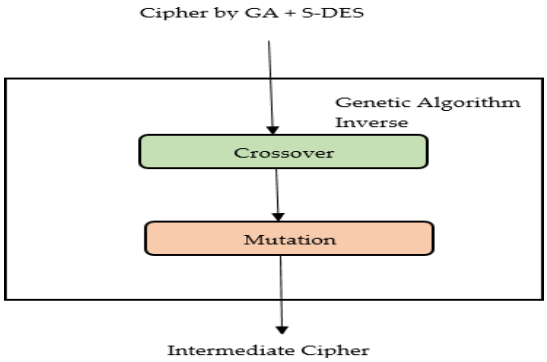


Figure 8. Genetic Algorithm Inverse

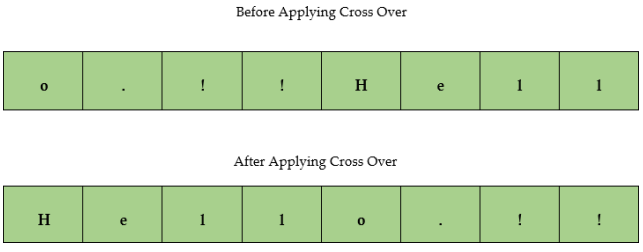


Figure 9. Crossover in Decryption

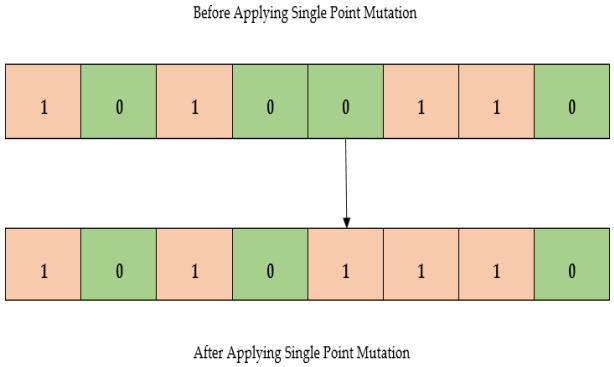
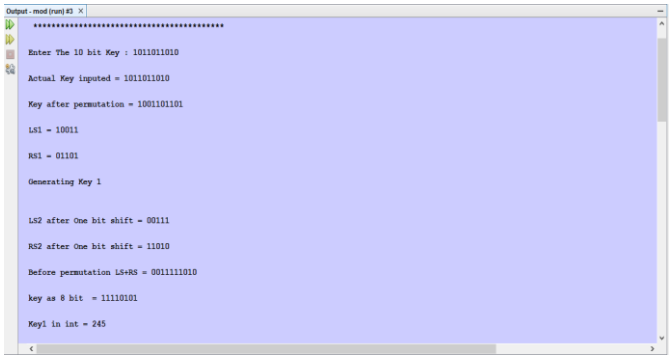


Figure 10. Mutation in Decryption Process

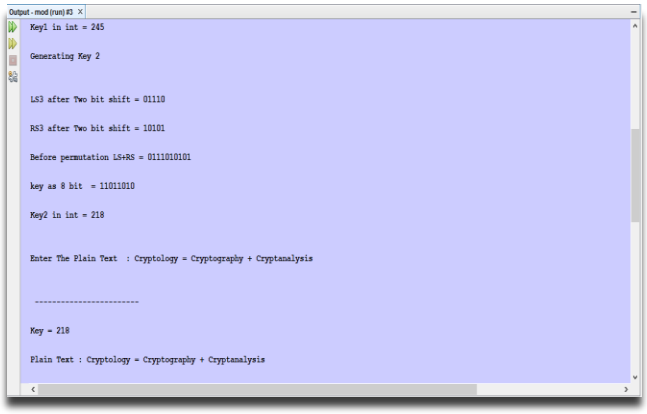
5. Results and Discussions

We have examined the above-proposed set of rules on various textual content documents, which incorporates records and undeniable textual content, numeric values, and unique characters. Since the proposed collection of rules paintings at the records' binary layout, this set of rules may be carried out on diverse forms of records together with video, audio, textual content, etc.

In figure 11, the S-DES key Generation process is demonstrated. Initial permutations were performed on a user-inputted 10-bit key. After the key is divided into two halves, shift operation will have completed. As per S-DES basic rule, the 8-bit key will be generated after shift and permutation.



(a)



(b)

Figure 11. S-DES Key Generation for Encryption (a) First Key Generation (b) Second Key Generation

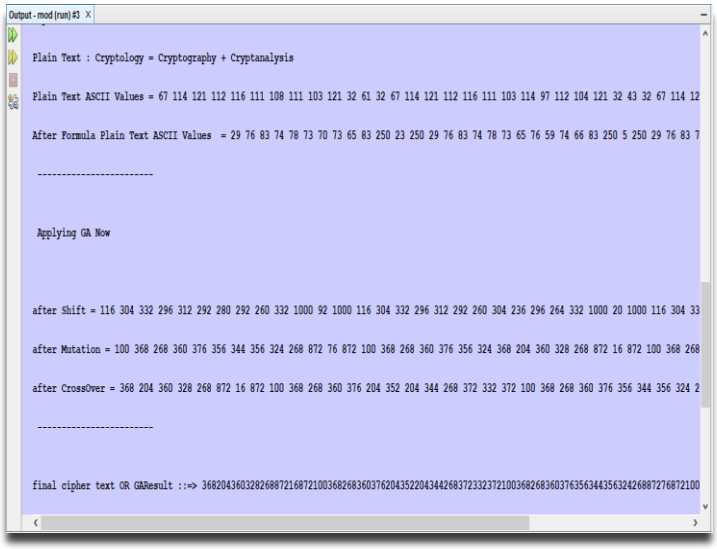


Figure 12. Encryption by applying GA after S-DES Key Generation

In figure 12 presented the Encryption process by applying GA after the S-DES Key Generation method. After generating the 8 bit key by the S-DES method, Plain text will be inputted by the user. ASCII values of text will be considered for the further process. Shift, Mutation, Crossover operations from Genetic Algorithms will be applied to these ASCII values, and final ciphertext will be generated.

The decryption process by GA inverse is demonstrated in figure 13. Crossover, Mutation, Shift Operation will be performed on ASCII values, and original plain text will be generated.

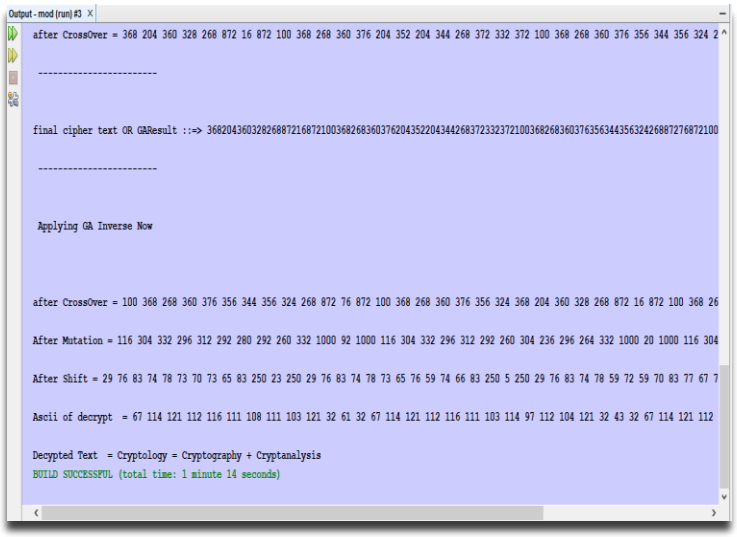


Figure 13. Decryption Process

Table 1 shows comparisons of traditional cryptography algorithms and GA-based proposed methods based on the key size, data input size, and a number of alternate keys. S-DES algorithm has the 8-bit key size and 10-bit input size, which provides 28 alternate keys; therefore, it is simple to break. DES algorithm has a 56-bit key size and 64-bit input size, which offers 256 alternate keys. AES algorithm has 128-bit key size and 128-bit input size, which provides 2128 alternate keys. The Triple-DES algorithm has a 168-bit key size and 128-bit input size, which provides 2168 alternate keys. The genetic algorithm-based proposed method has the

variable key length and variable output size, which provides 2256 number of alternative keys; therefore, it is arduous to break.

Table 1. Comparison of different cryptographic algorithms w.r.t. key size, input size, and a number of alternate keys.

We have plotted the graph for the above data and presented it in figure 14. We can summarize that GA based S-DES method is more secure than the traditional cryptosystem.

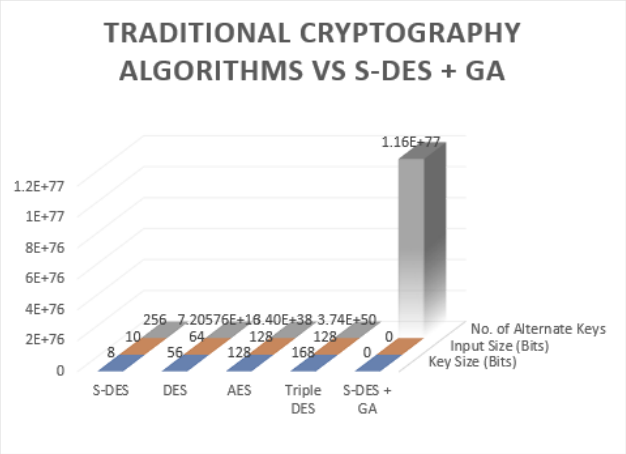


Figure 14. Comparisons of traditional cryptography algorithms and S-DES + GA

6. Conclusion

This paper presents a multilevel approach for Cryptography using the S-DES Key Generation method and genetic algorithm towards cyber security. Genetic algorithms (GA) are structured yet randomized search algorithm invented by Darwinian's evolutionary ideas about natural selection and genetics. Cryptography is the art of writing secret codes. Cryptographers try to write secret codes. Cryptanalysts will break secret codes. Cryptographers and cryptanalysts always try to be ahead of each other. Convergence of S-DES and Genetic Algorithm is more secure and unbreakable than traditional cryptosystem.
We would like to implement and upgrade the performance of genetic algorithms and experiments for different advanced ciphers like AES, DES.

Acknowledgements

We would like to thank Symbiosis International (Deemed University) for providing research facilities. We also want to thank KLE Dr. MSSCET and VTU Belgaum for providing facilities for our research work.

Author contributions

Pooja Bagane: Conceptualization, Methodology, Software, Data curation, Writing-Original draft preparation **Deepak Dharrao:** Software, Validation, Field study **S.Kotrappa:** Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] D. E. Goldberg, "Genetic Algorithms in Search, Optimization, and Machine Learning", 4th ed, Pearson Education, 2009.
[2] A. R. Dalimunthe, H. Mawengkang, S. Suwilo, and A. Nazam, "Vernam Cipher with Complement Method and Optimization Key with Genetic Algorithm," Journal of Physics: Conference Series, 2019.
[3] S. K. Pujari, G. Bhattacharjee, and S. A. Bhoi, "Hybridized Model for Im- age Encryption through Genetic Algorithm and DNA Sequence," Procedia Computer Science, 2018.
[4] A. Sen, A. Ghosh, and A. Nath, "Bit level symmetric key cryptography using genetic algorithm," Proceedings - 7th International Conference on Communication Systems and Network Technologies, 2017.
[5] S. F. U. Khan and Bhatia, "A NOVEL APPROACH TO GENETIC ALGO- RITHM BASED CRYPTOGRAPHY," International Journal of Research in Computer Science, vol. 2, no. 3, pp. 7–10, 2012.
[6] W. Stallings, "Cryptography and Network security Principles and Practices", Pearson Education, Fourth Edition, 2010.
[7] B. Delman, "Genetic Algorithms in Cryptography", Ronchester Institute of Technology, New York, 2004.
[8] R. Toemeh and S. Arumugam, "Applying Genetic Algorithms for Searching Key-Space of Polyalphabetic Substitution Ciphers," The International Arab Journal of Information Technology, vol. 5, no. 1, 2008.
[9] Dr, G. Poornima, G. R. Naik, and Naik, "Asymmetric Key Encryption using Genetic Algorithm," International Journal of Latest Trends in Engineering and Technology (IJLTET), vol. 3, no. 3, 2014.
[10] D. Dr, P. Singh, D. R. Rani, and Kumar, "To Design a Genetic Algorithm for Cryptography to Enhance the Security," International Journal of Innovations in Engineering and Technology (IJIET), vol. 2, 2013.
[11] P. Garg, "A Comparison between Memetic algorithm and Genetic al- gorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm," International Journal of Network Security & Its Applications (IJNSA), vol. 1, no. 1, 2013.
[12] L. Sharma and B. K. P. Ramgopal Sharma, "Breaking of Simplified Data Encryption Standard Using Genetic Algorithm," Global Journal of Computer Science and Technology, vol. 12, no. 5, 2012.
[13] G. Patel, "Genetic Algorithm for Cryptanalysis", BITs Pilani,2008.
[14] K. Sindhuja and D. S. Pramela, "Symmetric Key Encryption Technique Using Genetic Algorithm," International Journal of Computer Science and Information Technologies (IJCSIT), vol. 5, no. 1, pp. 414–416, 2014.
[15] D. R. M. L. Vimalathithan and Valarmathi, "Cryptanalysis of S-DES using Genetic Algorithm," International Journal of Recent Trends in Engineering, vol. 2, no. 4, 2009.
[16] A. Kumar and M. K. Ghose, "Information Security using Genetic Algorithm and Chaos", 2007.
[17] A. K. Verma, M. Dave, and R. C. Joshi, "Genetic Algorithm and Tabu Search Attack on the Mono-Alphabetic Substitution Cipher in Adhoc Networks," Journal of Computer Science, vol. 3, no. 3, pp. 134–137, 2007.
[18] G. N. Rajendra and B. R. Kaur, "A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves," International Journal of Scientific and Engineering Research, vol. 2, 2011.
[19] P. A. Bagane and K. V. Kulhalli, "Genetic Algorithm for Cryptography," International Journal of Computer Application, vol. 1, 2015.
[20] P. A. Bagane and S. Kotrappa, "Cryptanalysis for S-DES using Genetic Algorithm," International Journal of Technology and Science, no. 2, 2016.
[21] P. Bagane and S. Kotrappa, "Bibliometric Survey for Cryptanalysis of Block Ciphers towards Cyber Security", Library Philosophy and Practice, 2020.

[22] P. Bagane and S. Kotrappa, “Comparison between traditional cryptographic methods and ge- netic algorithm based method towards Cyber Security,” International Journal of Advanced Research in Engineering and Technology (IJARET), vol. 12, no. 2, pp. 676–682, 2021.

[23] K. Sandyarani and P. N. Kumar, “Design and analysis of AES-CM with non-linearity S-box architecture,” International Conference on Current Trends in Engineering and Technology (ICCTET), pp. 252–254, 2013.

[24] F. Rao and J. Tan, “Energy consumption research of AES encryption al- gorithm in ZigBee,” International Conference on Cyberspace Technology, pp. 1–6, 2014.

[25] S. Koteshwara, A. Das, and K. K. Parhi, “Performance comparison of AES-GCM-SIV and AES-GCM algorithms for authenticated encryption on FPGA platforms”, 51st Asilomar Conference on Signals, Systems, and Computers, pp. 1331-1336, 2017.

[26] P. Bagane and D. K. Sirbi, “Enriching AES through the key generation from Genetic Algorithm,” Indian Journal of Computer Science and Engineering, vol. 12, no. 4, 2021.

[27] R. S. Semente, A. O. Salazar, and F. D. M. Oliveira, “CRYSEED: An automatic 8-bit cryptographic algorithm developed with genetic programming,” IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, pp. 1065–1068, 2014.