IMPACT OF VARIATIONS IN THE POPULATION SIZE AND AGES OF GENETIC ALGORITHMS IN CRYPTOGRAPHY - AN EMPIRICAL STUDY

Sarthak Mendiratta

ABSTRACT

The usage of a Genetic calculation in the symmetric square figure Advanced Encryption Standard - 128 (AES-128) calculations to improve the exhibition of cryptographic tasks. The genetic calculation is utilized for creating the best fit non-dreary figure key and for key dissemination to plan a powerful Substitution confine AES-128. The examination uncovers that the productivity of the cryptographic calculation treated with the Genetic calculation is subject to the varieties in the number of ages and introductory populace size. The outcome demonstrates that the ideal populace size has less encryption and decoding time. Among the example populace size taken for the investigation, nearly the normal populace size has the least encryption and unscrambling time. Results from cycle varieties demonstrate that the normal number of emphasis has less encryption and decoding time. Upgrades: The half breed blend of the Genetic calculation and AES-128 can be additionally changed for pictures and sound messages moreover.

1. INTRODUCTION

Cryptography offers security and protection for the data when it is communicating through the network. In order to achieve high security, the data is encrypted at the sender side and again decrypted in the receiver side using either a same key or a pair of different keys. Encryption and decryption are performed using cryptographic algorithms which can be either symmetric or asymmetric according to the types of keys used. Symmetric algorithm uses same key for both encryption and decryption. Among many algorithms developed Advanced Encryption Standard (AES) is proven to be stronger in terms of cryptanalytic attacks1. The research work has been undertaken to implement the concept of Genetic Algorithm (GA) in S-box of AES algorithm2. The experimental result shows that the control parameters of GA play an important role in cryptographic operations. The focus of this paper is to provide the experimental detail that proves the variations in the parameters like population size and number of generation has an impact on the encryption and decryption time of the enhanced AES algorithm using GA.

2. STRUCTURE OF AES

The AES algorithm belongs to the symmetric cipher in which the cryptographic process uses a single key for both encryption and decryption. The key length is equal to the input block size. AES-128 has 10 rounds of each encryption and decryption process. There are four stages in each round. They are Substitution, Transposition, mixing input plaintext and converting it to cipher text. Conversion of cipher text into plaintext follows the reverse rounds process using the same key. The strength of AES depends on the confusion (substitution) and diffusion (permutation). The inverse round is performed for decrypting the cipher text into plain text.

3. GENETIC ALGORITHM

Genetic algorithms are based on natural selection and natural genetics, which combines the survival of the fittest mechanism with a randomized information exchange to form an optimized search algorithm3. Genetic algorithms provide an optimized solution available in the search space. A conventional GA is composed of populations, fitness function and operators which controls the process.The pseudo code for a simple genetic algorithm can be described as follows.

The initial population is generated randomly and the fitness criteria are applied to it to select the first generation chromosomes. The GA operators are performed to generate new set of chromosomes; the generated result is added to the next generation. The process continues till the optimized result is reached.

3.1 Basic Terms in Genetic Algorithm

In GA, the term chromosome typically refers to a candidate solution to a problem. The high quality candidate solution from different regions of the search space is referred as parent. The combination of chromosomes termed as population is randomly generated at the initial stage of the algorithm. The chromosomes are represented either as binary (0 or 1) or hex number depending on the type of population. They are iterative in nature and transform the population into a new generation. GA uses a fitness function which assigns a score to each chromosome of the current population. The individuals are selected by applying different combination of genetic operators

3.2 Genetic Operators

A simple genetic algorithm uses three basic operators:

namely selection, crossover and mutation. Selection:
The operator selects the chromosomes in the population for reproduction according to the fitness function.

Crossover:

The operator chooses the position of bits and exchanges the chromosomes between the chosen positions.

Mutation:

The operator randomly flips the bits in a chromosome, (i.e.,) from 0 to 1 or 1 to 0.

3.3 Parameters of Genetic Algorithm

There are three major parameters that determine the efficiency of GA:

1. Encoding method.
2. Type of operator used and
3. Control Parameters.

These control parameters refers to the population size and the number of generations which are randomly generated to apply the operators 4,5. The proposed algorithm uses binary coding which is the general encoding method. For efficiency uniform crossover, Roulette Wheel Selection and Inverse Mutation are used to develop the algorithm. The proposed work concentrates on analyzing the variations in the control parameter with respect to the efficiency (i.e.,) encryption time, decryption time and throughput time of AES-GA algorithm.

4. PROPOSED ALGORITHM

The proposed algorithm uses the Genetic Algorithm process in AES to strengthen the key generated by AES-128. The strength of AES lies in combination and permutation of the key generated. This is achieved by applying GA in the process of diffusion and confusion6,7. The randomly generated initial population and the GA operators produce non-repetitive combination of encryption keys which makes the cryptanalytic attack difficult. This research paper proposes an approach to generate unique keys by using the pseudo random number generator. The basic processes of GA are used to complicate the key generated by the 128-bit key AES8. The GA process is utilized to strengthen the key generated by AES-128 which is expected to increase the data parameters9 with respect to the cryptographic time and the throughput time of the AES-GA. The proposed algorithm is shown in simple steps.

5. VARYING POPULATION AND GENERATIONS

The process of GA starts with a randomly generated population keys which are known as chromosomes. The length of the key determines the number of genes (bits) in the population. This proposed work uses 128-bit key size. The generated initial population will be treated with the genetic operators which increases the total number of chromosomes. The individuals are selected according to the fitness value. The selection operator is impacted due to the variation in the population size. Basically, the GA starts with the fixed population size and fixed number of iterations. The proposed work uses Roulette wheel selection, inversion mutation and uniform crossover with constant probability for the operators. The fitness probability is maintained as constant value10. A GA with varying population size and varying iterations11 requires very less encryption time, decryption time and throughput time in comparison with the constant control parameters GA.

6. EXPERIMENTAL RESULT AND ANALYSIS

The technique which is explained in section III has been implemented using Matlab and the observations are compared and analysed. The GA parameters are initialized as:

6.1 Variation in the Population Size

The population size is taken to be varying. The sample size taken for this research paper is 10, 50, 75, 100, 200, 300, 500, 750 and 1000. Rest all the parameters are considered as constant values. Table 1 shows the changes in memory usage, encryption and decryption time due to the variation in the population size. By varying the population sizes, other evaluating functions like crossover and mutation are kept as constant. The result shows that there is an optimum population size, beyond or below which the performance of GA in cryptographic operation degrades. For a large population size the time taken for encryption and decryption are more compare to the small population size. In the sample population set taken, for the population size of 200, the encryption time and decryption time is comparatively less than the minimum population size 10 and the maximum population size 1000. The performance has reached the peak for the100 generations and 200 population size. An optimal solution will be reached with varying Pc and Pm which will be performed as the continuation in this research. The result is shown as a graph, plotted with the population size and encryption time and decryption time. Figure 3 shows the result graph of the encryption time with varying population. Figure 4 shows the result graph of decryption time with varying population.

6.2 Variation in the Number of Iterations

The number of iterations (generations) are varying. The sample iterations are taken as 10, 30, 100, 150, 200, 250, 300 and 350. The GA parameters are initialized as:

Table 2 shows the performance of GA with respect to memory usage, encryption and decryption time due to the variation in the number of iterations. The result shows that the cryptographic time is less when the number of iterations is neither too large nor too small. With respect to the sample iterations taken, iteration size of 200 with the population size of 250 has comparatively less encryption and decryption time. The optimal result can be achieved by varying Pc and Pm with suitable crossover and mutation operators. Figure 5 shows the result graph of the encryption time with varying iterations. Figure 6 shows the result graph of decryption time with varying iterations.

7. CONCLUSION

The effect of changes in GA parameters with respect to the encryption time and decryption time of AES -128 has been studied in this research paper. Keeping the evaluation function of crossover and mutation, cryptographic key size as constant, it is observed that the cryptographic time is varying depending only on the variation in population size and number of iterations. The aim of this paper is not to project the optimal population size and iteration size for AES- 128 cryptosystem, but to reach the general conclusion.