New Approach to Crossover of Encryption Algorithms

Peter Pekarčik, Eva Chovancová(✉), Martin Chovanec, and Tatiana Kuchčáková

Technical University of Kosice, 04001 Košice, Slovakia
{peter.pekarcik,eva.chovancova,martin.chovanec,
tatiana.kuchcakova}@tuke.sk

Abstract. Our work presents a novel approach to creating new encryption algorithms. We were inspired by genetic algorithms based on the Darwin evolution theory. As the method of invention, we chose the crossover technique. We aim to create unique encryption algorithms that will be more secure, faster, and require less memory space or computational energy. New encryption algorithms are based on the most commonly used encryption techniques. During the crossover process, we consider the most critical metrics for encryption algorithms. We also briefly described the crossover and mutation process. The developed method is in the state of design. The design presented in this article is in the form of a flowchart diagram and detailed decryption. We plan to implement it and test it.

Keywords: crossover · encryption · evaluation · fitness score · genetics algorithms

1 Introduction

According to the description in [1], cryptography is one of the oldies but still one of the most prospective subfields of informatics. It found its fulfillment in communication security, which is, according to [2], the essential aspect of every computer system. In [3], it is said that a long transformation occurred during history, from the most basic forms that have their roots in the Before Christ Era to the modern usage of quantum cryptography. There are several different encryption algorithms. Those most used today - *RSA* (Rivest-Shamir-Adleman), *DES* (Data Encryption Standard), *3DES* (Triple Data Encryption Standard), or *Blowfish*, were produced between 1976 and 1998. *AES* (Advanced Encryption Standard) and *Twofish* are probably the last well-known algorithms created. They were created in 1998. According to [4], they replaced obsolete *DES*, and they are used today.

Until 1998, there has been significant progress in the speed of computers. According to [5], the newest Intel processor used in 1998 was the *Intel Pentium II*, from *Sixth generation X86 Intel processors*. It was introduced in May 1997, consisted of 3.1 million transistors, and had a clock speed of 300 MHz. However, the newest *Intel i9-13980HX*

D. Perakovic and L. Knapcikova (Eds.): FABULOUS 2024, LNICST 596, pp. 9–17, 2025.
https://doi.org/10.1007/978-3-031-72393-3_2

processor, mentioned in [6], introduced in the first quartile of 2023, consists of 14200 million transistors and can reach clock speeds up to 0.76 TFlops/s.

The situation is much more complicated when we consider quantum computers. Modern computers are defined by [7] as based on the science of quantum mechanics and its unbelievable phenomena. According to [8], these computers represent a new generation. In [9], it is mentioned that *IBM* (International Business Machines Corporation) announced its intention to develop a 100,000-qubit system by 2033. In December 2023, they were closer to that goal with *Condor*, a 1,121-qubit chip unveiled at the *IBM Quantum Summit 2023*. In [9], RSA breakthrough should occur precisely with the help of quantum computers. RSA, the most used encryption algorithm, should be broken around 2035. This algorithm is widely used in commerce, banking, telecommunication, and the following sectors to protect data, like customer information, transaction records, credit cards, or office computers. Some scientists are skeptical about this estimate, but even if this breakthrough happens later, we can assume it will happen one day. Until this time, new encryption algorithms have to be developed.

In history, new encryption algorithms, according to [10], were created by mathematicians. These people understand the mathematical concept behind these algorithms, like number theory, which involves the difficulty of large primes or permutations. The idea of these algorithms is crucial for working with them effectively. The advantage of computers, unlike of people, is the disproportionately higher speed with which they can perform different mathematical operations. Today, computers can process information incomparably faster than people. On the other hand, there is still the question of computers creativity. [11] says that today, computers can generate novel and innovative solutions based on algorithms, data, and programming. Still, they lack the consciousness, emotions, and subjective experiences of human creativity. The present newest encryption algorithms were still created by mathematicians. Is afford focused on searching for the first post-quantum algorithm, for example by *National Institute of Standard and Technologies*. However, the algorithms competing for the first post-quantum algorithm are created by large scientific groups. What can be a shortcoming when using computers to create new algorithms? Are today's computers at such a development level that we can use them to develop new encryption algorithms?

2 The Newest Encryption Algorithms

[11] says that meeting new trends has become crucial. During the last decade, cryptanalytics have considered modifying well-known encryption algorithms. They decide to expand existing solutions with new approaches like dividing the alphabet of definition into vocals and consonants or transforming letters of the input string to the binary string and performing different operations on the binary level of the string. The result of this approach is a couple of brand-new encryption algorithms:

- [12] modified the simple Ceasar cipher, which produces ciphertext that can be read and created **Modified Ceasar cipher**;
- [13] modified Playfair's cipher so that he converted each character of the input string to the binary code, chose pairs of characters and swapped parts of the strings within the pair;

- [14] decides to use the simple substitution of letters in plaintext and combine it with a rounded cipher technique and mathematical triangulation and create a **Modified Substitution cipher**;
- [15] reduced the key size of the DES algorithm to a 10-bit key and added the use of mathematical operations, such as permutation and left shift, and named this approach as **S-DES** (Simplified Data Encryption Standard);
- [16] added to the calculation of some partial steps in RSA's new operations with input variables and create **M-RSA** (Modified-RSA);
- [17] added to the calculation of some partial steps in the Rabin cryptosystem variable primes p, q, r, where $p \equiv q \equiv r \equiv 3 \ mod \ 4$, that result is the **HRabin algorithm**.

All of the mentioned algorithms were created between 2013 and the present, so there are still attempts to develop new encryption algorithms. In the creation process, they used well-known algorithms, but they were modified somehow. The goal in the creation process should be to create new algorithms that will be faster, require less memory, and, most importantly, be safer. All of these goals can be reached in the process of optimization. One of the popular methods for searching for new solutions and their optimization is genetic algorithms.

3 Genetic Algorithms

Genetic algorithms, described by [18], aim to imitate the natural changes in living ecosystems, which are social systems, evaluate the psychological consequences and model the variable methods. They are widely popular search and optimization methods for resolving highly intricate problems. At the beginning of the algorithm, an **initial population** is created. The initial population forms the first generation, noted in *Fig. 1.* as gen = (). After that, follows operation:

- **evaluation** of each chromosome from the initial population. During the evaluation is computing **fitness score** for each chromosome. The fitness score determines the suitability of chromosomes for the crossover process.
- **assign the fitness score** to chromosomes from the initial population. The best candidates are chosen according to the value of the fitness score. This process can be also named as **elitism** or **elitist selection**;
- **reproduction** of selected chromosomes and pairing up of selected individuals to swap information through a crossover;
- **crossover** of results of selection is the process during which chromosomes randomly choose a locus and exchange the subsequences before and after the locus between two chromosomes to create new offspring;
- **mutation** randomly flips some chromosomes, resulting of crossover operation.

After these steps, it is created new generation, labeled in diagram as $gen + 1$. It is checked if the result of the mutation operation meets the established criteria. If yes, the algorithm is successfully terminated, resulting in a new generation as the algorithm's output. If not, the algorithm continues evaluating and assigning fitness scores again. The diagram can also describe all of these steps:

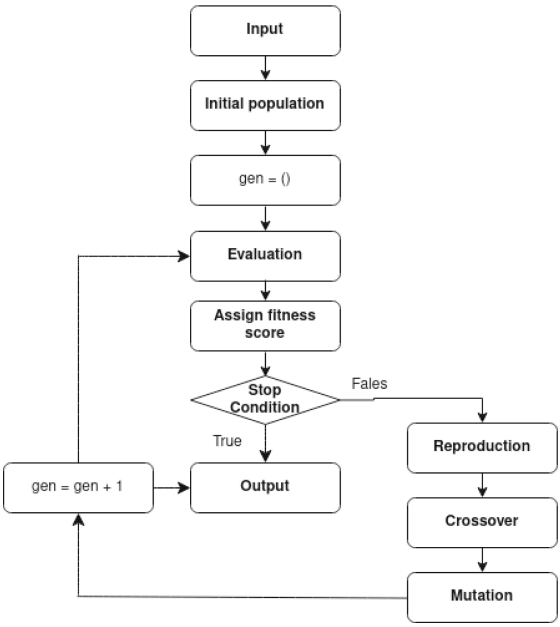

Fig.1. Flowchart of genetic algorithm[19]

It follows from the definition of genetic algorithms that this method is suitable for creating new encryption algorithms. There, we will use it as the basis of our new approach.

4 Our New Approach to the Creation of New Encryption Algorithms

In our new approach to creating new encryption algorithms, we combined the theory of genetics algorithms with the theory of encryption algorithms. As the first step, we must create the **initial population** formed by the ten most used encryption algorithms nowadays. According to [20], the most used encryption algorithms are:

- AES (Advanced Encryption Standard);
- DES (Data Encryption Standard);
- 3DES (Triple Data Encryption Standard);
- RSA (Rivest-Shamir-Adleman);
- Diffie-Hellman;
- Elliptic curve;
- Rabin encryption;
- McEliece;
- IDEA (International Data Encryption Algorithm); – Blowfish; – Twofish.

The other algorithms may be more suitable for our approach during our following research. However, we can easily add them to the initial population in this case.

When we look in detail at the steps of these algorithms, we will see that they are using:

– simple mathematical operations of counting, subtracting, multiplying, and dividing;
– operation of modulo;
– operation of comparing two variables;
– exponentiation operation;
– test if the result of dividing two numbers is an integer;
– mathematical operations with matrices;
– XOR (eXclusive OR) operation;
– rotation of bits and shifts of bits;
– recombination of bit string;
– permutations; – the inverse of the bit blocks; – shift of rows, etc.

These steps can be combined in some new form, which will help create unique encryption algorithms. The second step is the **evaluation of the fitness score**. It depends on how well the element from the population can solve the problem. Our research aims to find new encryption algorithms that will be better in some way. However, how do we appropriately establish methods for comparison of encryption algorithms? According to [21], we have to consider metrics like the type of algorithm, function, key size, number of rounds, complexity, strength, and best-known attacks. [22] moreover, it says that there are metrics for evaluating the effectiveness of an encryption algorithm: encryption time, decryption time, the throughput of encryption, the throughput of decryption, CPU (Central Processing Unit) clock cycle, CPU process time, power consumption, and memory utilization. These metrics serve as inputs to models for evaluating the performance of encryption algorithms. The models are computed parameters as: – average encryption time;

– level of the percentage of remaining battery of the computer for one run;
– average battery consumed by the computer for one run;
– average battery consumed per iteration;
– B cost of encryption (Basic cost of encryption);
– total energy cost;
– energy cost; concerning the properties of encryption algorithms, such as:
– type;
– functions;
– key size;
– number of rounds;
– complexity;
– best-known attacks; – strength, etc.

Based on these models, we can unambiguously determine all the ambiguous properties of the encryption algorithm. In the next step, we can use these models to verify whether the new algorithm's creation improved its properties. The check of improvement of all models can serve as a stop condition. It is likely not possible to reach progress in

all metrics and models at the same time. In this case, we have to decide which metrics and models will be the most important for us in creating the new algorithm.

We can check the stop condition when we have calculated the fitness score. We can continue the **reproduction process** if it is false. In our case, it means to select candidates from the initial population of encryption algorithms that best fit our model. This means that the model must be computed for all members from the initial population, and this member (these members) must be chosen to match our model best. Exactly two members may appear selected from the initial population, but more may be selected. We can check the stop condition when we have calculated the fitness score. We can continue the **reproduction process** if it is false. In our case, it means to select candidates from the initial population of encryption algorithms that best fit our model. This means that the model must be computed for all members from the initial population, and this member (these members) must be chosen to best match our model. Exactly two members may appear selected from the initial population, but more may be chosen.

We can continue with the **crossover** process when we have chosen appropriate candidates from the population of encryption algorithms. Actually, according to [23], several crossover methods exist, such as:

- **single-point crossover** - parental chromosomes are split randomly determined crossover point. Subsequently, a new child is created by appending the first part of the first parent with the second part of the second parent;
- **two-point crossover** - two crossover points are chosen, and the content between these points is exchanged between two mated parents;
- **k-point crossover** - more than two crossover points are chosen, and the contents between tuples of the neighbor points are exchanged;
- **arithmetical crossover** - arithmetic creates children with a weighted arithmetic mean of two parents. Children are feasible concerning the linear constraints and bounds.

Encryption algorithms selected for the initial population differ from the simplest ones in execution. Every one of them uses multiple different atomic operations. This is why we assume we cannot use simple single-point crossover or two-point crossover. In contrast, k-point crossover and arithmetical crossover are appropriate candidates. However, there is still a question about appropriately choosing crossover points. This question still needs to be solved.

The last operation in the genetic algorithm is **mutation**. According to the description, this operation randomly flips chromosomes. If we let perform this operation entirely at random, its result can be unusable. One possible solution is not to choose randomly from all chromosomes but only from the concrete, which fits the solution. The second is to limit the randomness using any formula or conditions. If the result does not fulfill them, the operation of mutation has to be performed again.

The result of the mutation is the new generation. This is input to the evaluation of the fitness score, and the whole process is executed again. In assessing the fitness score, whether the new generation of algorithms achieves better results is checked. However, we mentioned totally eight different parameters in total. We must consider that improving one parameter can cause the deterioration of another. These parameters must be logically arranged based on their importance for the final solution. This approach allows us to create several generations of new encryption algorithms that have assigned the fitness

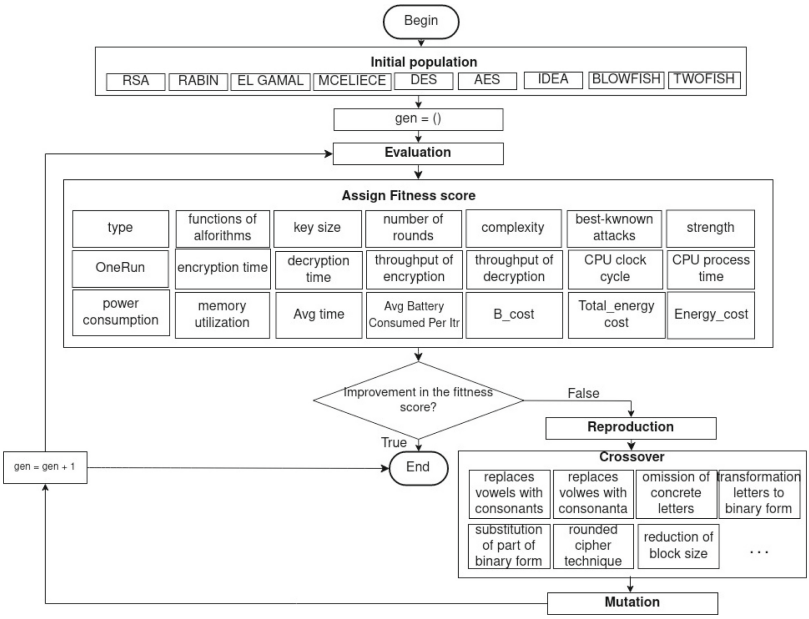

Fig.2. Flowchart of genetic algorithm

score. Ultimately, we have to select the generation with the best result of the fitness score from the set of all generations. The whole process can be described by the diagram, which was created by modification of the diagram in Fig. 2.

5 Future Work

The article presented a new approach to the construction of new encryption algorithms. This approach is based on knowledge of encryption algorithms, described in Chapter 2, with the combination of the theory of genetic algorithms described in Chapter 3. The result of this combination is described in Chapter 4, where there is also a Flowchart diagram of our design. Our work is actually in the design stage. We plan to evaluate metrics for all the most used encryption algorithms mentioned in Chapter 4. The metrics will be recorded in the database. This evaluation will serve as the initial state. After that, we plan to apply the approach and get a new set of encryption algorithms. We get the new set of encryption algorithms if all the processes terminate. After that, we will evaluate the fitness score for all algorithms from the new collection. If we observe the improvement of the properties mentioned in Chapter 4 in any algorithm from the set, this algorithm will be intended as the output of our crossover algorithm. If all processes terminate successfully, the result will be the set of new encryption algorithms. These new encryption algorithms will be faster, request less memory space, and, most importantly, be more secure.

6 Conclusion

The article presented our new approach to the creation of new encryption algorithms. As the foundation of our strategy, we choose a crossover technique applied to encryption algorithms. This technique is a widely popular search and optimization method for resolving highly intricate problems. Our work is in the state of design. We have implemented some modules (*the module for computation of the fitness score* and *the module for crossover*). We plan to test this module soon. After that, we have to design and implement next modules. New developed modules will also have to pass the series of the tests. Of course, after implementing of all modules, the system has to be also tested. The final tests will consist of tests on the correctness of new algorithms and tests of improving the fitness score of newly created algorithms. If the tests are successful, the result will be a new set of encryption algorithms that will be better than the algorithms used nowadays.

References

1. Bohen, D., Shoup, V.: A Graduate Course in Applied Cryptography. Draft . 2 (2015)
2. Vokorokos, L., Balaˇz, A., Madoˇs, B.: Application Security through Sandbox Virtualization, p. 1, (2009)
3. John Singh, K., Manimegalai, R.: Evolution of Encryption Techniques and DataSecurity Mechanisms. World Appl. Sci. J. **33**(10) 1597−1613 (2015)
4. Vokorokos, L., Pekarár, A., Adám, N., Daránvi, P.: Yet Another Attempt in UserAuthentication. Acta Polytech. Hung. **10**(3), 37−50 (2013)
5. Kent Webb, G.: Predicting processor performance. Issues Inf. Syst. **5**(1), 340 (2004)
6. Heng, W., Changqing, D., Xingyi, L., Chenxu, S., Jiaming, Z.: Research on anodepressure control and dynamic performance of automotive fuel cell system (2023)
7. Marella, S.T., Parisa, H.S.K.: Introduction to Quantum Computing. pp.1, (2020) 8. Ugwuishiwu, C., H., Ujah, J., Egi, A.E.: An Overview on Quantum Computing: The Next Generation in Computing Technology (2019)
8. Muller, I., van Heesch, M.: Migration to quantum-safe cryptography: about making decisions on when, what and how to migrate to a quantum-safe situation (2020)
9. Dorostkar, Z.: Mathematics for Cryptography: A Guide to Mathematical Fundamentals of Different Classes of Cryptography Algorithms (2023)
10. Signorelli, C.M.: Can Computers Become Conscious and Overcome Humans?. Frontiers Robot. AI **5**, 306019 (2018)
11. Vokorokos, L., Pekár, A., Fecil'ak, P.: IPFIX Mediation Framework of the SLAmeter Tool. In: 2013 IEEE 11th International Conference on Emerging eLearning Technologies and Applications (ICETA), pp. 311−314 (2013)
12. Purnama, B., Rohayani, H.: A New Modified Cesar Cipher Cryptography MethodWith Legible Ciphertext From a Message To Be Encrypted (2015)
13. Mohammed, M., S.: Novel Method Using Crossover (Genetic algorithms) WithMatrix Technique To Modifying by Using Playfair (2013)
14. Mahata, S.K., Dey, M.: A Novel Approach for Cryptography using Modified Substitution Cipher and Triangulation (2016)
15. Keshav, R., Bharti, S., Neeraj, K., Daveer, K.: Differential Cryptanalysis on SDES (2012)
16. Nivetha, A., Preethy Mary, S., Santosh, K.: Modified RSA Encryption Algorithmsusing Four Keys (2015)

17. Hayder, R., H.: H-RABIN CRYPTOSYSTEM (2014)
18. Emmerich, M., Shir, O.,M., Wang, H.: Evoluation strategies (2015)
19. Abdesiam, A., EI Boanani, F., Benazza, H.: Four Parallel Decoding Schemes of Product Block Codes (2014)
20. Matta, P., Arora, M., Sharma, D.: A comparative survey on data encryption Techniques: Big data perspective (2021)
21. Jorsrad, N.D.: Cryptographic algorithm metrics (1997)
22. Bharathi, B., Manivasagam, G., Kumar, A.: Metrics for performance evaluation ofencryption algorithms (2017)
23. Kaya, Y., Uyar, M., Tekin, R.: A Novel Crossover Operator for Genetic Algorithms: Ring Crossover (2011)