ICORIS2022

The 4th International Conference on Cybernetics and Intelligent System

Kampus Merdeka

UNIVERSITAS POTENSI UTAMA

04th Conference ON ICORIS

INTERNATIONAL CONFERENCE

08-09 OCTOBER 2022

VENUE: HOTEL KHAS PARAPAT, LAKE TOBA
NORTH SUMATERA - INDONESIA

HOST

CO-HOST

SUPPORTED BY

2022 4th International Conference on Cybernetics and Intelligent System (ICORIS) | 978-1-6654-5395-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICORIS56080.2022.10031444

2022 Fourth International Conference on Cybernetics and Intelligent Systems (ICORIS)

Medan, Indonesia

(Hybrid Conference)

October 08th-09th, 2022

Part Number: CFP22BWC-ART
ISBN: 978-1-6654-5395-0

2022 4th International Conference on Cybernetics and Intelligent System (ICORIS) | 978-1-6654-5395-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICORIS56080.2022.10031589

2022 Fourth International Conference on Cybernetics and Intelligent Systems (ICORIS)

Medan, Indonesia (Virtual)

Phone: +6281263411368

Email: icoris2022@potensi-utama.ac.id

Website: http://icoris.org/

October 08th-09th, 2022

Part Number: CFP22BWC-ART
ISBN: 978-1-6654-5395-0

2022 Fourth International Conference on Cybernetics and Intelligent Systems (ICORIS)

ISBN: 978-1-6654-5395-0

Additional copies of this publication are available from

Curran Associates, Inc.

57 Morehouse Lane

Red Hook, NY 12571 USA

+1 845 758 0400

+1 845 758 2633 (FAX)

PREFACE

Assalaamu ‘alaykum warahmatullahi wabarakaatuh,

After three successful sessions of ICORIS’s conference, we are proud to present the fourth edition of ICORIS. We believe that ICORIS 2022 is an excellent and exceptional opportunity which enables researchers to present and discuss the latest innovations, results and developments in their research topics. This years’ theme is "Build a trusted infrastructure system with blockchain technologies for society 5.0". The conference is expected to strengthen collaboration and provide a forum for academicians, professionals and researchers to discuss and exchange their research results, innovative ideas, and experiences to advance the field of Information Technology, Information Systems and Electronic Engineering in the modern world. The event will incorporate extensive discussions and consist of additional workshops, guest speaker sessions, and scintillating social events that will help our future leaders develop networks and transform their ideas into actions.

The ICORIS 2022 is in the general area of communication and information technology. It provides a forum for presenting and discussing the latest innovations, results, and developments in IT Management & organizations, IT Applications, Cyber & IT Security, and ICT. We present several tracks that are separated into nine thematic areas, each ICORIS 2022 track is a carefully curated selection of sessions and activities focused on an important current or emerging issue. There is 282 papers submission and only 106 papers are accepted to be presented in this Conference. The accepted papers will be presented in one of the regular sessions and will be published in the conference proceedings volume. All accepted papers are submitted to IEEEXplore. IEEE Conference Number: #56380.

On behalf of the ICORIS 2022 committee, we wish to extend our warm welcome and would like to thank all Keynote Speakers, Reviewers, Authors, and Committees, for their effort, guidance, contribution and valuable support.

Wa billahi taufiq wal hidaayah.

Wallahul muwaffiq ila aqwamit-tharieq.

Wasalaamu ‘alaykum warahmatullahi wabarakaatuh.

Husni Teja Sukmana, Ph.D

2022 4th International Conference on Cybernetics and Intelligent System (ICORIS) | 978-1-6654-5395-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICORIS56080.2022.10031587

THE COMMITTEE OF ICORIS 2022

STEERING COMMITTEE

1. Dr. Y. Johny W. Soetikno, SE.,MM. (Universitas Dipa Makassar, Indonesia)
2. Marthen Sengkey, PhD (Universitas Klabat)
3. Dr. Dadang Hermawan (ITB STIKOM Bali)
4. Dr. Ir. Djoko Soetarno, D.E.A (Binus University)
5. Prof. Dr. M. Suyanto, MM. (AMIKOM Yogyakarta)
6. Prof. Dr. Ir. Harjanto Prabowo, M.M. (Rektor Universitas Bina Nusantara)
7. Prof. Dr. Ir. Edi Noersasongko, M.Kom (Universitas Dian Nuswantoro Semarang)
8. Dr. Sandy Kosasi, MM., M.Kom. (STMIK Pontianak)
9. Dr. Rika Rosnelly, S.Kom., M.Kom. (Universitas Potensi Utama)
10. Restu Adi wiyono, M.Sc., M.Kom. (STMIK Tasikmalaya)
11. Dr. Po Abas Sunarya, M.Si. (STMIK Raharja)
12. Dr Berlilana , M.Kom (Univ Amikom Purwokerto, Indonesia)
13. Dr Anthony Anggrawan, M.T., PhD (Univ Bumigora Mataram, Indonesia)
14. Mus Aidah, S.Pd., MM. (STMIK Adhi Guna Palu)
15. Djuniharto, S.Kom., M.Kom(stmik PGRI, banyuwangi, Indonesia)
16. Dr. Hj. Rosiyati Mh Thamrin, SE., MM. (STMIK Sepuluh Nopember Jayapura)
17. M Hari Purwidiantoro, S.Kom., M.Kom(STMIK AMIKOM Surakarta, Indonesia)
18. Muchammad Naseer, M.Kom (STT Bandung, Indonesia)
19. Benedictus Effendy, ST., MT (STMIK Palcomtec Palembang, Indonesia)
20. Dr. Hadi Santoso, S.Kom., M.Kom.(Institut Sains dan Bisnis ATMALUHUR, INdonesia)
21. Suardi B Haruna, S.Si.,M.Si (STMIK PROFESIONAL, Makasar, Indonesia)
22. Bob Subhan Riza, S.T, M.Kom (Universitas Potensi Utama, Medan, Indonesia)

PROGRAM COMMITTEE

1. Prof. Riyanarto Sarno, Ph.D. (Institut Teknologi Sepuluh Nopember (ITS)), Indonesia
2. Prof. Pitoyo Hartono (Chukyo University, Toyota), Japan
3. Prof. Harold Boley (Faculty of Computer Science, University of New Brunswick, NB), Canada
4. Prof. Eko Sediyono, PhD (Universitas Satya Wacana, Indonesia)
5. Prof. Agus Buono (IPB University, Indonesia)
6. Prof. Joko Lianto Buliali, Msc, Phd (Institut Teknologi Sepuluh Nopember(ITS)), Indonesia
7. Prof. Ir. Arif Djunaidy M.Sc., Ph.D. (Institut Teknologi Sepuluh Nopember (ITS)), Indonesia
8. Prof. Dr.rer.nat. Achmad Benny Mutiara, Q.N, Ssi, Skom (Universitas Gunadarma), Indonesia

2022 4th International Conference on Cybernetics and Intelligent System (ICORIS) | 978-1-6654-5395-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICORIS56080.2022.10031353

9. Prof. Sri Hartati, M.Sc., Ph.D. (IndoCEIS/UGM)
10. Prof. Dr. Muhammad Zarlis (Universitas Sumatera Utara), Indonesia.
11. Prof. Dr Eri Prasetyo Wibowo, SSi, MMSI (Universitas Gunadarma), Indonesia
12. Rafał Dreżewski, Ph.D. (AGH University of Science and Technology), Poland
13. Assoc. Prof. Huynh Thi Thanh Binh (Hanoi University of Science and Technology (HUST)), Viet Nam
14. Prof. Dr. Mustafa Bin Mat Deris (Universiti Tun Hussein Onn Malaysia (UTHM)), Malaysia
15. Assoc. Prof. Somnuk Phon-Amnuaisuk (Universiti Teknologi Brunei), Brunei Darussalam
16. Amil Ahmad Ilham, ST.,MIT, PhD(Universitas Hasanuddin), Indonesia
17. Daniel Oranova, S.Kom., M.Sc.PD.Eng. (Institut Teknologi Sepuluh Nopember (ITS)), Indonesia
18. Arief Setyanto, S.Si., M.T., Ph.D. (AMIKOM Yogyakarta), Indonesia
19. Dr. Ir. Untung Rahardja, M.T.I.,MM. (Universitas Raharja), Indonesia
20. Andrew Tanny Liem, PhD (Universitas Klabat), Indonesia
21. Husni Teja Sukmana, PhD (Universitas Islam Negeri Syarif Hidayatullah), Indonesia
22. Dr Evi Triandini (ITB Stikom Bali, Indonesia)
23. Dr Kusrini (Univ Amikom Yogyakarta, Indonesia)

Technical Program Committee (TPC)

Chair : Husni Teja Sukmana, Ph.D (UIN Syarif Hidayatullah Jakarta, Indonesia)

C0-Chair : Prof. Dr. Teddy Surya Gunawan (Universitas Potensi Utama, Indonesia)

Organizing Committee

1. Program Chair : Husni Teja Sukmana, PhD. (IEEE Member : 93016632)
2. Co Program Chair : Helmi Kurniawan, M.Kom
3. Publication Chair : Prof. Dr. Teddy Surya Gunawan (IEEE Member : 8286407700)
4. Secretary : Ratih Puspasari, M.kom
5. Treasurer : Linda Wahyuni M.Kom

Editing Team

Husni Teja Sukmana, Ph.D

Edy Victor Haryanto, M.Kom

M. Sadikin, M.Kom

Fujiati, M.Kom

Alfa Saleh, M.Kom

Khairani Puspita, M.Kom

TABLE CONTENT

2022 4th International Conference on Cybernetics and Intelligent System (ICORIS) | 978-1-6654-5395-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICORIS56080.2022.10031582

Optimization of Student Database Confidentiality Using Elgamal Algorithm and Fermat Method

Rubianto
Faculty of Engineering and Computer Science
Universitas Potensi Utama
Medan, Indonesia
rubiantoditpi@gmail.com

Roslina
Faculty of Engineering and Computer Science
Universitas Potensi Utama
Medan, Indonesia
roslinanich@gmail.com

Rika Rosnelly
Faculty of Engineering and Computer Science
Universitas Potensi Utama
Medan, Indonesia
rikarosnelly@gmail.com

2022 4th International Conference on Cybernetics and Intelligent System (ICORIS) | 978-1-6654-5395-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICORIS56080.2022.10031570

***Abstract*— Every Islamic boarding school institution must have many databases, one of which is the student database. Securing the student database is needed to protect student data and information from database theft. To create an optimal system in securing the student database with the aim of avoiding accessing and processing data and information by unauthorized persons, the student database processed in this study used the ElGamal algorithm and the Fermat method with key formation using prime numbers and solving the problem requires discrete logarithm calculations. The keys used by this algorithm are the public key and the private key. The result of testing this method is that the student database is encrypted. The algorithm used to generate these prime numbers is to use Fermat. The ElGamal algorithm is very helpful in securing the student database at the Darul Hikmah Islamic Boarding School TPI Medan. In testing the encryption of the student database file with the file name "santri.mdf" it was successfully converted into a file with the new name "santri_mdf.encrypt", and in the decryption process it could return to plaintext with the name "santri.mdf".**

Keywords*— *student database, Elgamal algorithm, Fermat method

I. INTRODUCTION

Computer system security is becoming increasingly important along with the development of computerized business processes. A computerized business process is a business process that most of its activities use computer technology and make computers as a storage medium for important data so that it can be said that computer media is an important factor in running business processes. Computer system security that is in the spotlight is not only the computer equipment, but also the security for the network, software or application programs and also database security [1].

Data processing is a routine thing in educational institutions, especially in Darul Hikmah Islamic Boarding School TPI Medan. For example, in teaching activities and evaluating the report of student learning outcomes at the end of each semester. This evaluation will be vulnerable if the work process carried out is still using the old system. The system still uses a simple method, namely handwriting and data processing using a computer system that relies on Microsoft Excel.

The security and confidentiality of the data stored in the database is one of the important aspects of an information system, as the data is safe from information leakage. Security of computer networks connected to databases no longer guarantees data security because data leaks can be caused by insiders or parties directly related to databases such as database administrators [2].

Database security can be done in various ways, starting from limiting user access rights to the database itself, using field names that are only understood by administrators so that not all employees who are given permission to access the database understand the existing database flows to avoid data theft, data destruction and so on [3]. So on, to the implementation of cryptographic algorithms by administrators on records in the database with the aim of making stored records more secret and difficult to read by other parties.

One mechanism to improve the security of data in the database is to use encryption technology. The data stored in the database is modified in such a way that it is not easy to read. So encryption is a process that is carried out to secure data (called plaintext) into hidden data (called cipher text). Cipher text is data that can no longer be read easily [4].

Elgamal's security is based on discrete logarithm problems to encrypt and decrypt messages separately. An intruder trying to decrypt a disconnected message can try to recover the private key [6]. For this purpose logarithms need to be calculated. There is no actual method for this, given that certain needs in the initial group are met.

Generating prime numbers is an essential problem in computer science and number theory, especially in the field of cryptography. This is because public key encryption protocols are based on the use of large prime numbers. While the security of public key cryptography systems is often based on the difficulty of getting the prime factors of a very large prime number. Although the algorithm to determine the primacy of a number that has been found is still relatively slow for the current problem, a probabilistic algorithm can be formed using the Fermat method [7].

Prime numbers are widely used by the field of cryptography. Even so, there is no exact algorithm that can determine the primacy of a number efficiently. By using Fermat's Theorem, an alternative can be done, namely creating a probabilistic algorithm to determine the prime value of a number [7].

Due to this probabilistic nature, the result of this algorithm is not exact but is probabilistic. However, the possibility of this algorithm producing errors can be minimized by using some calculations. In the computer world, several ways have been found to find these prime numbers, one of which is by using the Fermat method to find these prime numbers.

II. RELATED WORK

In a study conducted by Haval I. Hussein & Wafaa M. Abduallah proposed to overcome the existing weaknesses. Modifications are made to reduce the size of the cipher text

and speed up execution time. This is done by using additional operations instead of looping in the encryption process. Based on the experimental results, the proposed scheme reduces the expansion rate by 89%. As well as speed up execution time which makes the proposed scheme performs better. So, the goal of increasing the efficiency of the ElGamal Cryptosystem is significantly increased. The security of the proposed scheme is not affected in the same way as the existing security is based on the difficulty of solving discrete logarithm problems [8].

Another research conducted by Demba Sow & Mamadou Ghouraissiou Camara resulted in a new variant of ElGamal signature scheme called "General ElGamal signature scheme" proposed in 2011. The General ElGamal signature scheme is a modified ElGamal signature scheme. In this study, a proof of security of the Generalized ElGamal signature scheme is proposed in a random oracle model. Some security signature scheme ideas and demonstrate the security of modified ElGamal Signature scheme. We have succeeded in proving the existential exogism of the Generalized ElGamal signature scheme, adaptively to selected message attacks, in a random oracle model [9].

Research conducted by Djebaili Karima & Melkemi Lamine proposed a secure version of the Elgamal public key cryptosystem, and proved that it is semantically secure assuming what we call the two-dimensional Diffie-Hellman decision problem (2DDDH), this cryptosystem is distinguished by the speed of the encryption process and decryption and by its resistance to active enemies [10]. Since the 2DDDH problem is more difficult than the decisional Diffie-Hellman (DDH) problem (as will be seen), we can conclude that the model strengthens the security of the exchange compared to existing cryptosystems in the same context, also we discuss the difficulty of the problem that ensures its security. In this study, a new computational problem called the Diffie-Hellman (2DDDH) two-dimensional decision problem [11]. This extension can be used in many cryptographic constructs based on DL problems. In addition, the 2DDDH problem is more difficult than the regular DDH problem that some logarithmic problem-based schemas rely on. Our new paradigm has many applications. As one such application, we present a new variant of ElGamal encryption with very simple proof of security [11].

Research conducted by Gupta et al presents a cryptosystem derived from the quantum version of diffie-hellman as described previously, but it may be seen as an improvement because the Elgamal Cryptosystem can be used to sign messages or encryption in one direction without direct interaction between the parties. The protocol for exchanging qubit sequence pairs between two parties via a quantum channel and using a computational base as a parameter for the commutative quantum rotation transformation to decrypt the message. Quantum postal cryptography is the latest field of research to emerge after the introduction of the Short algorithm. Classic cryptosystems like RSA, Diffie-Hellman and ElGamal will be completely obsolete with quantum computers [12].

Research also conducted by E. Jincharadze explained that cryptography is the science or study of secret writing techniques, especially code and cipher systems, methods, and the like. Cryptography must ensure a high level of security in transferring and storing data. There are two types of cryptographic algorithms such as symmetric key cryptography and asymmetric key cryptography [13]. Currently there are various types of cryptographic algorithms that provide high information security, but they also have some drawbacks. To improve the weakness of this algorithm, in this paper we propose a new hybrid cryptographic algorithm model. This algorithm is designed using a combination of two cryptographic algorithms AES and Elgamal. An analysis and comparison of the performance of the proposed algorithm has been carried out by following the parameters of encryption time, decryption time and system requirements [14]. For this cryptographic algorithm, a program is made in Java in the NetBeans IDE. Implementation and analysis of the performance of the proposed model is carried out by Java. The final result shows that the hybrid model has better performance than the AES and Elgamal systems [15].

Another research conducted by Yuling Luo, et al resulted in research on security issues regarding key management and distribution for symmetric image encryption schemes, a new asymmetric image encryption method is proposed in this paper, which is based on ElGamal elliptic curve (EC-ElGamal) cryptography and chaotic theory. In particular, the SHA-512 hash was first adopted to generate the initial values of the chaotic system, and the cross permutations in terms of the order of the chaotic indexes were used to randomize the ordinary images [16]. Furthermore, the generated random image is embedded into an elliptic curve to be encrypted by EC-ElGamal which can not only improve security but can also help solve key management problems. Finally, a game of diffusion-combined chaos with DNA sequences is played to get the cipher image. Experimental analysis and performance comparison show that the proposed method has high security, good efficiency, and strong resistance to selected plain text attacks which makes it have potential applications for secure image communication [17].

Other research on Elgamal encryption was also carried out by Motilal Singh Khoirom, et al. Encrypting using Elgamal public key encryption in a limited field requires the insertion of messages represented by integers. This integer must be implanted to a coordinate location that satisfies the equation of the elliptic curve using the Koblitz embedding technique [18]. Thus, data expansion occurs because every integer must be represented as a coordinate. The recommended elliptic curve has a large modulo prime, so for any small integer representation of a message, the expansion in the cipher text is very large. The above factors hinder the use of the ElGamal method for encryption of large data sizes. In the ameliorated version, any coordinate in the elliptic curve equation can be used to perform encryption operations [19]. The typical Koblitz embedding technique to certain coordinates that satisfy the elliptic curve equation can be avoided. Data expansion issues are addressed by using basic conversion operations with some audio data. The simulation results and performance comparison with other public key cryptosystems indicate that the proposed method is suitable for audio encryption operations [20].

III. RESEARCH METHODOLOGY

The research methodology will greatly assist the author in the problem solving work process. This research has several stages in carrying out the activities contained in the sequence of research activities, namely identifying problems, analyzing problems, determining goals, studying literature,

collecting data, designing systems, implementing the Elgamal algorithm and the Fermat method on database security, testing and drawing conclusions.

The following will describe the methodology and sequence of research activities used in the completion of this research. The sequence of these activities is the stages that will be carried out in order to solve the problems that will be discussed. The sequence of activities from this research can be seen in Figure 1.

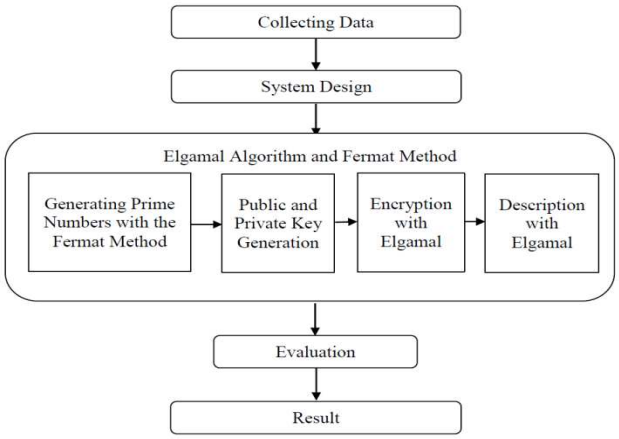

Fig. 1. Research Methodology

Based on Figure 1, the following is a description of the following sequences of research activities:

1. Collecting data, done by requesting data from the student admin about the student database at the TPI Medan Islamic Boarding School, taking data from books and journals about database security. This data will be used as a reference in making the student database security application.
2. Designing the system, at this stage the data collected is then designed into a system that will be processed and implemented with predetermined methods. The design of the system is to change the raw data that has been obtained into data that is ready to be processed so that it is expected that the results of the processing can be as expected.
3. Implementing the Elgamal and Fermat Algorithms, the data obtained are then analyzed and implemented to produce useful information. At this stage, data processing is carried out to secure the student database at the TPI Medan Islamic Boarding School. In accordance with data processing, at the implementation stage, testing of the application of the Elgamal algorithm is carried out to secure the database of the designed application.
4. Evaluation, at this stage, the results of data analysis that have been processed previously will be tested using the specified application. Testing the Elgamal Algorithm can be done by trying the encryption and decryption process of the student database at the TPI Medan Islamic Boarding School. At the system testing stage, two methods are used, namely functionality testing and validity testing. The functionality test is carried out by black box testing while the validity test is carried out by testing the similarity of the calculation results of the program code and manual calculations. The approach taken by writing in testing the system made is Black Box Testing where this test aims to show the software functions on how to operate, whether the encryption and decryption processes are running correctly and the application can be used by users.
5. Results, after being tested, at this stage the database security cryptography application passes the testing stage and the results are ready to be used by Windows users. It is possible that this system will experience changes when it is used by users. Changes can occur due to errors that appear and are not detected during testing. The support or maintenance phase can repeat the development process starting from specification analysis for changes to existing information systems, but not to create new information systems.

IV. ANALYSIS AND RESULT

The steps in the general stage of analysis will be almost the same as those in the steps that will be taken in defining the system plan. In the analysis phase, the scope of the task is more detailed. In this system analysis, the research that will be carried out by systems analysis is a detailed study, while in system planning it is only a preliminary study.

The first step is to do a system analysis. System analysis aims to gain knowledge related to the confidentiality of the SQL Server database using the Elgamal algorithm and the Fermat method. This application is used to convert the original text contained in the SQL Server database into secret text so that it cannot be read by the authorities.

The problem of database security and confidentiality is one of the important aspects of an information system. Information is only intended for certain parties, it is related to how the information cannot be accessed by unauthorized people. File security in the database can be done by using several asymmetric algorithms that can lock database files, including the Elgamal algorithm and the Fermat method.

In this case, there are still many people who do not understand how to access or secure database files so that the data contained in them cannot be seen by others. This is due to the difficulty of computer security procedures when using the facilities provided by each operating system. For that, we need an application that can easily and quickly lock and secure the user's computer by using the password entered into it.

Therefore we need a database security system that aims to improve data security, protect data or messages from being read by unauthorized parties, and prevent unauthorized parties from inserting, deleting, or changing data.

The problem-solving stage is carried out starting from the process of analyzing, designing, evaluating and improving the system according to needs, so that the system that is being made can be used optimally. This study uses the Elgamal algorithm and the Fermat method for cryptographic techniques as a way to secure the student database at the Darul Hikmah Islamic Boarding School TPI Medan.

This research resulted in an Elgamal encryption and decryption application program which was built using visual basic. The resulting application is used to encrypt the database files. The results of the research carried out are changing the original database file into an encrypted database file where the contents of the database file cannot be read, returning the unreadable database file to the original

database file with the Elgamal method without destroying and changing the contents of the database file, and changing the file. The original database as the plaintext change into cipher text, which will be unreadable codes.

The following is the application of the Elgamal algorithm and examples of manual calculations on securing student data at the Darul Hikmah Islamic Boarding School TPI Medan:

1. Encryption Process

   Suppose A generates a key pair by choosing a random prime number as the key used is p = 97, g = 7 and x = 2.

   Then p, g, x are used to calculate y.

   So, y = gx mod p = 72 mod 97 = 49.

   So A's public key is: y = 49, g = 7, p = 97 and A's private key is: x = 2, p = 97. Convert characters into ASCII numbers denoted by m. Determine the value of k, in this case k = 2.

   Suppose B wants to send plaintext "ABDUL MEIZAR" to A, then each character of the plaintext is converted into ASCII form denoted by m, resulting in the following:

   m = ABDUL MEIZAR

   ASCII plaintext

   A = 65

   B = 66

   D = 68

   U = 85

   L = 76

   space = 32

   M = 77

   E = 69

   I = 73

   Z = 90

   A = 65

   R = 82

   Then the ASCII values are entered into blocks of m values sequentially.

   For the plaintext block (m1), namely the character "A", change the character "A" to an ASCII value of 65. Then do the encryption process, in this process the values a and b will be obtained as cipher text obtained by the formula: $a = g^k \bmod p$ and $b = y^k m \bmod p$. For more details see the following calculations.

   Character A = 65 as the value of m1.

   Then, we get the cipher text (a, b):

   $a = g^k \bmod p = 72 \bmod 97 = 49$

   $b = y^k m \bmod p = (492 \times 65) \bmod 97 = 89$

   From the above calculation results obtained cipher text of the letter A is block C1 = (49.89).

   Character B = 66 as the value of m2.

   Then, we get the cipher text (a, b):

   $a = g^k \bmod p = 72 \bmod 97 = 49$

   $b = y^k m \bmod p = (492 \times 66) \bmod 97 = 65$

   From the above calculation results obtained cipher text of the letter B is block C2 = (49.65).

   Character D = 68 as the value of m3.

   Then, we get the cipher text (a, b):

   $a = g^k \bmod p = 72 \bmod 97 = 49$

   $b = y^k m \bmod p = (492 \times 68) \bmod 97 = 17$

   From the results of the above calculation, it is obtained that the cipher text of the letter D is block C3 = (49,17).

   Character U = 85 as the value of m4.

   Then, we get the cipher text (a, b):

   $a = g^k \bmod p = 72 \bmod 97 = 49$

   $b = y^k m \bmod p = (492 \times 85) \bmod 97 = 94$

   From the results of the above calculation, it is obtained that the cipher text of the letter U is block C4 = (49.94).

   Character L = 76 as the value of m5.

   Then, we get the cipher text (a, b):

   $a = g^k \bmod p = 72 \bmod 97 = 49$

   $b = y^k m \bmod p = (492 \times 76) \bmod 97 = 19$

   From the results of the above calculation, it is obtained that the cipher text of the letter L is block C5 = (49,19).

   Space character = 32 as the value of m6.

   Then, we get the cipher text (a, b):

   $a = g^k \bmod p = 72 \bmod 97 = 49$

   $b = y^k m \bmod p = (492 \times 32) \bmod 97 = 8$

   From the calculation results above, the cipher text of spaced letters is block C6 = (49,8).

   The character M = 77 as the value of m7.

   Then, we get the cipher text (a, b):

   $a = g^k \bmod p = 72 \bmod 97 = 49$

   $b = y^k m \bmod p = (492 \times 77) \bmod 97 = 92$

   From the above calculation results, the cipher text of the letter M is block C7 = (49.92).

   Character E = 69 as the value of m8.

   Then, we get the cipher text (a, b):

   $a = g^k \bmod p = 72 \bmod 97 = 49$

   $b = y^k m \bmod p = (492 \times 69) \bmod 97 = 92$

   From the above calculation results obtained cipher text of the letter E is block C8 = (49,90).

   Character I = 73 as the value of m9.

   Then, we get the cipher text (a, b):

   $a = g^k \bmod p = 72 \bmod 97 = 49$

   $b = y^k m \bmod p = (492 \times 73) \bmod 97 = 91$

From the above calculation results, the cipher text of the letter E is block C9 = (49,91).

Character Z = 90 as the value of m10.

Then, we get the cipher text (a, b):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 90) \bmod 97 = 92$

From the results of the above calculation, it is obtained that the cipher text of the letter E is block C10 = (49.71).

Character A = 65 as the value of m11.

Then, we get the cipher text (a, b):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 65) \bmod 97 = 89$

From the results of the above calculation, it is obtained that the cipher text of the letter E is block C11 = (49.89).

The character R = 82 as the value of m12.

Then, we get the cipher text (a, b):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 82) \bmod 97 = 69$

From the results of the above calculation, it is obtained that the cipher text of the letter E is block C12 = (49.69).

After getting the values of a and b, the calculation results are arranged in the following pattern: a1, b1, a2, b2, a3, b3, a4, b4, a5, b5, a6, b6, a7, b7, a8, b8, …a12, b12 . Then obtained:

Plaintext = ABDUL MEIZAR

Ciphertext=49,89,49,65,49,17,49,94,49,19,49,8,49,92,49,90,49,91,49,71,49,89,49,69.

2. Decryption Process

A decrypts the cipher text of B by doing calculations with the keys used are p = 97, g = 7 and x = 2. So, y = gx mod p = 72 mod 97 = 49. Determine the value of k, in this case k = 2.

Cipher text= 49,89,49,65,49,17,49,94,49,19,49,8,49,92,49,90,49,91,49,71,49,89,49,69.

For the cipher text block (C¬1) = a,b with values a = 49 and b = 89, the decryption process to produce plaintext is carried out by calculation using the formula a(p-1-x) mod p, then proceed with the calculation with the formula b* (a(p-1-x) mod p) mod p. Then the ASCII value will be obtained, change this value into the form of character values to get plaintext. For more details, see the following calculation.

Ciphertext1(a,b) = (49,89)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (89 \times 4) \bmod 97 = 65.$

Convert the ASCII number 65 to the character i.e. m1 = "A".

C2(a,b) = (49.65)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (65 \times 4) \bmod 97 = 66.$

Change the ASCII number 66 to the character i.e. m2 = "B".

C3(a,b) = (49,17)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (17 \times 4) \bmod 97 = 68.$

Convert the ASCII 68 number to the character i.e. m3 = "D".

C4(a,b) = (49.94)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (94 \times 4) \bmod 97 = 85.$

Convert the ASCII 85 number to the character i.e. m4 = "U".

C5(a,b) = (49,19)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (19 \times 4) \bmod 97 = 76.$

Convert the ASCII number 76 to the character i.e. m5 = "L".

C6(a,b) = (49,8)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (8 \times 4) \bmod 97 = 32.$

Convert the ASCII 32 number to the character i.e. m6 = "SPACE".

C7(a,b) = (49.92)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (92 \times 4) \bmod 77 = 76.$

Change the ASCII number 77 to the character i.e. m7 = "M".

C8(a,b) = (49,90)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (90 \times 4) \bmod 77 = 69.$

Change the ASCII number 69 to the character i.e. m8 = "E".

C9(a,b) = (49.91)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (91 \times 4) \bmod 77 = 73.$

Change the ASCII number 73 to the character i.e. m9 = "I".

C10(a,b) = (49.71)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

$b * (a^{(p-1-x)} \bmod p) \bmod p = (71 \times 4) \bmod 77 = 90.$

Convert the ASCII number 90 to the character i.e. m10 = "Z".

C12(a,b) = (49,89)

$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$

b * ($a^{(p-1-x)}$ mod p) mod p = (89 x 4) mod 77 = 65.

Convert the ASCII number 65 to the character i.e. m11 = "A".

C13(a,b) = (49.69)

$a^{(p-1-x)}$ mod p = $49^{(97-1-2)}$ mod 97 = 4

b * ($a^{(p-1-x)}$ mod p) mod p = (69 x 4) mod 77 = 82.

Change the ASCII number 82 to the character i.e. m12 = "R".

After getting the value of the results of the decryption process, the calculations are arranged in a pattern: m1, m2, m3, m4, m5, m6, m7, m8, m9, m10, m11, m12.

Then obtained:

Cipher text= 9,89,49,65,49,17,49,94,49,19,49,8,49,92,49,90,49,91,49,71,49,89,49,69.

plaintext = ABDUL MEIZAR

V. CONCLUSIONS

Based on the research and discussion conducted, the author can make the following conclusions that the stages of the research process regarding securing student databases at the Darul Hikmah Islamic Boarding School TPI Medan with an application designed using the Elgamal algorithm, it can be concluded that the Elgamal algorithm can be used to encrypt the contents and database files (cipher text) so that they cannot be read by data thieves, and can only be decrypted into the contents and the original database file (plaintext) if the password is entered correctly.

REFERENCES

[1]. V. Subbarao, K. Srinivas, and R. S. Pavithr, "A survey on internet of things based smart, digital green and intelligent campus," in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019, pp. 1–6.

[2]. A. Al-Harrasi, A. K. Shaikh, and A. Al-Badi, "Towards protecting organisations' data by preventing data theft by malicious insiders," *Int. J. Organ. Anal.*, 2021.

[3]. R. O. Obe and L. S. Hsu, *PostgreSQL: up and running: a practical guide to the advanced open source database*. " O'Reilly Media, Inc.," 2017.

[4]. E. S. I. Harba, "Secure data encryption through a combination of AES, RSA and HMAC," *Eng. Technol. Appl. Sci. Res.*, vol. 7, no. 4, pp. 1781–1785, 2017.

[5]. V. Edy, "Optimizing the Confidentiality of Lecturer Database using Elgamal Algorithm," 2020.

[6]. M. Al-Zubi and A. A. Abu-Shareha, "Efficient signcryption scheme based on El-Gamal and Schnorr," *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 11091–11104, 2019.

[7]. M. Kasianchuk, I. Yakymenko, S. Ivasiev, R. Shevchuk, and L. Tymoshenko, "The method of factorizing multi-digit numbers based on the operation of adding odd numbers," 2018.

[8]. H. I. Hussein and W. M. Abduallah, "An efficient ElGamal cryptosystem scheme," *Int. J. Comput. Appl.*, vol. 43, no. 10, pp. 1088–1094, 2021.

[9]. D. Sow and M. G. Camara, "Provable security of the generalized elgamal signature scheme," *J. Math. Res.*, vol. 11, no. 6, pp. 1–77, 2019.

[10]. A. Ali *et al.*, "Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography," *Sensors*, vol. 22, no. 2, p. 528, 2022.

[11]. D. Karima and M. Lamine, "Two dimensional ElGamal public key cryptosystem," *Inf. Secur. J. A Glob. Perspect.*, vol. 28, no. 4–5, pp. 120–126, 2019.

[12]. D. S. Gupta and G. P. Biswas, "Design of lattice-based ElGamal encryption and signature schemes using SIS problem," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 6, p. e3255, 2018.

[13]. P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing," in *Inventive Communication and Computational Technologies*, Springer, 2021, pp. 537–547.

[14]. S. Rani and H. Kaur, "Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal.," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 3, 2017.

[15]. E. Jincharadze, "Hybrid Encryption Model of Symmetric and Asymmetric Cryptography with AES and Elgamal Encryption Algorithms," *Sci. Pract. cyber Secur. J.*, pp. 2587–4667, 2018.

[16]. A. Sahasrabuddhe and D. S. Laiphrakpam, "Multiple images encryption based on 3D scrambling and hyper-chaotic system," *Inf. Sci. (Ny).*, vol. 550, pp. 252–267, 2021.

[17]. Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.

[18]. A. Abdaoui, A. Erbad, A. K. Al-Ali, A. Mohamed, and M. Guizani, "Fuzzy Elliptic Curve Cryptography for Authentication in Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9987–9998, 2021.

[19]. A. Banik, Z. Shamsi, and D. S. Laiphrakpam, "An encryption scheme for securing multiple medical images," *J. Inf. Secur. Appl.*, vol. 49, p. 102398, 2019.

[20]. M. S. Khoirom, D. S. Laiphrakpam, and T. Tuithung, "Audio encryption using ameliorated ElGamal public key encryption over finite field," *Wirel. Pers. Commun.*, vol. 117, no. 2, pp. 809–823, 2021.

[21]. L. Tanti, Safrizal, M. A. E. Nasution, R. Puspasari, B. S. Riza, and J. Indriani, "Modeling of Decision Support System as an Assistant Tool in Selecting Health Equipment Suppliers with TOPSIS Method," 2021, doi: 10.1109/CITSM52892.2021.9588818.

Kampus Merdeka
INDONESIA JAYA
UNIVERSITAS POTENSI UTAMA

CERTIFICATE
Of Appreciation

Proudly Presented To

Rubianto, Roslina, Rika Rosnelly

As an Author with The Title:

Optimization of Student Database Confidentiality Using Elgamal Algorithm and Fermat Method

The 4th International Conference on Cybernetics and Intelligent System (ICORIS)

ICORIS INTERNATIONAL CONFERENCE

8th & 9th 2022, Hotel Khas Parapat - North Sumatera

UNIVERSITAS POTENSI UTAMA - MEDAN - INDONESIA

HOST CO-HOST SUPPORTED BY

Dr. Rika Rosnelly, S.Kom., M. Kom
Rector of Universitas Potensi Utama

Dr. Ir. Djoko Soetarno, DEA
CORIS Advisor

Heimi Kurniawan, M. Kom.
ICORIS Chairman