EDY VICTOR

by Diperiksa Oleh Lppm Universitas Potensi Utama

Submission date: 02-Jun-2020 01:54PM (UTC+0700)
Submission ID: 1336379776
File name: asi_Kerahasiaan_Database_Dosen_Menggunakan_Algoritma_Elgamal.pdf (219.45K)
Word count: 4207
Character count: 22030

Optimizing the Confidentiality of Lecturer Database Using Elgamal Algorithm

Abstract

Each Higher Education Institution must have many databases, one of which is a database of lecturers who store the confidentiality of data and information from lecturers as instructors. Securing lecturer databases is needed to protect lecturer data and information from database theft. Creating an optimal system in securing lecturer databases to avoid individuals who have no right to access and process data and information. The lecturer database processed in this study uses the ElGamal algorithm with key formation using primes and solving the problem requires discrete logarithmic calculations. The keys used in this algorithm are public keys and private keys. The results of testing this method is the encrypted lecturer database. ElGamal's algorithm is very helpful in securing the lecturer database at the Universitas Potensi Utama.

Keywords: Database, Encryption, Algorithm, ElGamal, Decryption, Cryptography

1. Introduction

Utilization of computer applications in a company or organization today is a necessity. Almost in all fields of work using tools in the form of computer applications [1]. Computer system security is becoming increasingly important as the development of computerized business processes. Computerized business process is a business process that most of its activities use computer technology and make the computer as a medium for storing important data so that it can be said that computer media is an important factor in the business processes that are carried out. Computer system security is the focus not only of the computer device, but also the security of the network, software or application programs and database security [2].

Security and confidentiality of data stored in a database is one important aspect of an information system, such as the data is safe from information leakage [3]. 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 [4].

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 the administrator so that not all employees who are given permission to access the database understand the existing database flow to avoid data theft, data destruction and others et cetera, until the implementation of cryptographic algorithms by the administrator of the records in the database with the aim of making the stored records more confidential and difficult to read by others [5].

Sometimes the database is also stored in the Cloud Server, the information owner saves the information on a trusted server. Most people believe that the cloud is a dangerous place and once you save your information to the cloud, you lose complete control over it. The information owner cannot trust the cloud server to control secure access to information. In this way, the problem of safe access to information has turned into the most basic testing problem in storage distributed by the general public. So any ordinary security advances cannot be linked directly to him [6].

One mechanism to improve data security in databases is to use encryption technology [7]. The data stored in the database is modified so that it is not easy to read. So encryption is a process carried out to secure a data (called plaintext) into hidden data (called ciphertext). Ciphertext is data that cannot be read easily [8].

One method that can be used for database security is the Elgamal Algorithm. The Elgamal algorithm invented by Egyptian scientists [9], namely Taher Elgamal in 1985, is a public-key cryptographic algorithm. Elgamal algorithm process consists of three processes, namely the process of key formation, the encryption process, and the decryption process. Elgamal cryptography was initially used for digital signature requirements, but was later modified so that it could be used for security such as encryption and description [10]. Elgamal cryptography is used in security software developed by GNU, the PGP program, and in other security systems [11].

ElGamal security is based on a discrete logarithmic problem to encrypt and decrypt messages separately. An intruder who attempts to decrypt a disconnected message can try to recover the private key. For this purpose logarithms need to be calculated. There is no actual method for this, given the specific needs of the initial group are met [12].

The research aims to optimize the security of database processing that is used in the database security application of lecturers using the Elgamal algorithm at the Potential Main University.

2. Research Methodology

The research methodology will greatly assist the writer in the work process of solving problems. This study has several stages in the implementation of activities contained in the order of research activities, namely identifying problems, analyzing problems, determining goals, studying literature, collecting data, designing systems, implementing Elgamal algorithms on database security, testing and making conclusions.

2.1. Sequence of Research Activities

The sequence of activities is the stages that will be carried out in order to solve the problem that will be discussed. The sequence of activities from this study can be seen in Figure 1.

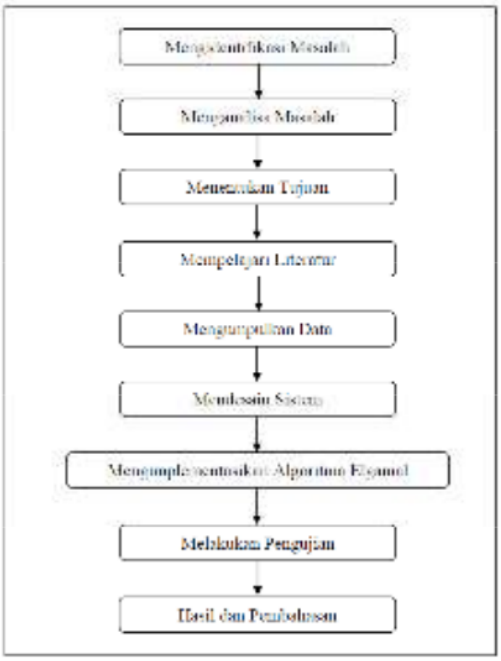

Figure 1. Sequence of Research Activities

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

a. Identifying Problems, the problem identified in this study was to optimize the safety of lecturer databases at the University of Potentials by applying the Elgamal algorithm to the process of encrypting and decrypting existing databases.

b. Analyzing Problems, the problems found will then be analyzed. The step in the problem analysis process is the step to understanding the problem that has been determined. By analyzing the problems that have been determined, it is hoped that the problem can be understood properly. Analysis of the problem in this study was carried out by applying the Elgamal algorithm for the encryption and decryption process into the lecturer database system so as to produce a more optimal lecturer database security.

c. Determine the Goals, based on an understanding of the problems that have been analyzed, the next step is to determine the objectives to be achieved in this study. In this goal the target to be achieved, especially those that can overcome existing problems, is to produce a database security application for lecturers at the Universitas Potensi Utama using the Elgamal algorithm.

d. Studying Literature, studying the literature that will be used as reference material in this research. The literature used is from scientific journals, learning modules and books on cryptography in particular relating to the application of the Elgamal algorithm. The literature will be a guideline for conducting research to assist and facilitate the research process.

e. Collecting Data, the method of data collection is done by requesting data from the lecturer admin about the lecturer database at Universitas Potensi Utama, taking data from books and journals about database security. From this data, it will be used as a reference in making lecturer database security applications.

f. 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 the expected results of the processing can be as expected.

g. Implementing Elgamal Algorithm, the data obtained, then analyzed and implemented in order to produce useful information. At this stage data processing is carried out to secure the lecturer database at the Potential Main University. In accordance with data processing, the implementation phase is tested by applying the Elgamal algorithm to secure the database of the designed application.

h. Conduct Testing, at this stage, the results of data analysis that has been previously processed will be tested using the specified application. Elgamal Algorithm Testing can be done by trying the encryption and decryption process of the lecturer database at the Universitas Potensi Utama. The approach taken by writing in testing the system made is Black Box Testing where this test aims to show the software's function of how it operates, whether the encryption and decrypt process runs correctly and the application can be used by the user.

i. Making Conclusions, after being tested, at this stage the database security cryptographic application passes the testing phase and is ready for use by Windows users. Do not rule out the possibility of this system experiencing changes when it has been used by users. Changes can occur due to errors that appear and are not detected during testing. The support or maintenance stage can repeat the development process starting from specification analysis to changes to existing

information systems, but not to creating new information systems.

2.2. Computer Security

The field of computer security is continuously experiencing extraordinary developments because information technology has an increasingly high influence on how we work, communicate, shop and enjoy entertainment [13]. Along with this development, the threats to our computer security are increasing, both physical and non-physical threats such as security holes in the operating system, attacks on networks, viruses, and others. In building an internet-based network system, security issues are absolutely necessary. A system built without a good security system is the same as inviting a thief to enter our house and let him take everything we have [14]. Often when building a system, we find various vulnerabilities in our system. But we consider it a small thing because we do not consider it a security hole (hole). We are not aware that these small vulnerabilities are used by people who are not responsible for carrying out their crimes [15].

2.3. Information System Security

One of the commonly used ways to secure information is to regulate access to information through an "access control" mechanism. Implementation of this mechanism, among others, by using "password" [16]. To further enhance the security of information systems, protection can be added. This protection can be in the form of filters (in general) and more specifically is a firewall. Filters can be used to filter e-mail, information, access, or even at the packet level. One mechanism for increasing security is to use encryption technology. The data that you send is modified so that it is not easily intercepted. Many services on the Internet still use "plain text" for authentication, such as using a pair of userid and password. This information can be seen easily by the tapping (sniffer) program [17].

Following the information system security methodology is described in the form of a security level pyramid [18]

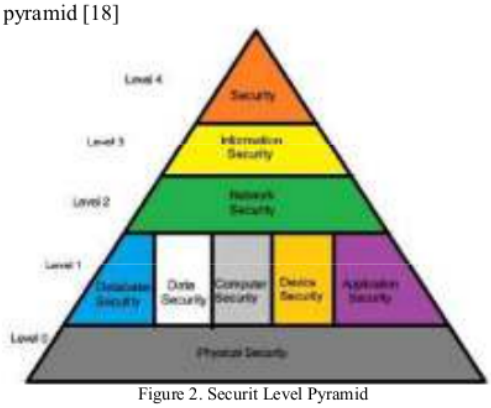

Figure 2. Securit Level Pyramid

There are 5 levels of Information Systems Security, namely [17]:

a. Security level 0: physical security, is the initial security of computer security. Physical security only focuses on physical features such as door locks, CCTVs, ID cards and so on. If physical security is not maintained properly, then data or even computer hardware cannot be secured.

b. Level 1 security: consists of database security, data security, computer security, device security, application security. Only people who have the authority can access all the security mentioned earlier. Examples such as the admin of a computer that stores various data and information.

c. Level 2 security: network security, computers connected to networks such as LAN, WAN or the internet are very vulnerable to security problems because computers can be accessed by client computers, therefore level 2 security must be designed so that network leaks do not occur, illegal access that can damage security of these data. Therefore, after finishing level 1 security, level 2 security is designed so that no unwanted things occur such as network leaks, illegal access, and other illegal actions.

d. Level 3 security: information security, security that is sometimes overlooked by the admin such as leaving a password on paper or giving a password to a friend, so eating can be a very fatal thing because it can be misused.

e. Security level 4: is security that covers the whole of the computer system. If level 1-3 has been executed properly, level 4 has been fulfilled. But it does not rule out the possibility that illegal things can occur such as an intruder or data destruction, etc.

2.4. Network Security

The network security model shown by a message will be exchanged starting from one point to another through the Internet administration network as shown in the figure below [11].

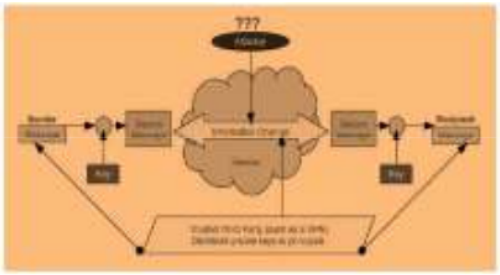

Figure 3. Network Security Model

A network security analysis system implements a high-speed and high-volume data volume analytic framework that engulfs and analyzes a variety of network data, such as Net Flow data, DNS data, and security and management information data [19]. The system detects, categories, and reports abnormal activity. This system applies natural language

processing (NLP) techniques that examine network analysis content and time series to establish and maintain a network condition condition model (for example, "normal" or nominal). The system analyzes its multi-dimensional perspective of network activity [20].

2.5. Elgamal Algorithm

The Elgamal algorithm was discovered in 1985 by an Egyptian scientist, Taher Elgamal. Elgamal algorithm is an algorithm based on the concept of a public key. This algorithm is generally used for digital signatures, but then modified so that it can be used for encryption and decryption. The security of the Elgamal algorithm lies in the difficulty of calculating discrete logarithms in large prime modules, so that efforts to solve these algorithm problems are difficult to solve [21]. This algorithm has the advantage of generating keys using discrete logarithms and decryption encryption methods that use large computational processes so that the encryption results are twice the original size [22]. The weakness of this algorithm is that it requires a large resource because the ciphertext is generated twice the length of the plaintext and requires a processor that is able to do large computations for large-scale logarithmic calculations [23].

3. Results and Discussion

The issue of database security and confidentiality is one important aspect of an information system. An information is only intended for certain parties, it is related to how the information cannot be accessed by unauthorized persons. Security of files on the database can be done by using several asymmetric algorithms that can lock database files, including the Elgamal algorithm [24]. 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 facilities provided by each operating system. For that, we need an application that can easily and quickly lock and secure the user's computer using keywords 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 [25]. In terms of database security techniques, many cryptographic methods can be used. The cryptographic methods have their own techniques and methods. The steps for each method are different, both in terms of length and complexity. One cryptographic method that can be used is the Elgamal method. Then it is necessary to do more in-depth research on the use of the Elgamal method applied to database security to achieve a high level of security.

3.1. Problem Solving Strategies

The problem solving phase is carried out to start from the process of analysis, design, evaluation and improve the system in accordance with needs, so that the system being made can be utilized optimally. In this study using the Elgamal method for cryptographic techniques as a way to secure a lecturer database at Universitas Potensi Utama, Medan.

Stages of searching for sources of knowledge or data are done through literature studies and interviews from:

a. Journals related to database security and the Elgamal method.

b. Books on database security and the Elgamal method.

c. A trusted website that contains matters relating to how to secure a database using the Elgamal method.

d. Direct interview to get data to the admin lecturer at Universitas Potensi Utama, Medan regarding the lecturer database that is managed.

Sources of knowledge and data obtained from this study are expected to be valid knowledge and data and can be used in the development of lecturer database security applications at the Universitas Potensi Utama.

3.2. Application of the Elgamal Method

With the many exchanges of information that occur, so many people who want these information for personal and group interests. This can happen if there is no high level of security from the exchange of important information. Based on these problems, the system to be built is a database security system that functions to secure database information in the form of lecturer data available at the Unviersitas Potensi Utama from irresponsible tappers. Then a database security is needed, in this case the database security is done by using the Elgamal method as the encryption and decryption process.

In this study, the author tries to create a database security application using a combination of Elgamal methods. By utilizing this method, it is hoped that a database security application can be developed that allows the user to encrypt the database with the Elgamal method and can decrypt the encrypted database.

The properties of the Elgamal method are as follows:

a.	Primes, p	(not secret)
b.	Randoms, g ($g < p$)	(not secret)
c.	Random, x ($x < p$)	(secret, private key)
d.	$y = g^x \bmod p$	(not secret, public key)
e.	m (plaintexts)	(secret)
f.	γ and δ (ciphertext)	(not seceret)

There are 3 stages carried out in applying the Elgamal method, namely the formation of keys, the encryption process and the decryption process.

3.2.1. Key Formation Process

The key formation process is the process of determining a number which will then be used as a key in the message encryption and decryption process. The key for encryption consists of the values p, g, y while the key for decryption consists of the values x, p. Each value has a requirement that must be met.

The steps in making a key are as follows:

a. Select any prime number p (p can be shared among group members).

b. Choose two random numbers, g and x, with the terms $g < p$ and $1 \leq x \leq p - 2$.

c. Calculate $y = gx \bmod p$.

The results of this algorithm:

- Public Key: triple (y, g, p)
- Private Key: double (x, p)

From the steps above, the public key used for encryption is the value of p, g, y and the private key used for decryption is the value x, p. The p, g, y values are not confidential while the x values are confidential.

This following is flowchart of the process of forming the Elgamal method is key.

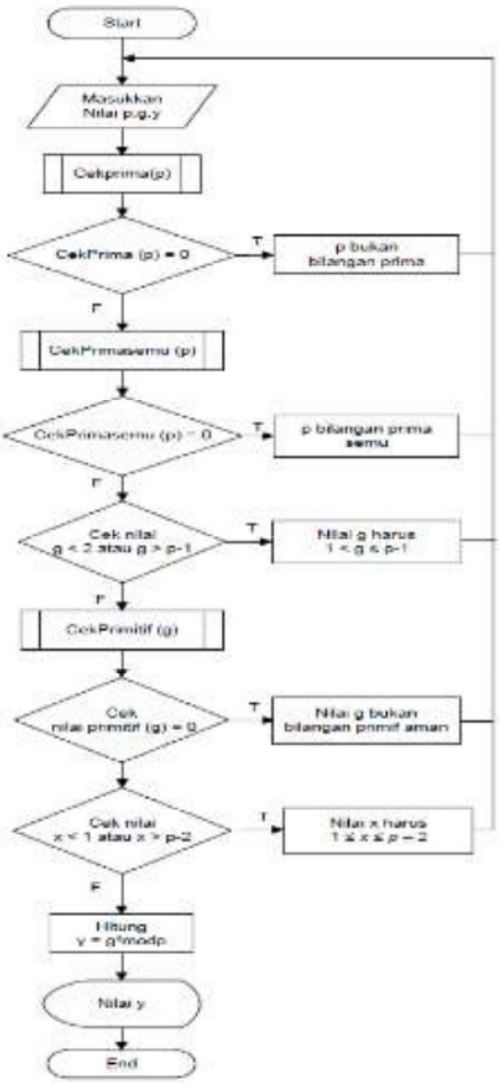

Figure 4. Key Formation Flowchart

Example :

Key Generation (By Budi)

- For example p = 2357, g = 2, dan x = 1751.
- Calculate: $y = g^x \bmod p = 21751 \bmod 2357 = 1185$
- Result : Public Key: (y = 1185, g = 2, p = 2357)
  Private key: (x = 1751, p = 2357).

3.2.2. Encryption Process

The encryption process is the process of changing the original message (plaintext) into a secret message (ciphertext). In this process public keys (p, g, y) are used. The steps in encrypting messages are as follows:

a. Arrange plaintext into blocks m1, m2, ..., (the value of each block in the interval [0, p - 1]).

b. Change the message block value to ASCII value.

c. Choose the random number k, which in this case is $1 \leq k \leq p - 2$.

d. Each block m is encrypted with a formula:

$\gamma = g^k \bmod p$

$\delta = y^k m \bmod p$

e. Arrange ciphertext in sequence $\gamma_1,\delta_1, \gamma_2,\delta_2,...,\gamma_n,\delta_n$.

f. The pairs γ and δ are ciphertexts for message blocks m. So, ciphertext is twice the size of the plaintext.

Following is the encryption process flowchart:

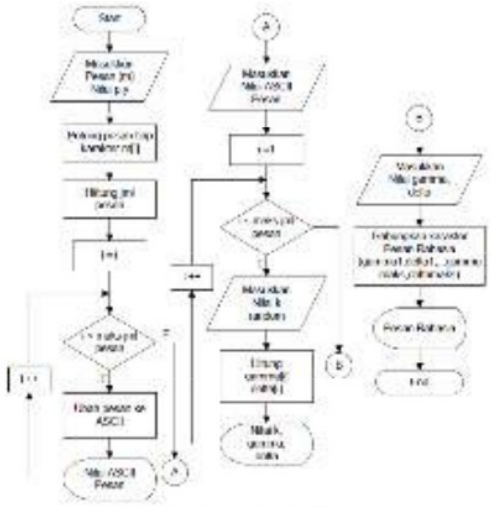

Figure 5. Encryption Process Flowchart

Example :

Encryption (By Ani)

- For example message m = 2035 (m value is still in the interval [0, 2357 – 1]).
- Bob chooses random numbers k = 1520 (the k value is still in the interval [0, 2357 – 1]).
- Ani calculates :

  $\gamma = g^k \bmod p = 21520 \bmod 2357 = 1430$

  $\delta = y^k m \bmod p = 11851520 \times 2035 \bmod 2357 = 697$

- So, the resulting ciphertext is (1430, 697).
- Ani sent this ciphertext to Budi.

3.2.3. Decryption Process

The decryption process is the process of changing a secret message (ciphertext) into an original message (plaintext). In this process private keys (x, p) are used. The steps in decrypting a message are as follows.

a. Determination of gamma and delta values. The gamma value (γ) is obtained from ciphertext in odd order while delta (δ) is in even order..

b. Use x private key to count:

$(\gamma^x)^{-1} = \gamma^{p-1-x} \bmod p$

c. Calculate plaintext m with equation:

d. $m = \delta / \gamma^x \bmod p = \delta\,(\gamma^x)^{-1} \bmod p$

e. Change the value of m obtained to ASCII value.

f. Arrange plaintext in sequence $m_1,m_2,...,m_n$.

The following is a flowchart of the Elgamal method decryption process.

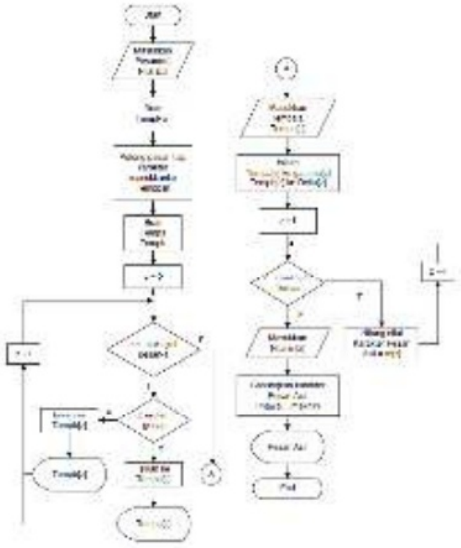

Figure 6. Decryption Process Flowchart

Contoh :

Decryption (By Budi)

- $1 / \gamma^x = (\gamma^x)^{-1} = \gamma^{p-1-x} \bmod p = 1430605 \bmod 2357 = 872.$
- $m = \delta / \gamma^x \bmod p = 697 \times 872 \bmod 2357 = 2035$

4. Conclusion

After carrying out the stages of the research process regarding the security of lecturer databases at Universitas Potensi Utama, Medan using the elgamal algorithm, it can be concluded that the elgamal algorithm can be used to convert the text contained in

the database into a secret text (ciphertext) so that it cannot be read by data thieves.

References

[1] M. Zayyadi, L. Supardi, and S. Misriyana, "Pemanfaatan Teknologi Komputer Sebagai Media Pembelajaran Pada Guru Matematika," *J. Pengabdi. Masy. Borneo*, vol. 1, no. 2, pp. 25–30, 2017.

[2] P. SAPTIAWAN, "RANCANG BANGUN KEAMANAN SISTEM PENDATAAN GUDANG BERBASIS CLIENT SERVER MENGGUNAKAN ALGORITMA ATBASH, VIGENERE DAN AFFINE CIPHER," 2018.

[3] P. Priyono and P. Tarigan, "IMPLEMENTASI ALGORITMA TRANSPOSISI CIPHER DAN VIGENGERE CIPHER UNTUK KEAMANAN BASIS DATA DALAM JARINGAN KOMPUTER," *Pelita Inform. Inf. dan Inform.*, vol. 16, no. 2, 2017.

[4] A. Siburian, A. P. Harianja, T. Informatika, U. St, J. Setia, and B. No, "Perancangan Aplikasi Pengamanan Basis Data Menggunakan Algoritma Caesar Cipher," vol. 02, no. 479, pp. 1–6, 2017.

[5] A. Pengamanan, D. Keuangan, B. Desktop, and M. Algoritma, "Aplikasi Pengamanan Database Keuangan Berbasis Desktop Menggunakan Algoritma Rc4 Dan Vigenere," vol. 1, no. 1, pp. 237–242, 2018.

[6] S. Bade, S. Jadhav, and K. Pakhare, "A ROBUST MULTI AUTHORITY VERIFICATION IN CLOUD USING ELGAMAL ENCRYPTION SCHEME," pp. 303–309.

[7] T. Erlangga and D. Kusumaningsih, "IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD-128 (AES-128) UNTUK PENGAMANAN DATABASE BERBASIS DESKTOP PADA ICALTOYS," *SKANIKA*, vol. 1, no. 2, pp. 565–569, 2018.

[8] C. V. B. Sakti, "IMPLEMENTASI PENGAMANAN DATABASE MENGGUNAKAN METODE BLOWFISH DAN AES PADA PERUSAHAAN," vol. 1, no. 1, pp. 366–372, 2018.

[9] A. D. Haryono and P. F. Ariyani, "APLIKASI PENGAMAN BASIS DATA PADA NUKLINDO LAB DENGAN ALGORITMA ELGAMAL DAN AFFINE CIPHER," *SKANIKA*, vol. 1, no. 1, pp. 186–192, 2018.

[10] D. Anggraini and S. Juanita, "Aplikasi E-Arsip Pengamanan Pesan Elektronik Berbasis Web dengan Mengimplementasikan Algoritma Kriptografi RSA dan Elgamal pada Klinik Dr. H. Hartono," *J. Ilm.*, vol. 6, no. 3, p. 122, 2018.

[11] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "A Review paper on Network Security and Cryptography," *Adv. Comput. Sci. Technol.*, vol. 10, no. 5, pp. 763–770, 2017.

[12] N. Kaur and H. Wadhwa, "Security Enhancement in Cloud Storage using ARIA and Elgamal Algorithms," *Int. J. Comput. Appl.*, vol. 171, no. 9, pp. 19–23, 2017.

[13] M. S. Hasibuan, "Keylogger Pada Aspek Keamanan Komputer," *J. Teknovasi J. Tek. dan Inov.*, vol. 3, no. 1, pp. 8–15, 2018.

[14] U. Rahardja, Q. Aini, and N. P. L. Santoso, "Pengintegrasian YII Framework Berbasis API pada Sistem Penilaian Absensi," *SISFOTENIKA*, vol. 8, no. 2, pp. 140–152, 2018.

[15] J. R. Batmetan, "Analisis Perilaku Mahasiswa PTIK di Unima dari Ancaman Keamanan Komputer," 2018.

[16] A. W. P. Putra, A. Bhawiyuga, and M. Data, "Implementasi Autentikasi JSON Web Token (JWT) Sebagai Mekanisme Autentikasi Protokol MQTT Pada Perangkat NodeMCU," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. e-ISSN*, vol. 2548, p. 964X, 2018.

[17] B. Rahardjo, *Berbasis Internet*, vol. 0. 1999.

[18] M. S. Herawati and N. Mintarsih, "PENINGKATAN KEAMANAN APLIKASI KONTROL DENGAN MENGGUNAKAN METODE FIREWALLDAN KASPERSKY ENDPOINT SECURITY 8," *UG J.*, vol. 7, no. 11, 2016.

[19] Y. Arta, "Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal," *IT J. Res. Dev.*, vol. 2, no. 1, pp. 43–50, 2017.

[20] P. J. Joyce and U. S. Ci, "(12) United States Patent," vol. 2, 2019.

[21] A. Karima, L. B. Handoko, and A. Saputro, "Pemfaktoran Bilangan Prima pada Algoritme ElGamal untuk Keamanan Dokumen PDF," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 6, no. 3, pp. 252–258, 2017.

[22] A. M. H. Pardede, "Aplikasi Pengamanan File Gambar Menggunakan Algoritma Elgamal," *J. Inf. Syst. Dev.*, vol. 3, no. 2, 2018.

[23] W. Sari *et al.*, "ANALISA ALGORITMA ELGAMAL DALAM PENYANDIAN DATA," vol. 2, no. 1, pp. 60–70, 2018.

[24] G. A. Sahputra and T. Fatimah, "IMPLEMENTASI KRIPTOGRAFI DENGAN METODE ALGORITMA ELGAMAL UNTUK KEAMANAN DATABASE BERBASIS JAVA DESKTOP PADA PT. MAKMUR SUPRA NUSANTARA," *SKANIKA*, vol. 1, no. 1, pp. 309–315, 2018.

[25] S. Sumarno, "Analisis Kinerja Kombinasi Algoritma Message-Digest Algortihm 5 (MD5), Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) Pada Keamanan E-Dokumen," *J. Sist. Inf. dan Ilmu Komput. Prima (JUSIKOM PRIMA)*, vol. 2, no. 1, 2018.

EDY VICTOR

ORIGINALITY REPORT

4%	0%	4%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Brickfields Asia College Student Paper	2%
2	Alexander Edi Suranta Kacaribu, Ratnadewi. "Multiplying cipher images on visual cryptography with ElGamal algorithm", 2015 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), 2015 Publication	2%

Exclude quotes	Off	Exclude matches	< 2%
Exclude bibliography	Off		