Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th February 2023. Vol. 2. No. 2

Development Of Hybrid Encryption Method Using Affine Cipher, Vigenere Cipher, And Elgamal Algorithm To Secure Text Messages In Data Communication System

[1]Raja Imanda Hakim Nasution, [2]Usman Gumanti, [3]Rifdahtul Ghinaa Sinambela, [4]Brema Arisma Sima, [5]Cindy Arista Br Bangun, [6]Bayu Krisna Sitepu, [7]Achmad Fauzi

[1,2,3,4,5,6,7]Informatic Engineering, STMIK Kaputama
Jl. Veteran No. 4A-9A, Binjai, North Sumatra, Indonesia
[1]rajaimandahakim@gmail.com,[2] ugumantu@gmail.com,[3]rgs011219@gmail.com, [4]bremaarismasima@gmail.com, [5]cindyarsitabrbangun@gmail.com, [6]bayukrisnastp@gmail.com, [7]fauzyrivai88@gmail.com

Abstract

With the development of technological advances in this day and age, it definitely requires a security system on messages and data. The way to maintain the security of data, messages or information requires a branch of science in its application, one of which is the algorithm or cryptography method. In its application, it requires more than one stage of the security process, because data security can be done by combining methods in its security techniques. This research aims to develop encryption methods using Affine Cipher, Vigenere Cipher, and ElGamal Algorithm to secure text messages. Affine cipher, Vigenere cipher and ElGamal are cryptography that can encrypt and decrypt text messages. Encryption is changing the message or plaintext into an unreadable message or ciphertext, on the other hand, decryption changes the ciphertext or message that initially cannot be read into a message that can be read or plaintext back in its original form. The result of this research is the development stage by doing three encryption and decryption processes. For the first encryption process using Affine Chiper which produces the initial ciphertext, then re-encrypted using Vigenere Cipher, then the previous encryption results are carried out ElGamal encryption which produces the final ciphertext. Conversely, the decryption process is first on ElGamal, then Vigenere Cipher, and finally Affine Cipher whose decryption results in plaintext back in the form of the initial text message. So that by developing and combining three algorithm methods can increase the security of information and text messages.

Keywords: *Affine, ElGamal, Security, Messages, Vigenere*

1. Introduction

Security and privacy protection of text messages is an important factor in today's information systems, due to the rapid development of technology that allows the emergence of new techniques that can be used unauthorizedly by parties that pose a threat to the security of information systems. Information owners can suffer financial losses if misused. Using encryption algorithms such as Affine Cipher, Vigenere Cipher, and Elgamal is one way to secure text messages.

Encryption and decryption are the two basic principles of cryptography. Decryption is the process of changing that form into the original information, while encryption is the process of using special algorithms to change data or information into a form that is almost impossible to recognize. One encryption method that can be used is the Vigenere Cipher, which hides text messages by replacing one letter with another based on the key used. This method uses a combination of 26 letters to secure the message and takes a long time to complete the algorithm. Besides Vigenere Cipher, another method that can be used is Affine Cipher, which is also an encryption method with a substitution cipher. The encryption process and the decryption process use the key n, where n is taken from the number of alphabets and the key m is taken from a prime number relative to the 26 number of alphabets.

ElGamal algorithm is one of the modern cryptographic techniques for encrypting and decrypting data that uses keys, plain text, and cipher text. Text cryptography, for example, is used to encrypt text into a password using a specific algorithm. However, the compression process is necessary to overcome the problem of lack of storage media for digital images.

In some previous studies, cryptography has been discussed, including those studied by Putra,2017 entitled: "APPLICATION OF CAMELIAN METHOD FOR CHATTINGBASED TEXT MESSAGE SECURITY" which concluded that cryptography is said to be a reliable strategy because in cryptography, cipher algorithms are used to disguise data sent over the network. Although the data can be read, unauthorized parties cannot understand it, so the data will remain safe because not everyone can access it freely [1]".

2. Theoretical Foundation

2.1 Cryptography

The study of how to encrypt or disguise a message so that it cannot be read by those without the key is called cryptography. The word "cryptography" comes from the Greek language and has two syllables: "crypto" and "graphia." Cryptography is writing, while graphia
is hiding. The confidentiality and integrity of messages are usually protected by cryptography.

2.2 Vigenere Cipher

Vigenere Cipher is one of the most popular encryption methods. It is one of the polyalphabetic encryption methods used to encode text messages by using a row of keywords in text form. Each keyword contains a single letter, and each letter in the keyword string repeats as many times as there are letters in the text message. This technique allows users to encode text messages by using several different keywords.

Vigenere Cipher Encryption Process, A single key is required to generate the ciphertext during the Vigenere Cipher encryption process. A combination of words or letters serves as the key. The specified key will then be converted to decimal form using a conversion table. The Vigenere Cipher must also convert the plain text (Pi) into decimal form using a conversion table. After that, the ciphertext (Ci) will be obtained by encrypting the plaintext with the solution:

Ci: (Pi + Ki) mod 26

Ci is the plaintext that changes the plaintext of the characters. Pi is the change in plaintext characters. Ki is the key consisting of a conversion table with decimal numbers representing the shift of the key characters.

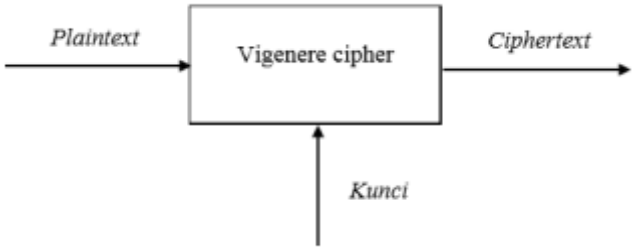

Figure 2.1 Vigenere Cipher Encryption

Figure 2.1 explains that the Vigenere cipher requires input in the form of plaintext and a key to convert plaintext into ciphertext.

Decryption with the Vigenere cipher A single key is required for the Vigenere cipher to generate plaintext. The key used is identical to the key used during the encryption process. The existing key will then be converted into decimal form using a conversion table. The Vigenere Cipher must also convert the ciphertext (Ci) using a conversion table which also produces a decimal number. After decrypting the plaintext with the following equation, the plaintext (Pi) can be obtained:

Pi: (Ci - Ki) mod 26

Pi is the plaintext of the character shift in the ciphertext. Ciphertext has a character shift called Ci. Ki is the key represented with a conversion result table represented with a decimal number based on the character shift the key uses. Then, to get Pi, and be able to subtract the Ci value from the Ki value, add the result with 26 to get modulo 26, then add the two numbers to get modulo 26. The result is a decimal

number, which is converted using the conversion table to the desired plaintext character of the decimal number.

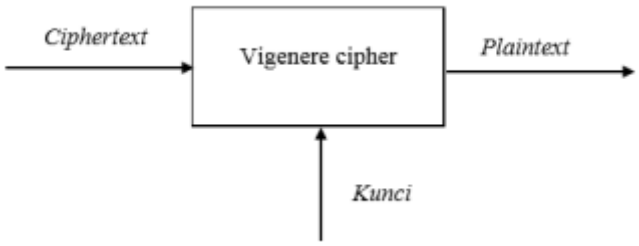

Figure 2.2. Vigenere Cipher Decryption

Figure 2.2 explains that the Vigenere cipher requires input in the form of ciphertext and key to convert ciphertext into plaintext [2].

2.3 Affine Cipher

An extension of the Caesar cipher is the affine cipher, a type of cipher. Affine ciphers are a component of classical algorithms, encryption techniques that predate the digital age. Substitution and transposition ciphers make up the majority of classical algorithms. The process of replacing characters from the plaintext is known as substitution cipher. While the process of exchanging letters in a string is a transposition cipher.

Keys 1(a) and 2(b) are required for the Affine cipher to be used for encryption. Using a conversion table, the plaintext (Pi) will be converted into decimal form. Ciphertext (Ci) will be obtained by encrypting the plaintext using lookup:

$$\mathbf{Ci : (a\ Pi + b)\ mod\ M}$$

The ciphertext of the character shift in the plaintext is called Ci. Pi is the character shift of the plaintext. The key is an integer that is relatively prime to 26; decryption is not possible if a is not relatively prime to 26. While the key b is a shift in the relative prime value of a, it is necessary to calculate using equation (1) to get the ciphertext. If the result is still a decimal number, it will be converted using a table into the desired ciphertext.

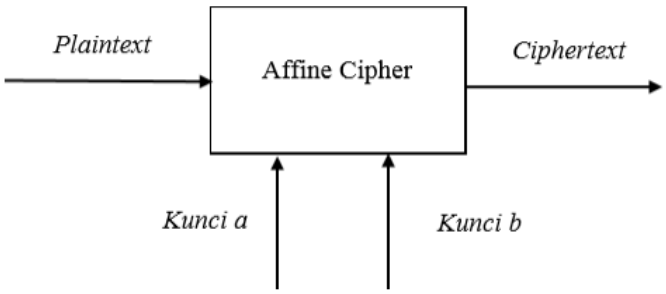

Figure 2.3 Affine Cipher Encryption

Figure 2.3 Encryption with Affine Cipher requires two keys, both of which must be used in the same way.

An Affine cipher requires two keys for decryption, and the two keys used must be identical to the keys used in encryption. Key 1 (a) will be converted into the inverse form of a (mod 26), which is represented by a -1, thus obtaining the plaintext. The equation will perform decryption if there is -1.

$$\mathbf{Pi : a\ -1\ (Ci - b)\ mod\ M}$$

Pi is the plaintext, the ciphertext has a character shift called Ci. The keys used during the encryption process are identical to a and b. Calculations with equations are required to obtain the plaintext. It is explained that Affine cipher requires input in the form of plaintext to be encrypted using two keys to get

the ciphertext, Pi and Ci must first be converted into decimal form before the first calculation can be done. conversion table. The calculation will produce numbers in decimal form which will be converted using the conversion table to produce plaintext.

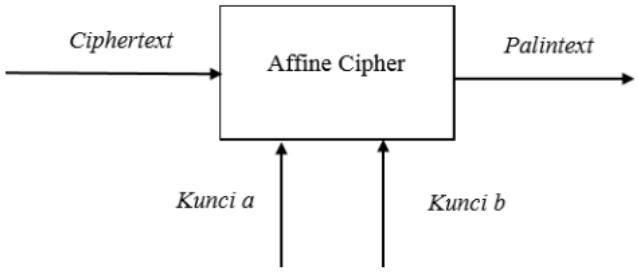

Figure 2.4 Decryption of Affine Cipher

Figure 2.4 explains that an affine cipher requires input in the form of ciphertext to be encrypted with two keys to get plaintext.

The key used in the Affine cipher is what makes it strong. Character shifts are indicated by this key, which has an integer value. Affine ciphers also utilize a sequence of numbers that act as key multipliers. The sequence used can be a specific number series, such as the even number series, odd number series, prime number series, and Fibonacci sequence. Homemade number series are also possible. Affine cipher is the best encryption system of all substitution encryption algorithms because it offers a wider range of keys and more encryption algorithms [2].

2.4 ElGamal Algorithm

ElGamal is a separate algorithm for creating public graphs. It was developed by Taher ElGamal in 1985. This algorithm has a key feature that can be seen in the logarithm analysis results. ElGamal Key Generation Algorithm uses various methods to perform key generation, encryption, and decryption processes [3].

Since it is difficult to compute discrete logarithms on large prime modulo, the ElGamal algorithm is secure. As a result, it is difficult to process this logarithmic problem-solving attempt. The advantage of this algorithm is that it generates the key using discrete logarithms and uses large processing for encryption and decryption, resulting in a result that is twice as large as the original. Since the resulting ciphertext is twice as long as the plaintext, this algorithm uses a lot of resources and requires a processor that can handle a lot of processing to calculate large exponential logarithms. The complexity of the decryption procedure requires a longer processing time for this algorithm. Since the ciphertext is larger than the plaintext, it needs to be processed twice [4].

Elgamal algorithm has two encryption and one decryption process.

The following are the properties of the ElGamal algorithm:

1. P :Prime numbers (not secret)
2. G :Random number (not secret)
3. X :Random number (secret)
4. Y :Public key (G^x mod P) (not secret)
5. K :Free key (not secret)

Encryption Process

a : g^k mod p
b : y^k m mod p

The encryption process is done by arranging the plaintext values according to the ASCII table.

Decryption Process

Mi : bi.ai $^{p-1-x}$ mod P

3. Research Methods

3.1 Encryption

Encryption is the process of transforming a message into a secret cipher in cryptography. Encryption is also known as cipher or code. By using a key that allows the message or information to be unreadable, the encryption process is carried out. Encryption is used to secure data or messages from unauthorized parties. Encryption can be expressed mathematically as follows: C (encryption process) = EK (M).
The message on M is encoded with key K during encryption, allowing it to produce message C, which is the ciphertext and message M is the plaintext.
In this research, there is a process to secure text messages by applying the functions of the encryption and decryption algorithms used. The steps taken, Figure 3.1 shows the encryption process:

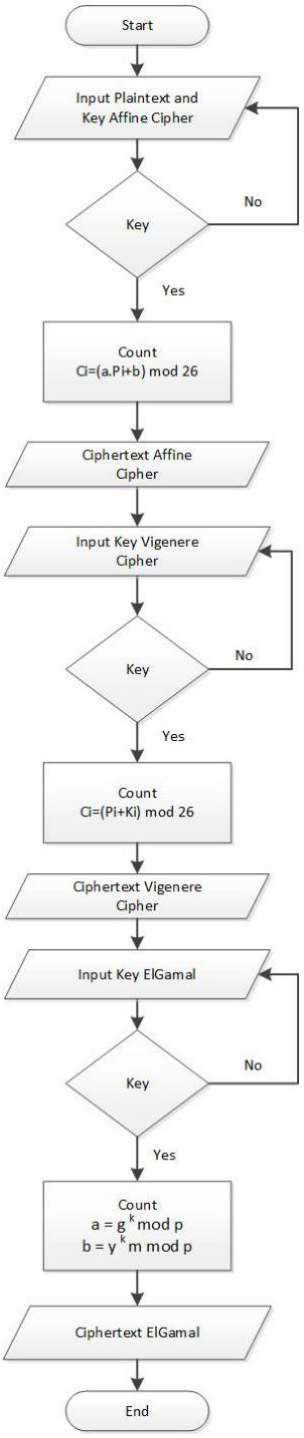

Figure 3.1 Flowchart of Encryption Process

In the encryption process, there are three encryption processes. The Encryption Process stage is performed on the following algorithm:

3.1.1 Encryption Process in Affine Cipher

The first encryption process is done with affine cipher, then the result of the encryption is encrypted again with vigenere cipher, with the following equation:

Ci : (a.Pi + b) mod M

Description: Ci: Ciphertext
Pi: Plaintext
A: First key
B: Second key
M: Total number of characters

With, Plaintext: MAHASISWA
Key: a: 3
b: 5

The calculation for the Encryption Process is:

C1 = ((3.12) + 5) mod 26
= 36 + 5 mod 26
= 15 : P

C2 = ((3.0) + 5) mod 26
= 0 + 5 mod 26
= 5 : F

C3 = ((3.7) + 5) mod 26
= 21 + 5 mod 26
= 0 : A

C4 = ((3.0) + 5)mod 26
= 0 + 5 mod 26
= 5 : F

C5 = ((3.18) + 5) mod 26
= 54 + 5 mod 26
= 7 : H

C6 = ((3.8) + 5) mod 26
= 24 + 5 mod 26
= 3 : D

C7 = ((3.18) + 5) mod 26
= 54 + 5 mod 26
= 7 : H

C8 = ((3.22) + 5) mod 26
= 66 + 5 mod 26
= 19 : T

C9 = ((3.0) + 5) mod 26
= 0 + 5 mod 26
= 5 : F

So, the result of **MAHASISWA** encryption is
Ciphertext: **PFAFHDHTF**

3.1.2 Encryption Process on VIGENERE CIPHER

The result of Affine Cipher encryption is encrypted back into Vigenere Cipher, with the following equation:

Ci : (Pi + Ki) mod 26

Description: Ci: Ciphertext
Pi: Plaintext
Ki: Key

With, Plaintext: PFAFHDHTF
Key : STMIK

P	F	A	F	H	D	H	T	F
S	T	M	I	K	S	T	M	I

The calculation for the Encryption Process is:

C1 = (15 + 18) mod 26
= 33 mod 26
= H

C2 = (5 + 19) mod 26
= 24 mod 26
= Y

C3 = (0 + 12) mod 26
= 12 mod 26
= M

C4 = (5 + 8) mod 26
= 13 mod 26
= N

C5 = (7 + 10) mod 26
= 17 mod 26
= R

C6 = (3 + 18) mod 26
= 21 mod 26
= V

C7 = (7 + 19) mod 26
= 26 mod 26
= A

C8 = (19 + 12) mod 26
= 31 mod 26
= F

C9 = (5 + 8) mod 26
= 13 mod 26
= N

So, the result of **PFAFHDHTF** encryption is Ciphertext: **HYMNRVAFN**

3.1.3 Encryption Process in Elgamal Algorithm

The result of Vigenere Cipher encryption is encrypted back into ElGamal, with the following equation:

a: g^k mod p
b : y^k m mod p

With, P : 257
G : 17
X : 11
Y : g^x mod p = 17^{11} mod 257 = 223
Plaintext : HYMNRVAFN

Character	Plaintext Mi	ASCII	Key
H	M1	72	11
Y	M2	89	22
M	M3	77	33
N	M4	78	44
R	M5	82	55
V	M6	86	66
A	M7	65	77
F	M8	70	88
N	M9	78	99

The calculation for Encryption Process A is:

A1 = 1711 mod 257
= 223

A2 = 1722 mod 257
= 128

A3 = 1733 mod 257
= 17

A4 = 1744 mod 257
= 193

A5 = 1755 mod 257
= 120

A6 = 1766 mod 257
= 32

A7 = 1777 mod 257
= 197

A8 = 1788 mod 257
= 241

A9 = 1799 mod 257
= 30

The calculation for Encryption Process B is:

B1 = 22311 72 mod 257
= 205
B2 = 22322 89 mod 257
= 236
B3 = 22333 77 mod 257
= 209
B4 = 22344 78 mod 257
= 202
B5 = 22355 82 mod 257
= 37
B6 = 22366 86 mod 257
= 214
B7 = 22377 65 mod 257
= 102
B8 = 22388 70 mod 257
= 92
B9 = 22399 78 mod 257
= 41

= a1 b1 a2 b2 a3 b3 a4 b4 a5 b5 a6 b6 a7 b7 a8 b8 a9 b9
So, the result of **HYMNRVAFN** encryption is Ciphertext: **223 205 128 236 17 209 193 202 120 37 32 214 197 102 241 92 30 41**

ASCII: ■ ═ Ç ý (Bell) Đ ┴ ╩ x % (Space) Í ┼ f ± \ (Record separator)

3.2 Decryption

Decryption is the process of unlocking the secret code resulting from encryption. Using the same key that was used during the encryption process, this procedure involves restoring the encrypted data or password to its original form. Decryption can be expressed mathematically as follows: M (Decryption Process) = DK (C).
The encrypted message (ciphertext) with key K will be translated into the original message (plaintext) during the decryption process. The message plaintext M is the end product of the decryption process.
In this research there is also a process for securing text messages by applying the functions of the algorithms used for encryption and decryption. The steps in the decryption process that must be carried out, as depicted in the Decryption Process flowchart image:

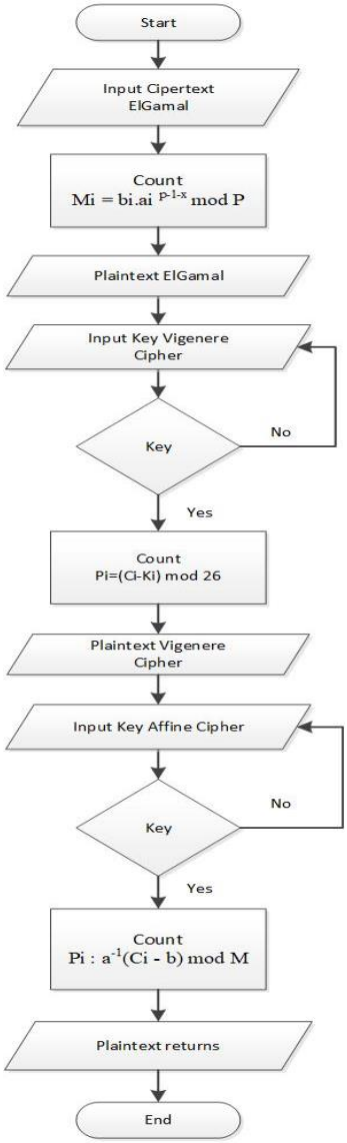

Figure 3.2 Flowchart of Decryption Process

The decryption process follows the opposite steps to convert the unintelligible code or ciphertext into understandable ciphertext. At this stage there are three decryption processes performed in the following algorithm:

3.2.1 Decryption Process in ElGamal Algorithm:

The decryption process of Elgamal produces a temporary plaintext, then decrypted with Vigenere cipher to produce a temporary plaintext as well, with the following agreement:

$$\mathbf{Mi : bi.ai^{p-1-x} \bmod P}$$

The calculation for the decryption process is:

M1 = 205.223245 mod 257
= 72
M2 = 236.128245 mod 257
= 89
M3 = 209.17245 mod 257
= 77
M4 = 202.193245 mod 257
= 78
M5 = 37.120245 mod 257
= 82
M6 = 214.32345 mod 257
= 86
M7 = 102.197245 mod 257
= 65
M8 = 92.241245 mod 257
= 70
M9 = 41.30245 mod 257
= 78

So, the result of the decryption is the temporary plaintext: 72 89 77 78 82 86 65 70 78: **HYMNRVAFN**

3.2.2 Decryption Process of Vigenere Cipher

The decryption process of Vigenere Cipher produces a temporary plaintext, then decrypted with Affine Cipher to produce plaintext again, with the following agreement:

Pi : (Ci - Ki) mod 26

With, Ciphertext: HYMNRVAFN
Key: STMIK

H	Y	M	N	R	V	A	F	N
S	T	M	I	K	S	T	M	I

The calculation for the decryption process is:

P1 = (7 – 18) mod 26
= 15 : P
P2 = (24 – 19) mod 26
= 5 : F
P3 = (12 – 12) mod 26
= 0 : A
P4 = (13 – 8) mod 26
= 5 : F
P5 = (17 – 10) mod 26
= 7 : H
P6 = (21 – 18) mod 26
= 3 : D
P7 = (0 – 19) mod 26
= -19 : H
P8 = (5 – 12) mod 26
= -7 : T
P9 = (13 – 8) mod 26
= 5 : F

So, the decryption result of **HYMNRVAFN** is the temporary plaintext: **PFAFHDHTF**

3.2.3 Decryption Process of Affine Cipher

The decryption result of Affine Cipher to produce plaintext again, with the following equation:

Pi : a^{-1}(Ci - b) mod M

Description: a-1 : relative prime between a and m
With, Ciphertext: PFAFHDHTF
Calculating the value of a-1 i.e:

a = 3, b = 5, m (number of characters) = 26
: 3 multiplied by what number, so that when mod 26 the result is 1.
a.a-1 = 1 (mod 26)
3.a-1 = 1 (mod 26)
3.9 = 27

3.9 = 1 (mod 26)
a-1 = 9

The calculation for the decryption process is:

P1 = 9 (15 – 5) mod 26
= 9 x 10 mod 26
= 12 : M

P2 = 9 (5 – 5) mod 26
= 9 x 0 mod 26
= 0 : A

P3 = 9 (0 – 5) mod 26
= 9 x (-5) mod 26
= 7 : H

P4 = 9 (5 – 5) mod 26
= 9 x 0 mod 26
= 0 : A

P5 = 9 (7 – 5) mod 26
= 9 x 2 mod 26
= 18 : S

P6 = 9 (3 – 5) mod 26
= 9 x (-2) mod 26
= 8 : I

P7 = 9 (7 – 5) mod 26
= 9 x 2 mod 26
= 18 : S

P8 = 9 (19 – 5) mod 26
= 9 x 14 mod 26
= 22 : W

P9 = 9 (5 – 5) mod 26
= 9 x 0 mod 26
= 0 : A

So, the decryption result of **PFAFHDHTF** is the original plaintext: **MAHASISWA**

4. CONCLUSIONS

To improve the security of text messages, we developed a method that combines all three by going through the encryption and decryption process three times. This method uses Affine Cipher to encode the text message using a string of keywords. Then, the encrypted message will be re-encrypted using Vigenere Cipher and Elgamal to increase the security level. This method will ensure that the text message is securely encrypted and cannot be read by other parties. Thus, our method can be used to protect text messages from unwanted parties.

References

[1] D. Putra, “PENERAPAN METODE CAMELIAN UNTUK KEAMANAN,” vol. 6, pp. 238–240, 2017.
[2] Y. Religia, P. Studi, T. Informatika, F. I. Komputer, U. Dian, and N. Semarang, “IMPLEMENTASI ALGORITMA AFFINE CIPHER DAN VIGENERE CIPHER UNTUK KEAMANAN LOGIN”.
[3] P. Hasil, P. Skripsi, J. T. Elektro, F. Teknik, U. Brawijaya, and P. Studi, “IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK FILE CITRA 2 DIMENSI”.
[4] F. Husaini, A. M. H. Pardede, and I. Gultom, “Penerapan Enkripsi Menggunakan Metode Elgamal guna Meningkatkan Keamanan Data Text dan Gambar,” *JUKI J. Komput. dan Inform.*, vol. 4, pp. 55–61, 2022.