Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 13-18
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3122
Website https://ejurnal.seminar-id.com/index.php/jussi

Modifikasi Algoritma El-gamal Dengan Menerapkan Algoritma Kargers Min Cut Untuk Pembangkitan Kunci

Rizki Darmawan Ritonga

Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Budi Darma,
Jalan Sisingamanganraja No. 338,Medan, Sumatera Utara, Indonesia
Email: rizkidermawanr04@gmail.com

Abstrak−Algoritma El-gamal mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. Algoritma ini memiliki keamanan yang terletak pada kesulitan dalam menghitung alogaritma diskrit. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Algoritma El-gamal tipe algoritma kriptografi asimetris terdiri atas dua buah kunci yaitu kunci publik untuk melakukan enkripsi sedangkan kunci pribadi untuk melakukan dekripsi. Dalam algoritma El-gamal, kunci yang didistribusikan adalah kunci publik yang tidak diperlukan kerahasiannya sedangkan kunci pribadi tetap disimpan atau tidak didistribusikan. Setiap orang yang memiliki kunci publik dapat melakukan proses enkripsi tetapi hasil dari enkripsi tersebut hanya bisa dibaca oleh orang yang memiliki kunci pribadi. Untuk meningkatkan kekuatan dari algoritma tersebut, maka kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi akan dimodifikasi terlebih dahulu menggunakan algoritma pengacakan yaitu Algoritma Karger Min Cut. Algoritma Karger Min Cut adalah algoritma acak probabilistik yang digunakan untuk memverifikasi perkalian matriks. Tujuan dalam menggunakan algoritma Kargers Min Cut ini adalah agar kunci yang dihasilkan lebih sulit ditebak sehingga mempersulit kriptanalis dalam membaca pesan atau informasi tersebut.

Kata Kunci : Kriptografi; Modifikasi; Kunci; Pengacakan; Algoritma El-Gamal; Algoritma Kargers Min Cut.

Abstract− El-gamal algorithm has two keys, namely public key and secret key. This algorithm has security that lies in the difficulty in calculating discrete algorithms. Both encryption and decryption keys are integers. El-gamal algorithm type asymmetric cryptography algorithm consists of two keys namely public key to encrypt while private key to decrypt. In El-gamal algorithms, distributed keys are public keys that are not required confidentiality while private keys remain stored or not distributed. Anyone who has a public key can do the encryption process but the result of that encryption can only be read by the person who has the private key. To increase the strength of the algorithm, the key used to perform the encryption and decryption process will be modified first using the randomization algorithm that is Karger Min Cut Algorithm. Karger Min Cut algorithm is a probabilistic random algorithm used to verify matrix multiplication. The purpose of using Kargers Min Cut algorithm is to make the resulting key more difficult to guess, making it difficult to read the message or information..

Keywords : Cryptography; Modification; Key; Randomize; El-Gamal Algorithm; Min Cut Kargers Algorithm.

1. PENDAHULUAN

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandingkannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah *plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *ciphertext* (teks sandi). Berdasarkan sejarahnya kriptografi dapat dibagi menjadi kriptografi klasik dan kriptografi modern dan berdasarkan kuncinya dapat dibagi menjadi kriptografi simetris dan kriptografi asimetris [1].

Algoritma pengacakan adalah yang menghasilkan permutasi acak dari suatu himpunan terhingga, dengan kata lain untuk mengacak suatu himpunan Adapun salah satu algoritma pengacakan yang di gunakan adalah Algoritma *Kargers Min Cut.* Algoritma *Kargers Min Cut* algoritma acak probabilistik yang digunakan untuk memverifikasi perkalian matriks. Algoritma ini digunakan untuk memodifikasi algoritma *El-Gamal* pada enkripsi yang menggunakan pasangan *plaintext* dengan sebuah kunci rahasia yang diperoleh secara acak.

Berdasarkan penelitian sebelumnya yang dilakukan oleh Nonik Indahwati,, Agus Prihanto yang dipublikasi pada jurnal *JINACS* (*Journal of Informatics and Computer Science*) yang berjudul Penerapan Algoritma Kriptografi Asimetris *El-gamal* dengan Modifikasi Pembangkit Kunci terhadap Enkripsi dan Dekripsi Gambar. Modifikasi pada pembangkit kunci yang dilakukan menghasilkan kecocokan kunci yang baik. Perbandingan kemiripan yang terdapat pada gambar asli dengan gambar setelah dienkripsi terdapat perbedaan, sedangkan perbandingan kemiripan gambar asli dengan gambar setelah didekripsi tidak terdapat perbedaan[2].

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Mengenai Metodologi penelitian yang digunakan penulis dalam penelitian Modifikasi Algoritma El-gamal Dengan Menerapkan Algoritma Kargers Min Cut Untuk Pembangkitan Kunci yaitu adalah sebagai berikut:

a. Perpustakaan (Library)

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 13-18
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3122
Website https://ejurnal.seminar-id.com/index.php/jussi

Penelitian perpustakaan merupakan bentuk penelitian yang dilakukan penulis berdasarkan kepustakaan, literatur, internet dan sumber lain yang mempunyai hubungan dengan masalah tersebut dengan maksud memperoleh data yang akurat.

b. Analisa (Analysis)
Mempelajari pokok permasalahan dan mempelajari modifikasi algoritma el-gamal dengan menerapkan algoritma kargers min cut. Pada tahap ini dilakukan perencanaan sistem yang akan dibangun dengan cara melihat terlebih dahulu latar belakang permasalahan dan kemudian dilakukan analisa langkah-langkah dalam mengimplementasikan algoritma el-gamal Roc dan kargers min cut.
c. Perancangan
Setelah analisa sistem siap dilakukan, jadi analisis sistem telah mendapatkan objek dengan nyata yang harus dibuat. berikutnya bagi pengamatan sistem untuk memperhitungkan bagaimana objek sistem tersebut.
d. Pengujian
Dari langkah ini dilakukan praktek sistem untuk menghasilkan apakah sistem tersebut sesuai dengan yang diinginkan dalam modifikasi algoritma el-gamal dengan menerapkan algoritma kargers min cut.
e. Implementasi
Dari langkah ini dilakukan perkodean program yang diterapkan dalam pembuatan sistem menggunakan Microsoft Visual Basic 2008.
f. Dokumentasi
Pada tahap ini dilakukan pengumpulan data dari data-data yang diperoleh memberikan pengertian atau bukti yang menyambung dengan proses pengumpulan informasi.

2.2 Modifikasi

Modifikasi mengacu kepada sebuah ciptaan, peyusuaian dan menampilkan suatu alat / sarana yang baru, unik dan menarik terhadap suatu proses pekerjaan, sebagai salah satu alternative atau solusi dalam mengatasi permasalahan yang tejadi dalam proses pekerjaan [3]

2.3 Algoritma

Menurut Rinaldi Munir algoritma adalah urutan logis langkah-langkah penyelesaian masalah yang disusun secara sistematis. Alur pemikiran dalam menyelesaikan suatu pekerjaan yang dituangkan secara tertulis. Yang ditekankan pertama adalah alur pemikiran sehingga algoritma seseorang dapat juga berbeda dari orang lain. Sedangkan penekanan kedua adalah tertulis, yang artinya dapat berupa kalima, gambar atau tabel tertentu. Algortima dapat dituliskan dalam berbagai notasi tertentu.[4][5]

2.4 Kriptografi

Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua, yaitu *kripto* dan *graphia*. *Kripto* berarti *secret* (rahasia) dan graphia berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern *kriptografi* adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan menyembunyikan pesan, namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi.[6][7]

2.5 Algoritma El-Gamal

Algoritma *El-gamal* merupakan algoritma dalam kriptografi yang termasuk dalam kategori algoritma asimetris. Keamanan algoritma *ElGamal* terletak pada kesulitan penghitungan logaritma diskrit pada bilangan modulo prima yang besar sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sangat sukar. Algoritma *ElGamal* mempunyai kunci publik berupa tiga pasang bilangan dan kunci rahasia berupa satu bilangan.[1][8][9][10]

Pembentukan kunci terdiri atas pembentukan kunci publik dan kunci rahasia. Pada proses ini dibutuhkan sebuah bilangan prima (p) yang digunakan untuk membentuk grup Zp*, elemen primitive α dan sembarang a { 0,1,…., p-2}. Kunci publik algoritma *ElGamal* terdiri atas pasangan 3 bilangan (p, α, β) di mana:

$$\beta = \alpha^a \bmod p \qquad (1)$$

Sedangkan kunci rahasianya adalah bilangan *a* tersebut. Proses pembentukan kunci untuk algoritma *ElGamal* terdiri atas:

a. Penentuan bilangan prima aman yang bernilai besar
b. Penentuan elemen primitif.
c. Pembentukan kunci berdasarkan bilangan prima aman dan elemen primitif.

2.6 Algoritma *Karger Min Cut*

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 13-18
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3122
Website https://ejurnal.seminar-id.com/index.php/jussi

Algoritma Karger Min Cut adalah algoritma acak untuk menghitung potongan minimum dari grafik yang terhubung. Ide algoritma didasarkan pada konsep kontraksi tepi (u, v) dalam grafik tidak terarah G = (V, E). Berbicara secara informal, kontraksi tepi menggabungkan node u dan v menjadi satu, mengurangi jumlah total node grafik dengan satu.

Adapun rumus pengacakan Algoritma *Karger Min Cut* sebagai berikut:[1][11]

$$\min = \{g^1\} \sum_{p_i \epsilon p} r(pi) + \sum_{q_j \epsilon Q} c\left(q_j\right). \quad (2)$$

Dimana :
Min{g$^{'}$} = Hasil Nilai pengacakan
r = Jumlah Grafik
(p_i,q_i) =Nilai Yang Diacakv

3. HASIL DAN PEMBAHASAN

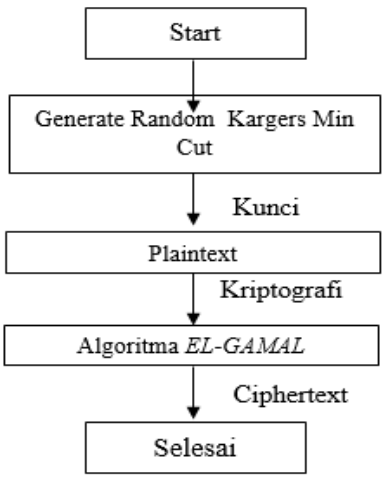
3.1 Pembahasan

Analisa terdapat suatu algoritma dapat bertujuan untuk melihat faktor efesiensi dan efektifitas dari algoritma yang sedang dianalisa , dapat dilakukan dengan melihat sisi waktu tempu dari suatu algoritma, proses, langkah langkah atau satuan waktu yang ditempuh dari suatu algoritma dalam menyelesaikan suatu masalah.kriptografi merupakan metode dengan menyandikan file teks menjadi yang sulit atau bahkan tidak dipahami melalui proses enkripsi, untuk memperoleh kembali informasi yang dapat dengan proses enkripsi, untuk memperoleh kembali informasih yang asli dan dapat dilakukan dengan proses enkripsi yang tentunya dapat digunakan dengan kunci yang benar, Untuk melindungi file teks dari pihak pihak yang tidak berkepintangan tersebut maka diperlukan enkripsi dan denkripsi agar dapat dilakukan dengan baik, dibutuhan suatu algoritma untuk endkripsi dan dekripsi salah satunya algoritma EL-GAMAL.

Algoritma EL-GAMAL mempunyai dua kunci, yaitu kunci publik dan kunci private. Algoritma ini memiliki keamanan yang terletak pada kesulitan dalam menghitung logaritma diskrit . Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. EL-GAMAL adalah salah satu teknik kriptografi dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi.

Kunci untuk melakukan enkripsi disebut sebagai kunci publik, sedangkan kunci untuk melakukan dekripsi disebut sebagai kunci private. Orang yang mempunyai kunci publik dapat melakukan enkripsi tetapi yang dalam melakukan deskripsi hanyalah orang yang memiliki kunci privat. Kunci publik dapat dimiliki oleh sembarang orang, tetapi kunci private hanya dimiliki oleh orang tertentu saja. Untuk meningkatkan kekuatan dari algoritma tersebut, maka kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi akan diimplementasikan terlebih dahulu menggunakan algoritma pengacakan yaitu Algoritma Karger Min Cut.

Pembangkit kunci dilakukan dengan menggunakan algoritma yang menggunakan bilangan random dengan memasukkan bilangan random, dianggap dapat menghilangkan kemungkinan penyerang menebak hasil dengan mengetahui algoritmanya. Telah banyak algoritma generator bilangan acak yang diusulkan dan digunakan hingga saat ini. Algoritma-algoritma tersebut menggunakan berbagai pendekatan berbeda untuk menghasilkan bilangan random seacak. Salah satu algoritma tersebut adalah Algoritma *Karger Min Cut*. Algoritma *Karger Min Cut* adalah algoritma acak untuk menghitung potongan minimum dari grafik yang terhubung. Buku itu ditemukan oleh David Karger dan pertama kali diterbitkan pada tahun 1993. Dengan mengulangi algoritma dasar ini beberapa kali, pemotongan minimum dapat ditemukan dengan probabilitas tinggi. Adapun proses Modifikasi kunci algoritma *EL-GAMAL* dengan menggunkan Algoritma *Karger Min Cut* dijelaskan mengenai rancangan sistem penambahan Modifikasi pada metode kriptografi yang diteliti. Secara garis besar, proses yang dilakukan pada penelitian ini digambarkan dengan block diagram berikut:

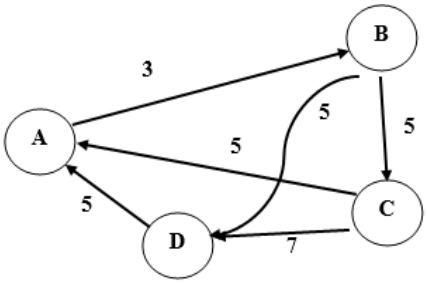


Gambar 1. Diagram Modifikasi Kunci Algoritma *EL-GAMAL*

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 13-18
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3122
Website https://ejurnal.seminar-id.com/index.php/jussi

Adapun proses modifikasi kunci algoritma *Elgamal* dengan menggunakan algoritma *Kargers Min Cut* yaitu contoh kasus dalam proses ini adalah file *teks.* Data *teks* yang diambil adalah "RIZKIDARMAWAN"

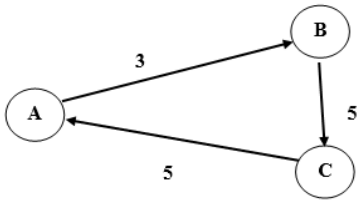
a. Proses pembentukan kunci menggunakan Algoritma *Elgamal*
   Proses pembentukan kunci merupakan proses penentuan suatu bilangan yang kemudian akan digunakan sebagai kunci pada proses enkripsi dan deskripsi pesan. Kunci untuk enkripsi dibangkitkan dari nilai p,g,y sedangkan kunci untuk deskripsi terdiri dari nilai x,p. Masing-masing nilai mempenyai persaratan yang harus dipenuhi.
b. Proses Pembentukan Kunci Dengan menggunkan *Karger Min Cut*
   Pada algoritma *Elgamal* mempunyai dua kunci, yaitu kunci publik dan kunci private dan bilangan yang di gunakan adalah bilangan prima. Oleh sebab itu penggunaan algoritma *Karger Min Cut* di gunakan untuk pembentukan 2 kunci dari algoritma *Elgamal* adalah sebagi berikut:



Gambar 2. Grafik Pengacakan *Karger Min Cut*

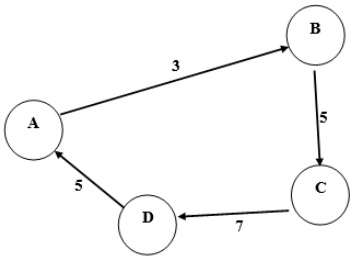
Penyelesaian :

a. Tentukan 2 grafik yang dapat dituju sampai pada dirinya sendiri



$$G = \sum_{pi \in P} r(pi) - \sum_{qi \in Q} c(qi)$$

G {A: B, D} = (4*(3+5+5)) + (3 *(3+5 + 5)
G {A: B, D} = (4*13) -(3*13)
G {A: B, D} = 52-39 =13



G {A: B, C, D} = (4 *(3 +5+7 +5) + (4 *(3 +5 +7+5)
G {A: B, C, D} = (4*20) +(4*20)
G (A: B, C, D} = 80 + 80 = 160

b. Proses Enkripsi Dengan menggunkan Algoritma *El-gamal*
   Enkripsi Metode *Elgamal* :
   Input : RIZKIDARMAWAN
   Kunci PRIVATE = (x,y) K_{public} = (3, 13)
   Kunci PUBLIC = (p,g,y) K_{public} = (160,3,13)

Tabel 1. Hasil Proses Enkripsi

Plainteks	Char	ASC	K	a=(g^k)mod p	b=((y^k)*M)) mod p	(a,b)
M1	R	82	1	3	106	3,106
M2	I	73	11	96	61	96,61
M3	Z	90	8	43	90	43,90
M4	K	75	5	32	95	32,95

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 13-18
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3122
Website https://ejurnal.seminar-id.com/index.php/jussi

M5	I	73	2	65	17	65,17
M6	D	68	12	100	70	100,70
M7	A	65	9	21	45	21,45
M8	R	82	6	96	98	96,98
M9	M	77	3	3	49	3,49
M10	A	65	0	30	45	30,45
M11	W	87	10	130	9	130,9
M12	A	65	7	96	5	96,5
M13	N	78	4	1	128	1,128

Susun plainteks menjadi blok-blok m1 , m2 , …, (nilai setiap blok di dalam selang [0, p – 1]. 2. Pilih bilangan acak k, yang dalam hal ini $1 \leq k \leq p-2 \, mod \, M$.

Pembentukan Nilai K_1=1 ≤ k ≤ p – 2.

K_1= 160-3 mod 13 = 1

a_1 = (g^k)mod p
= 3^1 Mod 160
= 3

b_1 = ((y^k)*M)) mod p
= ((13^1)* 82)) mod 160
= 106

…….

K_{13}= 160-39 mod 13= 4

a_{13} = (g^k)mod p
= 39^4 Mod 160
= 1

b_{13} = ((y^k)*M)) mod p
= ((13^4)* 78)) mod 160
= 128

Hasil chipertext dari enkripsi algoritma Elgamal adalah=(3,106), (96,61), (43,90), (32,95), (65,17), (100,70), (21,45), (96,98), (3,49), (30,45), (130,9), (96,5),(1,128). Dengan hasil chipertext berdasarkan ASCII menjadi**= *End of Text , Grave accent , Plus, Space, Uppercase A, Lowercase d, Negative Acknowledgement, Grave accent, End of Text, Record Separator, Single low9 quotation mark , Grave accent, Start of Heading,***

Setelah melakukan modifikasi dan mendapatkan hasil maka proses selanjutnya melakuakn Dekripsi dengan menggunkan Algoritma *Elgamal*

Chipertext **= *End of Text, Grave accent , Plus, Space, Uppercase A, Lowercase d, Negative Acknowledgement, Grave accent, End of Text, Record Separator, Single low9 quotation mark , Grave accent, Start of Heading***,

Diubah menjadi kode ASCII adalah= (3,106), (96,61), (43,90), (32,95), (65,17), (100,70),(21,45),(96,98),(3,49),(30,45),(130,9),(96,5),(1,128).

Kunci x= 3, p=160

Mencari *planteks* P1(3,106):

$S1= a^x \bmod p$

$S1=3^3 \bmod 160$

S1= 27

$P1= (b*s^{p-x}) \bmod p$

$P1= (160*27^{160-3}) \bmod 160$

$P1= (160*27^{157}) \bmod 160$

P1= 82=R

…….

Mencari plainteks p13(1,128)

$S13= a^x \bmod p$

$S13= 1^3 \bmod 160$

S13= 1

$P13= (b*s^{p-x}) \bmod p$

$P13= (160*1^{160-3}) \bmod 160$

$P13= (160*1^{157}) \bmod 160$

P13= 78 = N

Hasil *plaintext* dari dekripsi algoritma *Elgamal* adalah **RIZKIDARMAWAN**.

Berdasarkan hasil pengujian yang dilakukan dengan melakukan Modifikasi Algoritma El-gamal Dengan Menerapkan Algoritma Kargers Min Cut Untuk Pembangkitan Kunci dapat disimpulkan hasil eknripsi dapat dikembalikan lagi walaupun sudah terdapat perubahan dalam melakukan pengamanan data berdasarkan sampel data yang digunakan.


Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 13-18
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3122
Website https://ejurnal.seminar-id.com/index.php/jussi

4. KESIMPULAN

Dari hasil penelitian yang telah dilakukan maka dapat diambil kesimpulan berdasarkan hasil pengujian yang telah dilakukan maka diperoleh kesimpulan yaitu Proses penerapan Algoritma Karger Min Cut dengan cara melakukan pengacakan nilai untuk pembentukan kunci berdasarkan metode kriftografi Algoritma El-gamal dan Proses enkripsi teks dapat dilakukan serta hasil pengembalian enkripsi dengan cara melakukan proses depkripsi dapat dilakukan dengan baik menggunakan algoritma El-gamal berdasarkan kunci yang telah di modifikasi dengan algoritma Karger Min Cut, Perancangan aplikasi modifikasi pembangkitan kunci Algoritma El-gamal dapat dilakukan.

REFERENCES

[1] Agus Kurniadi, "Implementasi kriptografi ELGAMAL dalam keamanan pesan," INFOTEK, vol. 1, pp. 1–5, 2016.
[2] T. Cahyadi, "Implementasi steganografi LSB dengan enkripsi vigenere cipher pada citra JPEG," TRANSIENT, vol. 1, pp. 1–8, 2012.
[3] Ichsan Mohamad, "Penerapan Modifikasi alat untuk meningkatkan keterampilan bermain bulu tangkis" Jurnal Pendidikan Jasmani da Olahraga, vol. I, pp. 68–76, 2016.
[4] R. MUNIR, ALGORITMA & PEMOGRAMAN. Bandung: INFORMATIKA Bandung, 2011.
[5] P. D. Dr.Suarga, M.Sc., M.Math., Algoritma dan Pemograman. YOGYAKARTA: CV ANDI OFFSET.
[6] D. KAHN, THE CODEBREAKERS. New York: Library of Congress cataloging-in-publication Data is Available.
[7] R. Sadikin, KRIPTOGRAFI UNTUK KEAMANAN JARINGAN. YOGYAKARTA: C.V ANDI OFFSET, 2012.
[8] jon E. Bella Ariska, suroso, "Rancangan Kriptografi HYBRID kombinasi metode Vigenere Cipher dan ELGAMAL Pada pengamanan pesan Rahasia," Semin. Nas. Inov. dan Apl. Teknol. di Ind., 2018.