SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Jurnal & Penelitian Teknik Informatika
Volume 2 Nomor 2, April 2018
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Penyandian Pesan Berdasarkan Algoritma RC5 dan El-Gamal

Jonas Sahang Benor Tambunan
STMIK Budi Darma Medan
Jl. SM. Raja No. 338 Sp. Limun Medan
tambunanbenor1@gmail.com

Muhammad Indra Sukmana
STMIK Budi Darma Medan
Jl. SM. Raja No. 338 Sp. Limun Medan
m.indrasukmana@gmail.com

Sri Nofrida Siregar
STMIK Budi Darma Medan
Jl. SM. Raja No. 338 Sp. Limun Medan
srinofrida40@gmail.com

Abstract **—** Keamanan dan kerahasian sebuah data atau informasi di dalam pesan teks tidak akan berguna apabila disadap oleh orang-orang tertentu yang tidak berhak atau berkepentingan. Setiap pesan yang akan dikirimkan kepada penerima harus dapat dipastikan bahwa isi pesan belum mengalami perubahan. Bila aspek keamanan pesan terabaikan, maka kerahasiaan pesan tersebut tidak akan terjamin. Penyandian pesan teks berdasarkan algoritma kriptografi RC5 yang dikombinasikan dengan El-Gamal mampu mengoptimalkan kerahasiaan pesan teks sehingga hanya dapat dimengerti oleh pihak yang dituju. Penelitian ini menguraikan penyandian pesan teks berdasarkan algoritma RC5 dan El-Gamal. Pengkombinasian dua algoritma ini dilakukan dengan mengenkripsi pesan secara ganda, yang dimulai dengan enkripsi berdasarkan RC5 kemudian *cipher* dari RC5 dienkripsi kembali berdasarkan algoritma El-Gamal, sehingga menambah kerumitan bagi penyerang dalam upaya untuk mengetahui makna pesan teks yang sebenarnya.

Keywords—kriptografi, RC5, El-Gamal, Pesan, Teks.

I. PENDAHULUAN

Pesan teks umumnya digunakan untuk menyampaikan suatu informasi dalam berkomunikasi antara pengirim dan penerima. Informasi yang dikkomunikasikan dapat saja berupa pesan penting dan rahasia atau pesan yang tidak penting. Berdasarkan penelitian terdahulu mengatakan bahwa media *internet* saat ini menjadi jalur pendistribusian pesan yang sangat vital untuk isi file yang bersifat rahasia [1]. Oleh karena itu, dibutuhkan teknik pengamanan data dengan tujuan untuk menghindari tindakan-tindakan dari pihak lain seperti penyadapan dan penyalahgunaan pesan yang sedang didistribusikan.

Pesan rahasia atau pribadi dapat diamankan dengan memanfaatkan berbagai algoritma kriptografi. Penelitian sebelumnya mengatakan bahwa salah satu ruang lingkup dari teknik kriptografi adalah distribusi informasi yang berlangsung dua arah yang terdiri dari proses enkripsi dan dekripsi[2][3]. Penelitian lain mengatakan bahwa teknik kriptografi sangat penting diimplementasikan untuk melindungi data yang ditransmisikan melalui suatu jaringan komunikasi[4].

Algoritma RC5 maupun El-Gamal merupakan algoritma kriptografi yang mampu diimplementasikan pada enkripsi dan dekripsi pesan. Algoritma RC5 memberikan akses keamanan secara akurat dan menggunakan kunci yang sama[5]. Algoritma El-Gamal mampu membangkitkan kunci yang berdasarkan logaritma diskrit yang sangat rumit untuk dipecahkan[6].

Penelitian ini menguraikan proses penyandian sebuah pesan berjenis teks berdasarkan algoritma RC5 dan El-Gamal. Proses yang dilakukan adalah menyandikan pesan secara ganda, dimana teks pesan asli dienkripsi terlebih dahulu berdasarkan algoritma RC5, kemudian *cipher* dari RC5 dienkripsi kembali berdasarkan algoritma El-Gamal. Tujuan adalah untuk menambah kerumitan kemudahan para penyerang untuk mengetahui makna asli dari pesan teks yang didistribusikan.

II. LANDASAN TEORI

A. *Kriptografi*

Kriptografi merupakan salah satu teknik yang dapat digunakan dalam menjaga dan mengamankan informasi yang bersifat pribadi atau rahasia. Kriptografi dapat berfungsi untuk merubah pesan yang terbaca (*plaintext*) menjadi pesan yang tidak

dapat dibaca (*ciphertext*), sehingga hanya pengirim dan penerima pesan yang dapat mengganti, menghapus dan membaca pesan tersebut[7][8]. Proses pengubahan *plaintext* menjadi *ciphertext* disebut dengan enkripsi sedangkan proses pengembalian *ciphertext* menjadi *plaintext* disebut dengan dekripsi. Proses pembentukan kunci sangat penting dilakukan dalam mengimplementasikan teknik kriptografi karena kunci akan digunakan dalam transformasi enkripsi dan dekripsi.

Beberapa aspek keamanan yang harus dicapai dalam mengamankan data berdasarkan teknik kriptografi, yaitu kerahasiaan (*confidentiality*), integritas data *(data integrity*), autentikasi *(authentication*), ketiadaan penyangkalan *(non-repudiation*) [9][10]. Kekuatan yang dimiliki oleh algoritma kriptografi dalam proses mengenkripsi data [11], yaitu :

1. Konfusi/pembingungan (*confusion*), yaitu suatu proses dimana teks sulit dikembalikan pada bentuk awal secara tanpa melalui proses dekripsi.
2. Difusi/peleburan *(difusion*), yaitu suatu proses dimana karakteristik suatu teks dihilangkan sehingga mengamankan suatu informasi.

B. Algoritma RC5

Algoritma RC5 adalah algoritma *block cipher* yang dirancang oleh Prof. Ronal L. Rivest dari MIT dan dipublikan pada bulan Desember 1994. RC sendiri merupakan singkatan dari *Rivest Cipher* atau *Ron's code* sejak dipublikasikan RC5 menarik perhatian para ahli dan upaya memberikan akses keamanan secara akurat[5].

Algoritma RC5 merupakan salah satu dari algoritma kriptografi primitif yang merupakan sasaran pengkajian RC5. Algoritma RC5 memiliki tiga tahap utama[1][5], yaitu :

1. *Key expansion algorithm*, yaitu proses yang dilakukan untuk membentuk tabel kunci S.
2. *Encryption algorithm*, yaitu proses untuk
3. *Decryption algorithm*, yaitu proses yang dilakukan untuk mengembalikan *ciphertext* menjadi *plaintext*.

C. Algoritma El-Gamal

Algoritma ini dibuat oleh Taher El-Gamal pada tahun 1984, dan algoritma ini termasuk algoritma asimetris. El-Gamal pada awalnya hanya digunakan untuk *digital signature*, namun dimodifikasi sehingga dapat digunakan dalam proses enkripsi dan dekripsi. Kelebihan El-Gamal dibandingkan algoritma yang lain yaitu memiliki kunci publik berupa tiga pasang bilangan dan kunci rahasia berupa dua bilangan[12]. Algoritma ini memberikan *cipher* teks yang berbeda setiap kali proses plainteks tersebut dienkripsi.

III. METODE PENELITIAN

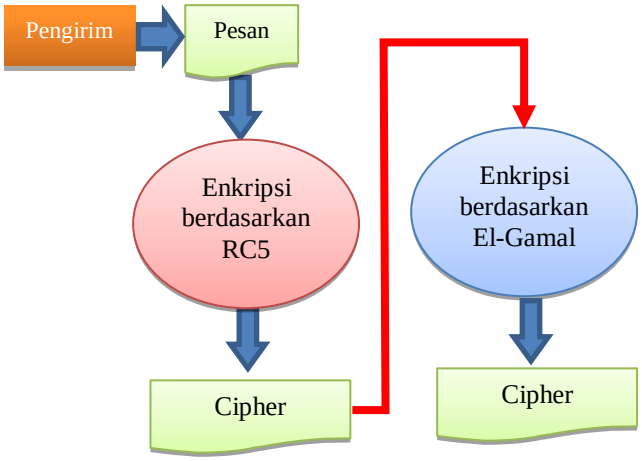
Metode penelitian yang digunakan dalam pelaksanaan penelitian adalah :

1. Studi Pustaka
   Mencari dan mempelajari berbagai referensi yang relefan dengan keamanan data serta algoritma El-Gamal dan RC5.
2. Analisa Masalah
   Mengidentifikasi permasalahan yang timbul dalam hal pengamanan pesan teks yang sifatnya penting dan rahasia agar dapat ditentukan solusi penyelesaiannya.
3. Desain Sistem
   Mendesain *layout* sistem yang digunakan untuk mengimplementasikan pengamanan pesan teks.
4. Implementasi dan Pengujian
   Mengimplementasikan pengamanan pesan teks berdasarkan desain yang telah dibuat sebelumnya menggunakan bahasa pemrograman serta melakukan pengujian apakah sistem telah berjalan dengan baik atau tidak.

IV. PEMBAHASAN

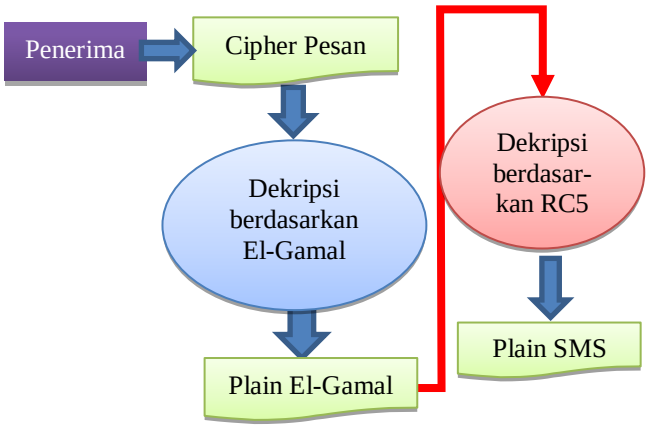
Masalah pengamanan pesan teks yang bersifat penting dan rahasia memang menjadi salah satu aspek utama dalam berkomunikasi. Berdasarkan uraian pada pendahuluan bahwa penerapan algoritma kriptografi menjadi salah satu solusi untuk menangani permasalahan tersebut. Kriptografi mampu meminimalisir tindakan-tindakan penyalahgunaan pesan yang bersifat rahasia dan penting dari tindakan pihak-pihak yang tidak bertanggungjawab dengan cara menyandikan pesan tersebut ke bentuk lain berupa sandi (simbol-simbol) yang jauh berbeda dengan simbol-simbol pesan aslinya. Hal inilah yang dapat mempersulit para penyerang untuk mengetahui dengan mudah makna dari pesan yang didistribusikan.

Skema penerapan dua algoritma ini dalam penyandian pesan teks dapat diilustrasikan pada gambar di bawah ini.



Gambar 1. Skema Enkripsi Pesan Penerapan RC5 dan El-Gamal

Berdasarkan gambar 1 di atas, diketahui bahwa sebelum pesan didistribusikan kepada penerima, maka pesan tersebut disandikan terlebih dahulu. Proses penyandian diawali dengan menggunakan algoritma RC5, kemudian *cipher* yang dihasilkan dari algoritma RC5 dienkripsi kembali berdasarkan algoritma El-Gamal. *Cipher* yang dihasilkan dari algoritma El-Gamal adalah *cipher* akhir yang distribusikan kepada penerima.



Gambar 2. Skema Dekripsi Pesan Penerapan RC5 dan El-Gamal

Berdasarkan gambar 2 di atas, terlihat bahwa proses dekripsi merupakan kebalikan dari proses dekripsi. Dekripsi diawali dengan mendekripsi *cipher* pesan berdasarkan algoritma El-Gamal, kemudian *plain* tersebut didekripsi kembali berdasarkan algoritma RC5 hingga didapatkan *plain* pesan asli.

1. Proses Penyandian Pesan berdasarkan Algoritma RC4

   Berdasarkan uraian pada teoritis bahwa proses enkripsi berdasarkan algoritma RC5 diawali oleh proses peruasan kunci. Proses *key expansion* (perluasan kunci) membutukan dua nilai konstanta yaitu P dan Q yand didapatkan dari fungsi yang melibatkan bilangan irasional, dimana :

   $P = Odd[(e - 2)2^w]$ dan $Q = Odd[(f - 1)2^w]$

   e = 2.718281828459.....

   f = 1.618033988749....

   Proses pembentukan kuci dilakukan dengan membuat *array* kunci K[0-1] ...K[b], kemudian isi *array* K disalin ke dalam array L[0-1] ... L[b] yang di-*padding* dengan karakter 0 hingga ukuran L[i] menjadi w/2 bit.

   Inisialisasi tabel kunci internal dengan ukuran t = 2r + 2, yang dilakukan dengan *pseudocode* :

```
P = KI[0]
for i = 1 to t – 1 do
    KI[i] = KI[i – 1]
end for
```

   Nilai S dan L digabungkan berdasarkan *pseudocode* berikut :

```
i = 0 ; j = 0; X = 0 ; Y =  0 ; n = 3*max(r,c)
for k = 1 to  n do
    KI[i]= (KI[i] + X + Y)<<< 3
    X = KI[i]
    i  = (i + 1) mod t
    L[j] = L[j] + X + Y)<<< 3
    Y = L[j]
    j  =(j + 1) mod c
endfor
```

   nilai *max* (r,c) merupakan fungsi penentuan bilangan terbesar antara r dan c, sedangkan c adalah nilai maksimum dari panjang kunci b/4.

   Selanjutnya adalah melakukan proses enkripsi terhadap teks pesan. Proses enkripsi dilakukan dengan menggunakan dua buah blok input A dan B sebagai *word* sebesar 32 bit yang telah dihasilkan dari proses konversi pada *file input* kedalam 32 bit *array of integer*. Enkripsi akan dilakukan berdasarkan *pseudocode* berikut :

```
A = A + KI[0]
B = B + KI[1]
for i =  to r do
    A = ((A ⊕ B) <<< B) + KI[2i]
    B = ((B ⊕ A) <<< A) + KI[2i+1]
endfor
```

   Cipher yang dihasilkan pada proses enkripsi berdasarkan algoritma RC5 inilah yang digunakan sebagai input *plain* pada proses enkripsi berdasarkan algoritma El-Gamal.

   Proses dekripsi berdasarkan algoritma RC5 merupakan kebalikan dari algoritma enkripsi. Bila pada proses enkripsi terdapat pergeseran ke kiri,

maka pada proses dekripsi dilakukan pergeseran ke kanan. *Pseudocode* untuk melakukan proses dekripsi adalah :

```
for i = r downto 1 do
    B = ((B – KI[2i+1])>>>A) ⊕ A
    A = ((A – KI[2i])>>>B) ⊕ B
endfor
B = B - KI[1]
A = A - KI[0]
```

2. Proses Penyandian Cipher Hasil Enkripsi RC5 berdasarkan Algoritma El-Gamal

Algoritma El-Gamal dalam menyandikan pesan, akan melakukan proses pembangkitan kunci *public* dan *private*. Proses pebangkitan kunci ini dilakukan oleh pihak penerima pesan, dimana kunci publiknya akan dibagikan kepada pengirim pesan.

Proses awal yang dilakukan adalah proses pembentukan kunci yang terdiri dari kunci rahasia dan kunci publik. Pada proses ini bilangan prima *p* dibutuhkan untuk membentuk element primitif α dan semabarng a€{0,1,…, *p*– 2}. Kunci publik algoritma el – gamal mempunyai tiga pasangan bilangan, antara lain (*p*, α, β,), dengan

$$\beta = \alpha^a \bmod p$$

dimana a adalah kunci rahasianya.

Diasumsikan contoh di bawah ini :
p = 257
g = 11
x = 13

Kemudian p, g, x digunakan untuk menghitung y :
y = g x mod p
y = 1113 mod 257
y = 22

Maka kunci *public* A adalah y = 22, g = 11, p = 257 dan kunci *private* A adalah x =13, p = 257.

Perhitungan Enkripsi, Misalkan B ingin mengirim plainteks **ENKRIPSI** kepada A, kemudian setiap karakter plainteks tersebut diubah kedalam bentuk ASCII sehingga menghasilkan tabel sebagai berikut :
Rubah teks pesan ke nilai desimal ASCII :
E =69, N =78; K = 75; R = 82; I = 73;
P = 80; S = 83; I = 73

Kemudian nilai ASCII tersebut dimasukkan kedalam blok-blok nilai m secara berurutan, sehingga menjadi :
m1 = 69, m2 = 78, m3 = 75, m4 =82, m5 = 73, m6 = 80, m7 = 83, m8 = 73.

Kemudian B memilih bilangan acak k untuk masing-masing nilai m dimana nilai ki ini bernilai 0 < k < p -1. Sehingga diambil nilai acak k untuk masing-masing nilai m sebagai berikut :

Pn	Nilai	ki
P1	69	58
P2	78	178
P3	75	251
P4	82	62
P5	73	137
P6	80	27
P7	83	256
P8	73	173

Kemudian B menghitung :
Perhitungan a :
a = g^k mod p

Nilai P1 :
a1 = gk mod p
a1 = 1158 mod 257
a1 = 30

Nilai P2 :
a2 = gk mod p
a2 = 11178 mod 257
a2 = 137

Nilai P3 :
a3 = gk mod p
a3 = 11251 mod 257
a3 = 73

Nilai P4 :
a4 = gk mod p
a4 = 1162 mod 257
a4 = 17

Nilai P5 :
a5 = gk mod p
a5 = 11137 mod 257
a5 = 190

Nilai P6 :
a6 = gk mod p
a6 = 1127 mod 257
a6 = 184

Nilai P7 :
a7 = gk mod p
a7 = 11256 mod 257
a7 = 1

Nilai P8 :
a8 = gk mod p
a8 = 11173 mod 257
a8 = 235

Perhitungan bi :
bi = yk. m mod p

Nilai P1 :
b1 = yk m mod p
b1 = 2258.69 mod 257
b1 = 201

Nilai P2 :
b2 = yk m mod p
b2 = 22178.78 mod 257
b2 = 82

Nilai P3 :
b3 = yk m mod p
b3 = 22251.75 mod 257
b3 = 147

Nilai P4 :
b4 = yk m mod p
b4 = 2262.82 mod 257
b4 = 220

Nilai P5 :
b5 = yk m mod p
b5 = 22137.73 mod 257

Nilai P6 :
b6 = yk m mod p
b6 = 2227.80 mod 257

b5 = 16 b6 = 203

Nilai P7 :
b7 = yk m mod p
b7 = 22256.83 mod 257
b7 = 83

Nilai P8 :
b8= yk m mod p
b8 = 22173.73 mod 257
b8 = 249

Setelah mendapatkan nilai a dan b, hasil perhitungan tersebut disusun dengan pola a1, b1, a2, b2, a3,b3, a4, b4, a5, b5, a6, b6, a7, b7, a8, b8. Sehingga diperoleh nilai desimal chipher pesan adalah 30 201 137 82 73 147 17 220 190 16 184 203 1 83 235 249.

3. Proses Dekripsi

Berdasarkan diagaram skema dekripsi (gambar 2), bahwa proses dekripsi dilakukan secara terbalik yaitu dimulai dari proses dekripsi *cipher* pesan berdasarkan algoritma El-Gamal, kemudian plain yang didapatkan didekripsi kembali berdasarkan algoritma RC5 untuk menghasilkan *plain* pesan.

Kunci yang digunakan pada proses dekripsi berdasarkan algoritma El-Gamal adalah kunci private yang dibangkitkan sendiri oleh penerima pesan pada saat pembentukan kunci publik yang telah dibagikan kepada pengirim pesan sebelumnya. Kunci *private* yang digunakan dapat berperan sebagai pemeriksa authentikasi dan keaslian pesan yang diterima apakah benar dienkripsi oleh orang yang benar dan menggunakan kunci publik yang benar sesuai dengan kunci yang dibagikan sebelumnya.

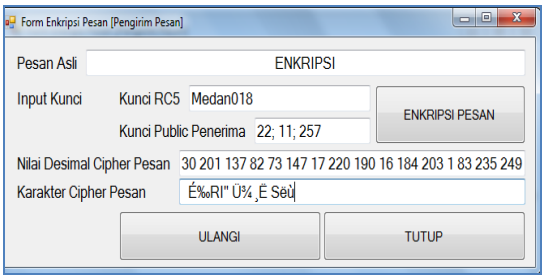
Setelah proses dekripsi berdasarkan El-Gamal dilakukan, maka dilanjutkan dengan dekripsi berdasarkan algoritma RC5 hingga dihasilkan teks pesan asli.

V. IMPLEMENTASI

Berdasarkan analisa dan desain sistem yang telah dilakukan, maka hasil implementasi pengamanan pesan berdasarkan algoritma RC5 dan El-Gamal ditunjukkan pada gambar berikut.

1. Implementasi Proses Enkripsi

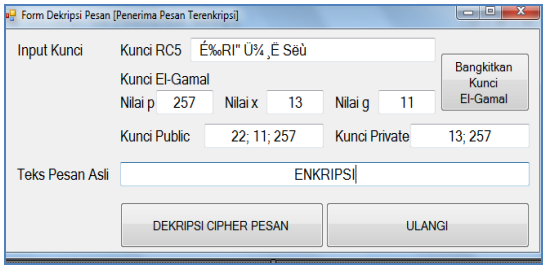
Proses implementasi proses dilakukan oleh pengirim pesan. Enkripsi diawali dengan menginput pesan yang akan dienkripsi, kemudian menginput nilai kunci RC5 dan kunci publik penerima pesan. Selanjutnya adalah melakukan proses enkripsi sehingga didapatkan *cipher* dari pesan asli. Implementasi dari proses enkripsi ditunjukkan pada gambar 3 berikut ini.



Gambar 3. Implementasi Proses Enkripsi

2. Implementasi Proses Dekripsi

Proses dekripsi diawali dengan menginput *cipher* dari pesan, kemudian menginput kunci RC5 (sama seperti kunci pada proses enkripsi, karena algoritma ini tergolong algoritma kunci simetris) sedangkan nilai kuci El-Gamal pada saat melakukan proses dekripsi yang digunakan oleh penerima pesan adalah kunci *private*. Tampilan implementasi ditunjukkan pada gambar 4 berikut ini.



Gambar 4. Implementasi Proses Dekripsi

VI. KESIMPULAN

Berdasarkan uraian pembahasan penelitian ini, maka disimpulkan beberapa hal sebagai berikut :

1. Pengkombinasian algoritma RC5 dan El-Gamal dalam penyandian pesan cukup member hasil yang sinifikant dan mampu mewujudkan prinsif pembingungan dan pengaburan makna pesan asli untuk mempersulit para penyerang untuk mengetahui makna asli dari pesan.
2. Pengkombinasian algoritma RC5 dan El-Gamal, membutuhkan waktu yang lama karena proses enkripsi dan dekripsi dilakukan secara ganda.

REFERENSI

[1] S.H. Suryawan, Hamdani, "Pengamanan Data File Dengan Menggunakan Algoritma Enkripsi Rivest Code 5 ," *Jurnal Informatika Mulawarman* , vol.8, no. 2 , pp. 44-49, Juli 2013.

[2] E. Setyaningsih, *Kriptografi & Implementasinya Menggunakan Matlab*, Yogyakarta:Andi, 2015.

[3] T. Zebua and E. Ndruru, "Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4," *J. Teknol. Infomasi dan Ilmu Komput.*, vol. 4, no. 4, pp. 275–282, Desember 2017.

[4] E. Setyaningsih, "Penyandian Citra Menggunakan Metode Playfair Cipher", J. Teknol., vol. 2, no. 2, pp. 213–219, 2009.

[5] Hamdani, S.H. Suryawan, A. Septiarini,"Pengujian Algoritma Rivest Code 5 Untuk Enkripsi Struktur File Dokumen," *Jurnal Informatika Mulawarman*, vol. Vol. 8 No. 2, pp. 44-49, Juni 2013.
[6] B. Parmadi, "Implementasi Algoritma Kriptografi Elgamal pada Data Text," *J. Inf. Technol.*, vol. 5, no. 1, pp. 1–5, Juni 2017.
[7] F. Azmi and R. Anugrahwaty, "Analisis Matriks 5x7 Pada Kriptografi Playfair Cipher," *J. Penelit. Tek. Inform.*, vol. 1, no. 2, pp. 27–30, April 2017.
[8] Rifki Sadikin, *Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*, Yogyakarta: Andi, 2012.
[9] T. Zebua, "Penerapan Metode LSB-2 untuk Menyembunyikan Ciphertext pada Citra Digital," *Pelita Inform. Budi Darma*, vol. 10, no. 3, pp. 135–140, 2015.
[10] H. Pandiangan and S. Sijabat "Perancangan Media Pengiriman Pesan Teks Dengan Penyandian Pesan Menggunakan Algoritma RC4 Berbasis Web," *Jurnal Matik Penusa* , vol. XIX, no.1, pp. 63-71, Juni 2016
[11] T. Zebua, "Analisa dan Implementasi Algoritma Triangle Chain Pada Penyandian Record Database," *Pelita Inform. Budi Darma*, vol. 3, no. 2, pp. 37–49, April 2013.
[12] D. Suhendri, "Menggunakan Vigenere Cipher dan Algoritma El-Gamal," *J. INFOTEK*, vol. 1, no. 3, pp. 1–6, Oktober 2016.