Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 32-38
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Analisa Keamanan Data Teks Dengan Menerapkan Kriptografi RSA dan Steganografi LSB

Lindia Ali Fitriani

Prodi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Email: lindiaaf@gmail.com

Abstrak−Untuk berbagai alasan, keamanan dan kerahasiaan sangat dibutuhkan dalam komunikasi data. Terdapat beberapa usaha untuk menangani masalah keamanan data rahasia yang dikirimkan melalui Internet, diantaranya adalah menggunakan teknik kriptografi dan steganografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Teknik kriptografi dapat menimbulkan kecurigaan pada pihak ketiga yang tidak berhak menerima informasi karena pesan disamarkan dengan cara mengubah pesan yang asli menjadi seolah-olah tidak terbaca. Selanjutnya pihak ketiga tersebut akan memiliki keinginan untuk mengetahui isi pesan rahasia tersebut dan berusaha memecahkan informasi yang sebenarnya. Sedangkan steganografi lebih mengurangi kecurigaan karena pesan yang disamarkan disembunyikan ke dalam pesan lainnya. Steganografi dapat menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan. Hal ini dikarenakan hasil keluaran steganografi adalah data yang memiliki bentuk persepsi yang sama dengan data aslinya apabila dilihat menggunakan indera manusia dalam kriptografi dapat dilihat dan disadari langsung oleh indera manusia. Pada steganografi, data rahasia disisipkan pada data lain yang disebut cover-object dan menghasilkan stego-object (hasil steganografi). Untuk mengamankan pesan dengan teknik steganografi digunakan steganografi LSB dan menggunakan metode RSA.

Kata Kunci: Kriptografi, Steganografi, Metode RSA dan LSB.

Abstract−For various reasons, security and confidentiality are needed in data communication. There have been several attempts to deal with the issue of security of confidential data sent over the Internet, including using cryptographic and steganographic techniques. Cryptography is the science and art of maintaining the confidentiality of a message by encoding it in a form that cannot be understood anymore. Cryptographic techniques can arouse suspicion of third parties who are not entitled to receive information because the message is disguised by changing the original message as if it were unreadable. Furthermore, the third party will have the desire to find out the contents of the secret message and try to solve the real information. Whereas steganography further reduces suspicion because a message disguised is hidden in other messages. Steganography can disguise messages into a media without other people realizing that the media has inserted a message. This is because the output of steganography is data that has the same form of perception as the original data when viewed using human senses in cryptography can be seen and realized directly by the human senses. In steganography, confidential data is inserted into other data called cover-objects and produce stego-objects (the results of steganography). To secure messages using steganography techniques LSB steganography is used and uses the RSA method.

Keywords: Cryptography, Steganography, RSA and LSB Methods.

1. PENDAHULUAN

Saat ini, teknologi komunikasi dan informasi berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Contoh dari perkembangan ini adalah jaringan *internet*, yang pada saat ini telah memungkinkan banyak orang untuk saling bertukar data secara bebas melalui jaringan tersebut. Karena kemudahan yang dimilikinya, *internet* sudah berkembang menjadi salah satu media yang paling populer di dunia. Namun, kemudahan ini juga dimanfaatkan oleh sebagian pihak yang mencoba untuk melakukan kejahatan. Dengan berbagai teknik, banyak yang mencoba untuk mengakses informasi yang bukan haknya. Oleh karena itu, sejalan dengan berkembangnya media *internet* ini harus juga dibarengi dengan perkembangan sisi keamanan.

Untuk berbagai alasan, keamanan dan kerahasiaan sangat dibutuhkan dalam komunikasi data. Terdapat beberapa usaha untuk menangani masalah keamanan data rahasia yang dikirimkan melalui *internet*, diantaranya adalah menggunakan teknik kriptografi dan steganografi. Teknik pengamanan data sudah banyak dikembangkan pada saat ini, hal tersebut tentu semakin memudahkan semua pihak dalam melakukan pengamanan data. Salah satu yang banyak dipergunakan saat ini adalah sistem pengamanan berbasis komputerisasi yang dapat dipergunakan kapan saja dan dimana saja. Pada kriptografi, terdapat proses enkripsi yang mengubah teks polos menjadi *ciphertext* dan proses *dekripsi* yang mengubah *ciphertext* menjadi teks polos kembali algoritma ini juga dapat memanfaatkan kunci yang dimasukkan dari luar. Teknik kriptografi dapat menimbulkan kecurigaan pada pihak ketiga yang tidak berhak menerima informasi karena pesan disamarkan dengan cara mengubah pesan yang asli menjadi seolah-olah tidak terbaca. Selanjutnya pihak ketiga tersebut akan memiliki keinginan untuk mengetahui isi pesan rahasia tersebut dan berusaha memecahkan informasi yang sebenarnya.

RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 32-38
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (sehingga disebut dengan kunci publik), namun kunci untuk dekripsi bersifat rahasia (kunci privat). Untuk menemukan kunci dekripsi, dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya. Kenyataannya, memfaktorkan bilangan bulat menjadi faktor primanya bukanlah pekerjaan yang mudah. Karena belum ditemukan algoritma yang efisien untuk melakukan pemfaktoran. Cara yang bisaa digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor. Jika semakin besar bilangan yang akan difaktorkan, maka semakin lama waktu yang dibutuhkan. Jadi semakin besar bilangan yang difaktorkan, semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA [2].

Sedangkan steganografi lebih mengurangi kecurigaan karena pesan yang disamarkan disembunyikan ke dalam pesan lainnya. Steganografi dapat menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan. Hal ini dikarenakan hasil keluaran steganografi adalah data yang memiliki bentuk persepsi yang sama dengan data aslinya apabila dilihat menggunakan indera manusia. Sedangkan perubahan pesan

dalam kriptografi dapat dilihat dan disadari langsung oleh indera manusia. Pada steganografi, data rahasia disisipkan pada data lain yang disebut *cover-object* dan menghasilkan *stego-object* (hasil steganografi). Media penampung yang umum digunakan pada teknik steganografi adalah citra, suara, video, atau teks. Adapun data yang disimpan juga dapat berupa citra, suara, video, teks, atau pesan lain. Pada penelitian ini, steganografi yang diterapkan adalah steganografi pada dokumen citra. Ada banyak metode yang digunakan untuk steganografi pada dokumen citra seperti metode *Least Significant Bit (LSB), Spread Spectrum Steganography.* Metode steganografi yang digunakan pada penelitian ini adalah *Least Significant Bit* (LSB) dan RSA.

Salah satu metode *steganografi* adalah LSB (*Least Significant Bit*). Langkah digunakan yaitu dengan menyisipkan *bit* terakhir (*least*) pada setiap *pixel* dengan *bit* pesan. Penyisipan pada LSB akan merubah nilai *bit*, tetapi tidak tampak kasat mata, sehingga pihak ketiga tidak mengetahui adanya pesan rahasia dibalik media *cover* [1].

Metode yang paling banyak digunakan untuk melakukan steganografi adalah *Least Significant Bit* (LSB). Penelitian mengenai steganografi teknik LSB pernah dilakukan oleh beberapa orang. Di antaranya, yang membahas steganografi LSB menggunakan media *file* gambar *Graphical Interchange Format* (gif). Namun demikian, steganografi LSB ini perlu diteliti, tentang bagaimana kemampuan metode sekuensial (berurutan) dan *random* (acak) dalam menyisipkan pesan. Untuk mengukur kemampuan tersebut, dibutuhkan alat ukur yang akan digunakan sebagai parameter analisis secara kuantitatif [2].

2. METODOLOGI PENELITIAN

2.1 Steganografi

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan di dalam pesan lain sehingga keberadaan pesan yang pertama tidak diketahui. Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos*, yang artinya “tersembunyi” atau “terselubung”, dan *graphein*, yang artinya “menulis” sehingga kurang lebih artinya adalah "menulis (tulisan) terselubung" [4]. Steganografi membutuhkan dua properti yaitu wadah penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara (*audio*), teks atau video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video.

2.2 Metode RSA

Sandi RSA merupakan algoritma kriptografi kunci publik (asimetris). Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (sehingga disebut dengan kunci publik), namun kunci untuk dekripsi bersifat rahasia (kunci privat). Untuk menemukan kunci dekripsi, dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya. Kenyataannya, memfaktorkan bilangan bulat menjadi faktor primanya bukanlah pekerjaan yang mudah. Karena belum ditemukan algoritma yang efisien untuk melakukan pemfaktoran. Cara yang bisaa digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor. Jika semakin besar bilangan yang akan difaktorkan, maka semakin lama waktu yang dibutuhkan. Jadi semakin besar bilangan yang difaktorkan, semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA [3].
Besaran-besaran yang digunakan pada algoritma RSA:

1. p dan q bilangan prima (rahasia)
2. r = p . q (tidak rahasia)
3. ϕ (r) = (p – 1)(q – 1) (rahasia)
4. PK (kunci enkripsi) (tidak rahasia)
5. SK (kunci dekripsi)

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 32-38
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

6. X (*plainteks*) (rahasia)
Y (*cipherteks*) (rahasia)

2.3 *Least Significant Bit*

Salah satu metode steganografi adalah LSB (*Least Significant Bit*). Langkah digunakan yaitu dengan menyisipkan bit terakhir (least) pada setiap pixel dengan bit pesan. Penyisipan pada LSB akan merubah nilai bit, tetapi tidak tampak kasat mata, sehingga pihak ketiga tidak mengetahui adanya pesan rahasia dibalik media *cover* [1]. Terdapat dua langkah dalam sistem steganografi yaitu proses penyembunyian (*embedding*) dan ekstraksi data dari berkas penampung. Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Pada susunan bit di dalam sebuah *byte* (1 byte = 8 bit), ada *bit* yang paling berarti (*most significant bit*) dan *bit* yang paling kurang berarti (*least significant bit*). *Bit* yang cocok untuk diganti adalah *bit* LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil [2][13].

3. HASIL DAN PEMBAHASAN

Sebelum Proses perancangan dimulai, maka diperlukanlah beberapa analisis terhadap sistem, metode ataupun teknik-teknik yang digunakan dalam tahap perancangan.Analisa dapat memberi uraian secara utuh tentang masalah yang sedang di analisa dengan melalukan identifikasi dan evaluasi terutama hambatan-hambatan yang terjadi serta kebutuha dalam memberi silusi penyelesaian masalah yang sedang dibahas.

Pada tahap ini, kita akan melihat bagaimana cara kerja metode RSA dalam mengkodekan karakter yang akan kita watermaking. *Plainteks* akan di enkripsi adalah : SAY

1. Proses Pembentukan Kunci
   a. Menentukan 2 bilangan prima sembarang dan acak yang diwakilkan oleh variable p dan variabel q. Misalkan $p = 13$ dan $q = 17$
   b. Menghitung (RSA) modulus (n) dengan formula n = p * q, dimana nilai p = 13 dan nilai q = 17.
      n = p*q
      n = 13*17
      n = 221
   c. Menghitung nilai m yang akan digunakan untuk mencari (RSA) *enciphering exponet* (e).
      m = (p – 1) * (q – 1)
      m = (13 – 1) * (17 – 1)
      m = (12) * (16)
      m = 192
   d. Menghitung nilai *e* dengan formula : gcd(e,m) = 1, dengan syarat e = bilangan prima dan 1 < e < m. dimisalkan e = 5, maka formula gcd(5,192) = 1 bernilai *true*.
   e. Menghitung nilai (RSA) *deciphering exponent* (d) dengan menggunakan formula e * d = 1 mod (m), dimana nilai e dan m didapatkan dari langkah sebelumnya e = 5 dan m = 192.
      e * d = 1 mod (m)
      d = 1 + (k * m) / e
      d = 1 (k * 192) /5
      dengan nilai k = *integer* sembarang, maka dimisalkan nilai d yang akan diambil adalah d yang bernilai *integer*. Nilai d yang diambil kali ini adalah d = 77.
   f. Dari langkah diatas, nilai n, e, dan d telah ditemukan yang berarti juga pasangan kunci telah terbentuk. Pasangan kunci publik (n,e) = (221, 5) Pasangan kunci rahasia (n,d) = (221, 77)
2. Dimisalkan terdapat himpunan karakter : “SAY” yang akan disandikan menggunakan kunci yang telah dibentuk pada langkah sebelumnya, maka terlebih dahulu karakter tersebut dikonversi kedalam bentuk numerik, proses konversi bisa menggunakan teknik tersendiri dari penggunaan atau menggunakan tabel ASCII decimal berikut :

Tabel 1. Koversi char SAY ke ASCII Desimal

Char	Ascii Desimal
S	83
A	65
Y	89

Dari tabel 1. hasil konversi setiap baris dijadikan satu deret, akan menghasilkan plaintext ASCII decimal (M) dari karakter yang akan dienkrip sebagai berikut : M = 836589

3. Untuk menjalankan proses enkripsi, digunakan kunci publik yang telah dibentuk sebelumnya yaitu kunci publik (221,5), dengan formula $C = M^e \bmod N$. Namun sebelum melakukan perhitungan, terlebih dahulu

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 32-38
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

dilakukan pemecahan deret plaintext ASCII menjadi blok yang panjang digit setiap bloknya kurang dari panjang digit n. Pada contoh kali ini, (RSA) modulus yang digunakan adalah = 221 (2 digit), jadi untuk setiap blok dibatasi maksimal 2 digit per blok. Dilakukan pemenggalan 3 digit per blok karena karakter yang digunakan dalam proses enkripsi adalah karakter ASCII yang setiap karakternya 8 bit, agar maksimal bit 8 digit (2^3). Hasil perhitungan enkripsi dengan formula $C = M^e \bmod N$ terlihat pada tabel 2. dibawah ini.

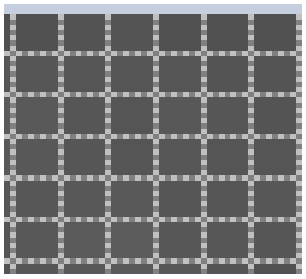
Tabel 2. Hasil Enkripsi

Blok ke	M	e	n	C
1	83	5	221	96
2	65	5	221	78
3	89	5	221	102

Metode *least significant bit* merupakan teknik penyembunyian data dengan mengganti bit-bit data dalam segmen sebuah citra dengan bit-bit rahasia dari data yang disembunyikan. Setelah kata dikodekan dengan algoritma RSA, hasil pengkodean tersebut akan disisipkan ke dalam citra/gambar dengan menggunakan metode *least significant bit*.

Adapun proses penyisipan kata tersebut adalah sebagai berikut : contoh :

Pada citra 6x6 piksel akan disisipkan pesan yaitu " ‘ N f ". Pesan yang disisipkan dirubah dalam bentuk bilangan ASCII. Bilangan ASCII dari pesan " ‘ N f " adalah ‘=96, N=78, f=102. Kemudian bilangan ASCII tersebut dirubah dalam bilangan biner yaitu ‘=01100000, N=01001110, f=01100110. Berikut citra 6 x 6 pixel :



Gambar 1. Citra 6 x 6 pixel

Kemudian merubah nilai derajat keabuan citra ke dalam bentuk desimal. Berikut nilai derajat keabuan citra tersebut :

Tabel 3. Nilai Derajat Keabuan

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	99	125	190	200

Nilai derajat keabuan citra diatas akan dirubah ke dalam bilangan biner, sebagai berikut :

11000100	00001010	01100001	10110110	01100101	00101000
01000011	11001000	01100100	00110010	01011010	00110010
00011001	10010110	00101101	11001000	01001011	00011100
10110000	00111000	01001101	01100100	00011001	11001000
01100101	00100010	11111010	00101000	01100100	00111100
00101100	01000010	01100011	01111101	10111110	11001000

Kemudian akan dilakukan proses penyisipan sesuai dengan algoritma metode *least significant bit*. Bit yang akan disisipkan adalah ‘=01100000, N=01001110, f=01100110.

a. Blok 1 = 11000100disisipkan adalah "0".
   Data : 11000100
   255 : 11111111 di AND kan
   Hasil 1 : 11000100,**0** di OR kan
   Data baru : 11000100
b. Blok 2 = 00001010disisipkan adalah "1".
   Data : 00001010
   255 : 11111111 di AND kan
   Hasil 1 : 00001010,**1** di OR kan

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 32-38
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Data baru : 00001011

c. Blok 3 = 01100001disisipkan adalah "1".
Data : 01100001
255 : 11111111 di AND kan
Hasil 1 : 01100001,**1** di OR kan
Data baru : 00001011

d. Blok 4 = 10110110disisipkan adalah "0".
Data : 10110110
255 : 11111111 di AND kan
Hasil 1 : 10110110,**0** di OR kan
Data baru : 10110110

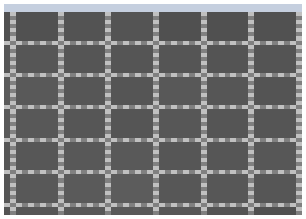
e. Blok 5 = 01100101disisipkan adalah "0".
Data : 01100101
255 : 11111111 di AND kan
Hasil 1 : 01100101,**0** di OR kan
Data baru : 01100100

Dari proses kerja atau algoritma dari metode *least significant bit* di atas dapat kita lihat bahwa metode ini melakukan penyisipan pada akhir bit dengan menggantikan nilai bit citra dengan bit data yang disisipkan. Hasilnya sebagai berikut :

11000100	00001011	01100001	10110110	01100100	00101000
01000010	11001000	01100100	00110011	01011010	00110010
00011001	10010111	00101101	11001000	01001010	00011101
10110001	00111000	01001100	01100101	00011001	11001000
01100101	00100010	11111010	00101000	01100100	00111100
00101100	01000010	01100011	01111101	10111110	11001000

Dalam bilangan desimal, maka hasilnya sebagai berikut :

196	11	97	182	100	40
66	200	100	51	90	50
25	151	45	200	74	29
177	56	76	101	25	200
101	34	250	40	100	60
44	66	99	125	190	200



Gambar 2. Stegano Image 6x6 Pixel

Pada tahap *retrieve* merupakan tahap ekstraksi pesan rahasia dari *stego image* yang akan menampilkan pesan rahasia yang terdapat pada *file* citra tersebut. Berdasarkan proses penyisipan pada tahap penyisipan, maka kata yang disisipkan akan diekstrak dari nilai biner derajat keabuan citra tersebut. Proses ekstraksikata sebagai berikut :

a. Blok 1 = 11000100 AND **0 = 0** x 2^7 = 0
b. Blok 2 = 00001011 AND **1 = 1** x 2^6 = 64
c. Blok 3 = 01100001 AND **1 = 1** x 2^5 = 32
d. Blok 4 = 10110110 AND **0 = 0** x 2^4 = 0
e. Blok 5 = 01100100 AND **0 = 0** x 2^3 = 0
f. Blok 6 = 00101000 AND **0 = 0** x 2^2 = 0
g. Blok 7 = 01000010 AND **0 = 0** x 2^1 = 0
h. Blok 8 = 11001000 AND **0 = 0** x 2^0 = 0

96 = '

i. Blok 9 = 01100100 AND **0 = 0** x 2^7 = 0
j. Blok 10 = 00110011 AND **1 = 1** x 2^6 = 64
k. Blok 11 = 01011010 AND **0 = 0** x 2^5 = 0
l. Blok 12 = 00110010 AND **0 = 0** x 2^4 = 0
m. Blok 13 = 00011001 AND **1 = 1** x 2^3 = 8
n. Blok 14 = 10010111 AND **1 = 1** x 2^2 = 4
o. Blok 15 = 00101101 AND **1 = 1** x 2^1 = 2
p. Blok 16 = 11001000 AND **0 = 0** x 2^0 = 0

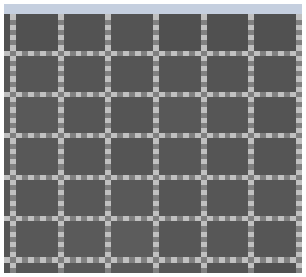
78 = N

q. Blok 17 = 01001010 AND **0 = 0** x 2^7 = 0
r. Blok 18 = 00011101 AND **1 = 1** x 2^6 = 64
s. Blok 19 = 10110001 AND **1 = 1** x 2^5 = 32
t. Blok 20 = 00111000 AND **0 = 0** x 2^4 = 0

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 2, Februari 2020, Page 32-38
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

u. Blok 21 = 0100110**0** AND **0** = **0** x 2^3 = 0
v. Blok 22 = 0110010**1** AND **1** = **1** x 2^2 = 4
w. Blok 23 = 0001100**1** AND **1** = **1** x 2^1 = 2
x. Blok 34 = 1100100**0** AND **0** = **0** x 2^0 = 0

102=f



Gambar 3. Citra 6x6 Pixel

Pada tahap ini, kita akan melihat bagaimana cara kerja metode RSA mengdekripsi karakter yang akan kita ekstrak, proses dekripsi dapat dilihat pada proses dibawah ini.
Chiperteks : ‘ N f
Chiperteks di atas akan didekripsi dengan menggunakan algoritma RSA, untuk proses dekripsinya dilakukan dengan cara berikut :

Tabel 4. Cipherteks

Blok ke	C
1	96
2	78
3	102

Untuk membuktikan pasangan kunci publik dan kunci rahasia berjalan sempurna, dicoba untuk mendekrip *ciphertext* yang telah dienkripsi sebelumnya. Proses dekripsi menggunakan kunci rahasia (221, 77), dengan formula $M = C^d \bmod N$. Hasil Perhitungan untuk proses dekripsi ditunjukkan pada tabel 3.5 dibawah ini.

Tabel 5. Hasil Dekripsi

Blok ke	C	d	n	M
1	96	77	221	83
2	78	77	221	65
3	102	77	221	89

Maka untuk *plainteks* menjadi : S A Y

4. KESIMPULAN

Berdasarkan hasil penelitian analisa dan juga berdasarkan data dan hasil perancangan maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Aplikasi pengamanan data menggunakan algoritma *RSA* mempunyai dua teknik pembacaan yaitu teknik enkripsi (mengubah *file* asli menjadi *file* yang tidak dapat dibaca) dan teknik dekripsi (mengubah *file* yang tidak dapat dibaca menjadi *file* asli).
2. Pesan rahasia berupa text disandikan dengan menggunakan algoritma enkripsi RSA dan disisipkan kedalam file gambar dengan menerapkan steganografi LSB.
3. Visual Basic menyediakan objek-objek yang sangat kuat, berguna, dan mudah dipakai. Dengan fasilitas tersebut saya menggunakannya untuk merancang aplikasi pengamanan data text.

REFERENCES

[1] Zebua, T, Nduru, E. 2017,*"Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4",* Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), Vol. 4 No. 4, pp. 279-282, e-ISSN : 2528-6579
[2] Zebua. T, 2018, *"Encoding The Record Database Of Computer Based Test Exam Based On Spritz Algorithm",* Lontar Komputer, Vol. 9, No. 1, DOI : 10.24843/LKJITI.2018.v09.I01.p06, e-ISSN : 2541-5832.
[3] Achmad, Komarudin, 2007, *"Aplikasi Analisis Multivariate Dengan Program SPSS,* Penerbit Andi, Yogyakarta.
[4] Sukrisno, dkk, 2010, *"Steganografi Menggunakan Teknik LSB Dengan Kombinasi Algoritma Vigenere dan RC4",* Jurnal Dinamika Informatika, Vol. 5, No. 2
[5] Krinawati, 2008, *"Metode Least Significant Bit dan End Of File Untuk Menyisipkan Teks Ke Dalam Citra Grayscale"* Seminar Nasional Informatika (Semnasif), Vol. 1, No. 1
[6] Sadikin, Rifki, 2012, *"Kriptografi Untuk Keamanan Jaringan",* Penerbit Andi, Yogyakarta.
[7] Ariyus, Dony, 2008, "*Computer Security*, Andi, Yogyakarta.

[8] Putra, Darma, 2010, "*Pengolahan Citra Digital"*, Penerbit Andi, Yogyakarta.
[9] Sitorus, S, dkk, 2006, *"Pengolahan Citra Digital,* Penerbit Andi, Yogyakarta.
[10] S, Riyanto, dkk, 2005,*"Step by Step Pengolahan Citra Digital"* hal ; 23, Penerbit Andi, Yogyakarta.
[11] Murni. A. 2008, *"Pengantar Pengolahan Citra",* Penerbit Alex Media Komputindo, Jakarta
[12] Nugroho, Adi, 2009, *"Rekayasa Perangkat Lunak Menggunakan UML dan Java"* Penerbit Andi, Yogyakarta.
[13] M. Mesran, "APLIKASI PENGAMANAN DATA TEKS PADA CITRA BITMAP DENGAN MENERAPKAN METODE LEAST SIGNIFICANT BIT (LSB)," *Pelita Inform. Inf. dan Inform.*, vol. 2, no. 1, Dec. 2012.