Management of Information System Journal
Vol 1, No 1, November, Hal 29 - 36
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Kombinasi Metode RSA, Secret Sharingasmuth-Bloom Dan Redundant Pattern Encoding Untuk Mengamankan Pesan

Muhammad Zairy Lubis

Program Studi Teknik Informatika, Fakultas Teknik Informatika, Universtias Budi Darma Medan, Indonesia
Jl. Sisingamangaraja No.338, Siti Rejo I, Kec. Medan Kota, Kota Medan, Sumatera Utara, Indonesia
Email: [1]muhammadzairy06@gmail.com

Abstrak−Kombinasi algoritma merupakan proses penggabungan lebih dari satu algoritma agar tingkat keamanan yang dihasilkan lebih baik. Penelitian ini mengkombinasikan 3 algoritma langsung agar tingkat pertahanan dalam pengamanan data lebih optimal. Algoritma-algoritma yang dikombinasikan dalam penelitian ini adalah algoritma RSA, secret sharing asmuth-bloom, dan redundant pattern encoding. Penelitian ini menguraikan bagaimana prosedur yang dilakukan untuk mengkombinasikan ketiga algoritma di atas yaitu RSA, secret sharing asmuth-bloom, dan redundant pattern encoding. Proses pengkombinasia dilakukan secara bertahap dengan melakukan proses enkripsi menggunakan RSA terlebih dahulu yang kemudian hasil dari enkripsi tersebut dienkripsikan lagi menggunakan secret sharing asuth-bloom, sehingga menghasilkan ciphertext baru dan kemudian ciphertext baru tersebut disisipkan ke dalam sebuah gambar menggunakan metode redundant pattern encoding. Hasil dari penelitian ini adalah merancang sebuah aplikasi pengaman data berbasis dengan menggunakan kombinasi algoritma RSA, secret sharing asmuth-bloom, dan redundant pattern encoding. Aplikasi ini dapat digunakan untuk mengamankan data berupa teks, sehingga tidak dapat diambil oleh orang lain. Selain itu, aplikasi yang akan dirancang ini lebih mudah untuk digunakan dalam pengamanan data.

Kata Kunci: Keamanan, Kunci, Algoritma, RSA, Secret Sharing Asmuth-Bloom, Redundant Pattern Encoding

Abstract−The combination of algorithms is the process of combining more than one algorithm so that the resulting level of security is better. This study combines 3 direct algorithms so that the level of defense in data security is more optimal. The combined algorithms in this study are the RSA algorithm, secret sharing asmuth-bloom, and redundant pattern encoding. This study describes how the procedure is carried out to combine the three algorithms above, namely RSA, secret sharing asmuth-bloom, and redundant pattern encoding. The combination process is carried out in stages by carrying out the encryption process using RSA first, then the results of the encryption are encrypted again using secret sharing asuth-bloom, resulting in a new ciphertext and then the new ciphertext is inserted into an image using the redundant pattern encoding method. The result of this study is to design a data-based security application using a combination of the RSA algorithm, secret sharing asmuth-bloom, and redundant pattern encoding. This application can be used to secure data in the form of text, so that it cannot be taken by others. In addition, the application that will be designed is easier to use in data security.

Keywords: Security, Key, Algorithm, RSA, Secret Sharing Asmuth-Bloom, Redundant Pattern

1. PENDAHULUAN

Perkembangan teknologi memberikan perubahan yang sangat signifikan bagi kehidupan manusia. Perubahan yang diberikan ada yang bersifat positif dan ada yang bersifat negatif. Pengaruh negatif yang ditimbulkan akibat dari perkembangan teknologi adalah penyalaah gunaan informasi oleh beberapa pihak yang tidak bertanggung jawab. Penyalah gunaan informasi memberikan kerugian tersendiri bagi pemiliknya. Apalagi informasi tersebut menyangkut tentang informasi pribadi yang tidak boleh diketahui oleh orang banyak, informasi tentang perusahaan dan berbagai informasi penting lainnya yang tidak bersifat umum atau lebih tepatnya bersifat rahasia. Informasi-informasi tersebut, sebaiknya diamankan dengan teknik tertentu agar tidak mudah diakses oleh orang lain. Salah satu teknik pengamanan informasi yang bisa digunakan adalah kriptografi. Kriptografi merupakan salah satu ilmu yang yang berperan penting dalam bidang pengamanan informasi. Kriptografi memiliki teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi misalnya kerahasiaan dan integritas data, serta otentikasi. Kuat lemahnya metode kriptografi tidak terletak dari hasil *enkripsi* atau *ciphertex*t, melainkan terletak pada kunci yang digunakan, oleh sebab itu kunci merupakan jantung dari pertahanan data tersebut agar tidak dapat diakses atau dibobol oleh orang-orang yang tidak bertanggung jawab(Guruh M Arindra Pratama, 2015). Algoritma di dalam kriptografi terbagi menjadi dua, yaitu algoritma kunci simetri dan algoritma kunci asimetri. Salah satu algoritma yang bisa dimanfaatkan untuk mengamankan data adalah metode *revest shamir adleman* (RSA), *secret sharing asmuth-bloom* dan *redundant Pattern encoding*.

Penelitian ini menguraikan bagaimana prosedur yang dilakukan untuk mengamankan pesan dengan menggunakan ketiga algoritma di atas. Proses pengkombinasian dari ketiga algoritma di atas memberikan pengamanan pesan yang lebih efektif dan efesien, sehingga tidak bisa dibobol dan disalah gunakan oleh pihak yang tidak bertanggung jawab.

2. METODOLOGI PENELITIAN

2.1 Metode Penelitian

Metode penelitian merupakan suatu cara atau langkah yang dapat dilakukan oleh peneliti dalam rangka untuk mengumpulkan informasi atau data dan melakukan investigasi terhadap data yang telah didapat. Adapun metode penelitian yang dilakukan dalam penelitian ini adalah :

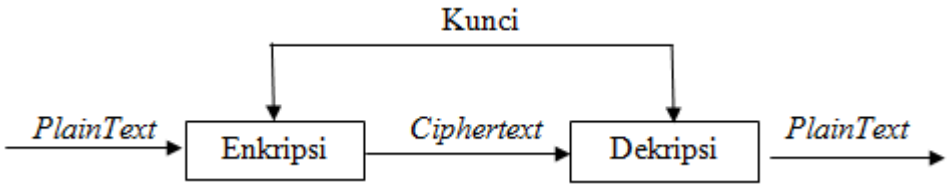
Management of Information System Journal
Vol 1, No 1, November, Hal 29 - 36
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

a. Studi pustaka
   Dilakukan dengan membaca literatur yang berkaitan dengan pembahasan dan tema yang dibuat. Cara yang dilakukan antara lain dengan membaca buku kriptografi, buku-buku pendukung lain yang membahas tentang kriptografi dan penerapan berbagai metode yang ada di dalamnya, dan juga dari situs-situs hasil browsing di internet.
b. Tahapan analisa dan perancangan
   Melakukan analisa terhadap kekurangan algoritma algoritma revest shamir adleman (RSA), secret sharing asmuth-bloom dan redundant Pattern encoding. Tahap ini juga menguraikan proses perancangan aplikasi pengamanan data yang digunakan untuk mengamankan pesan agar lebih efektif dan efesien.
c. Tahapan pengujian dan implementasi
   Tahap ini merupakan tahap pengujian terhadap hasil kombinasi algoritma revest shamir adleman (RSA), secret sharing asmuth-bloom dan redundant Pattern encoding apakah setelah dikombinasi kuat dan tidak mudah untuk dipecahkan atau sebaliknya. Setelah memastikan bahwa kombinasi tersebut kuat, maka dilakukan tahapan implementasi terhadap algoritma revest shamir adleman (RSA), secret sharing asmuth-bloom dan redundant Pattern encoding.

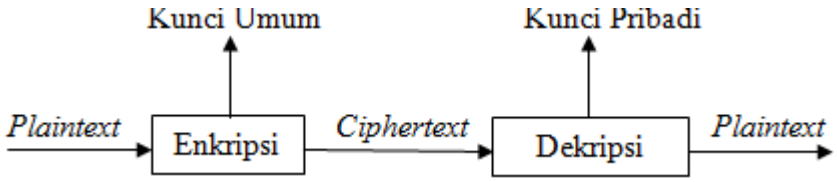
2.2 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa yunani yaitu "*cryptos*" artinya "*secret*" yang berarti rahasia, sedangkan "*graphein*" artinya "*writing*" yang berarti tulisan rahasia(Mukhtar, 2018). Kriptografi memiliki beragam metode untuk menyandikan pesan atau informasi yang ingin kita sembunyikan, seperti *Caesar cipher, polyalphabetic, vigenere transposisi*, dan masih banyak lagi metode yang ada di dalam kriptografi(Arrijal et al., 2016). Ada dua jenis kriptografi yaitu algoritma Simetris dan Asimetris. Ada beberapa komponen dalam kriptografi, yaitu(Mukhtar, 2018) :

1. *Plaintext*, yaitu pesan yang dibaca
2. *Ciphertext* yaitu pesan kunci atau pesan acak yang tidak bisa dibaca
3. *Key*, yaitu kunci untuk melakukan teknik kriptografi
4. *Algoritma* yaitu metode yang dilakukan untuk melakukan enkripsi dan dekripsi.



Gambar 1. Proses Enkripsi dan Deskripsi Algoritma Simetris



Gambar 2. Proses Enkripsi dan Deskripsi Algoritma ASimetris

2.3 Algoritma *Rivest Shamir Adleman*

Aloritma Rivest *Shamir Adleman* (RSA) merupakan teknik kriptografi dengan memanfaatkan 2 bilangan prima(Pratama et al., 2017). Pada algoritma RSA terdapat tiga proses yaitu, pembangkitan kunci, proses enkripsi dan proses dekripsi. Letak kesulitan algoritma ini adalah bagaimana menemukan dua faktor bilangan prima yang besar yang akan digunakan sebagai kunci publik dan kunci privat. Dua bilangan prima besar tersebut p dan q dimana $p \neq q$. Berikut adalah langkah-langkah penggunaan algoritma RSA(Pratama et al., 2017) :

1. Menentukan p dan q. p dan q adalah bilangan prima
2. Menghitung nilai n yang merupakan modulus dengan rumus
   n = p x q……(1)
   Dimana :
   n = Bilangan *Integer*
   p = Bilangan Prima Pertama
   q= Bilangan Prima Kedua
3. Menentukan nilai e yang bilangan prima dengan syarat.
   1 < e < n
4. Mencari nilai *deciphering exponent* (d) dengan menggunakan rumus :
   d = 1 + (k x n) / e)……(2)

Management of Information System Journal
Vol 1, No 1, November, Hal 29 - 36
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Dimana :
d = *deciphering exponent*
k = Sembarang Angka
n = Bilangan *Integer*
e = bilangan prima

2.4 Algoritma *Secret Sharing Asmuth-Bloom*

Algoritma *secret sharing asmuth-bloom* merupakan salah satu metode untuk mengamankan kerahasiaan suatu data atau file dengan membagi atau mengirim rahasia tersebut menjadi beberapa bagian yang dinamakan *share*, setiap bagian dari rahasia tersebut tidak memberikan informasi apa-apa mengenai rahasia yang dimaksud, bila tidak digabungkan dengan bagian yang lainnya(Saputra & Manalu, 2020).
Berikut adalah langkah-langkah penggunaan algoritma *secret sharing asmuth-bloom*(Pratama et al., 2017) :

1. Proses pembentukan kunci
   a. Tentukan sebuah bilangan prima p, dimana p lebih besar daripada bilai kode ASCII data M.
   b. Tentukan nilai m dan n dimana m ≤ n.
   c. Tentukan n buah bilangan yang lebih kecil daripada p, yaitu d1, d2, d3, …, dndalam urutan menaik dan setiap nilai direlatif prima terhadap setiap nilai dilainnya.
2. Proses pembentukan shadow
   a. Tentukan bilangan acak r.
   b. Hitung nilai M’ dengan rumus : M’ = M + rp
   c. Shadow-nya adalah : ki = M’ mod di.

2.5 Algoritma *Redundant Pattern Encoding*

Algoritma *redundant pattern encoding* merupakan salah satu tekni pengamanan data yang dapat digunakan dengan cara menyisipkan sebuah pesan yang akan di amankan ke dalam sebuah objek yang merupakan wadah tempat penampungan atau pengamanan yang selanjutnya akan dijadikan sebagai *noise*(Stefanus Yerian Elandha, Magdalena A. Ineke Pakereng, 2016). Kelebihan dari algoritma ini adalah bertahan terhadap *cropping*, dan kerugiannya adalah tidak dapat menggambar pesan yang lebih besar(Nugraha et al., 2011).

2.6 Data Teks

Data merupakan kenyataan yang menggambarkan suatu kejadian dan kesatuan yang nyata(Sutabri, 2012). Data teks merupakan sekumpulan huruf yang membentuk kalimat untuk menggambarkan kejadian atau informasi(Dwiyanto, 2020).

3. HASIL DAN PEMBAHASAN

Kriptografi merupakan salah satu ilmu yang yang berperan penting dalam bidang pengamanan informasi. Kriptografi memiliki teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi misalnya kerahasiaan dan integritas data, serta otentikasi. Algoritma di dalam kriptografi terbagi menjadi dua, yaitu algoritma kunci simetri dan algoritma kunci asimetri. Dalam kriptografi ada yang namanya ciphertext yang merupakan teks yang telah diacak, plaintext yang merupakan pesan asli yang akan diamankan, dan kunci sebagai jantung dari data yang akan diamankan. Salah satu algoritma yang bisa dimanfaatkan untuk mengamankan data adalah metode ravest shamir adleman (RSA), secret sharing asmuth-bloom dan redundant pattern encoding. Ketiga metode tersebut memilik kelamahan satu sama lain. Kelemahan-kelemahan tersebutlah yang dimanfaatkan untuk membuka data yang telah diamankan. Pada algoritma RSA, kelemahannya adalah lambat, pesan dan kunci harus dikirim bersamaan, penerima dapat mendeteksi kunci menggunakan kunci privat. Kemudian yang menjadi kelemahan algoritma secret sharing asmuth-bloom adalah data yang diamankan tidak dapat berukuran besar.
Proses untuk menyelesaikan masalah tersebut adalah dengan melakukan kombinasi terhadap 3 algoritma tersebut. Pengamanan data menggunakan kombinasi dari ketiga algoritma tersebut adalah dengan menginput teks yang akan diamankan, dimana teks tersebut akan diproses dengan menggunakan metode ravest shamir adleman. Pada tahapan ini akan dilakukan proses enkripsi yang akan menghasilkan ciphertext atau pesan acak yang kemudian pesan acak tersebut akan dienkripsikan lagi menggunakan metode secret sharing asmuth-bloom dan menghasilkan ciphertext terbaru. Setelah ciphertext diperoleh, maka tahap selanjutnya adalah dengan menyisipkan pesan tersebut ke dalam sebuah gambar menggunakan metode redundant pattern encoding dengan menjadikan pesan tersebut sebagai noise gambar namun tidak mengubah asli dari gambar tersebut.

3.1 Penerapan Kombinasi *Algoritma Ravest Shamir Adleman, Secret Sharing Asmuth Bloom* Dan *Redundant Pattern Encoding*

1. Tahapan pembangkitan kunci dengan menentukan nilai p dan q yang merupakan bilangan prima
   P = 47 dan q = 71

Management of Information System Journal
Vol 1, No 1, November, Hal 29 - 36
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

2. Kemudian menghitung nilai n dengan rumus n = p*q
   n = 47*71 = 3337
3. Kemudian menentukan nilai d dan c sebagai kunci privat
   d = 79
   c = 1019
4. Kemudian menentukan teks yang akan diamankan. Teks yang akan diamankan adalah LIBURAN. Kemudian teks tersebut dikonversikan ke dalam bentuk desimal ASCII

Tabel 1 Desimal ASCII

Teks	Desimal ASCII
L	76
I	73
B	66
U	85
R	82
A	65
N	78

5. Setelah dikonversi, memecah hasil nilai konversi tersebut menjadi blok-blok. Pesan yang telah dikonversi di atas dapat dipecah menjadi 5 blok yang terdiri dari 3 digit setiap blok blok blok tersebut adalah 767 366 858 265 078
6. Melakukan proses enkripsi menggunakan rumus:
   Ci = Plainteks^{d} mod n
   $x_1 = 767^{79} \bmod 3337 = 360$
   $x_2 = 366^{79} \bmod 3337 = 1055$
   $x_3 = 858^{79} \bmod 3337 = 666$
   $x_4 = 265^{79} \bmod 3337 = 865$
   $x_5 = 078^{79} \bmod 3337 = 1609$
   Dari perhitungan di atas, didapatkan hasil enkripsi yaitu **360105566686516O9**
   kemudian hasil dari enkripsi tersebut, di enkripsikan lagi dengan metode *secret sharing asmuth-bloom.* Berikut adalah proses enkripsi pesannya :

1. Memecah pesan di atas menjadi beberapa blok yang terdiri dari 3 digit dan menyusunnya seperti berikut :
   M1 = 360
   M2 = 105
   M3 = 566
   M4 = 686
   M5 = 516
   M6 = 09
2. Memilih bilangan prima yang dilambangkan dengan p
   P = 41
3. Menentukan bilangan acak yang dilambangkan dengan r
   r = 17
4. Hitung nilai M’ untuk setiap karakter
   M1’ = M1 + P * r = 360 + 41 * 17 = 1057
   M2’ = M2 + P * r = 105 + 41 * 17 = 802
   M3’ = M + P * r = 566 + 41 * 17 = 1263
   M4’ = M4 + P * r = 686 + 41 * 17 = 1383
   M5’ = M5 + P * r = 516 + 41 * 17 = 1213
   M6’ = M6 + P * r = 09 + 41 * 17 = 706
   Jadi pesan baru yang di dapat adalah 1057 802 1263 1383 1213 706
   Kemudian pesan di atas disisipkan ke dalam sebuah gambar dengan terlebih dahulu membagi nilai tersebutmenjadi beberapa blok yang tiap blok terdiri dari 2 digit dan mengkonversi nilai tersebut ke dalam biner. Berikut adalah pesan yang dikinversi dalam bentuk biner :

10 = 00001001	83 = 01010011
57 = 00111001	12 = 00001100
80 = 01010000	13 = 00001101
21 = 00010101	70 = 01000110

Management of Information System Journal
Vol 1, No 1, November, Hal 29 - 36
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

63 = 00111111 06 = 00000110
13 = 00001101
Kemudian menyiapkan gambar berwarna yang akan dijadikan seabagi tempat untuk menyisipkan pesan. Berikut adalah gambar tempat penyisipan pesan :

Gambar 2. Proses Enkripsi dan Deskripsi Algoritma ASimetris

Kemudian mencari nilai piksel gambar tersebut. Berikut adalah nilai gambar tersebut yang berukuran 500 piksel x 500 piksel.

Tabel 2 Nilai Piksel *Red* Gambar Yang Disisipkan Pesan

	1	2	3	4	5	6	7	8	9	10	…	500
1	25	24	23	22	23	24	23	23	23	23	…	23
2	25	25	24	24	25	26	26	25	25	24	…	24
3	26	23	22	22	23	24	24	23	22	21	…	25
4	28	24	23	23	24	25	25	23	23	22	…	26
5	29	27	25	25	26	27	28	27	28	27	…	26
6	29	28	26	24	25	26	27	27	27	27	…	26
7	29	30	28	25	26	25	26	26	26	26	…	27
8	27	28	26	25	26	26	26	26	26	26	…	28
9	25	24	24	24	25	26	26	25	26	26	…	28
10	24	24	24	25	25	26	26	25	25	25	…	29
…	…	…	…	…	…	…	…	…	…	…	…	…
500	0	5	1	6	54	102	101	100	108	101	…	152

Pada tabel di atas merupakan nilai R berukuran 500x500 piksel. Pada piksel (1,1). Nilai R = 25 dan pada piksel (500x500) nilai R = 152

Management of Information System Journal
Vol 1, No 1, November, Hal 29 - 36
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Tabel 3 Nilai Piksel *Green* Gambar Yang Disisipkan Pesan

	1	2	3	4	5	6	7	8	9	10	…	500
1	26	25	24	23	24	25	24	24	24	24	…	24
2	26	26	25	25	26	27	27	26	26	25	…	25
3	27	24	23	23	24	25	25	24	23	22	…	26
4	29	25	24	24	25	26	26	24	24	23	…	27
5	30	28	26	26	27	28	29	28	29	28	…	27
6	30	29	27	25	26	27	28	28	28	28	…	27
7	30	31	29	26	27	26	27	27	27	27	…	28
8	29	28	27	26	26	27	27	27	27	27	…	29
9	27	26	26	26	27	28	28	27	27	27	…	29
10	27	27	28	28	29	29	29	28	28	28	…	30
…	…	…	…	…	…	…	…	…	…	…	…	…
500	36	35	29	51	105	152	152	151	160	151	…	151

Pada tabel di atas matrik nilai G berukuran 500x500 piksel. Pada piksel (1,1) nilai G = 26 dan pada piksel (500,500) nilai G = 151

Tabel 4 Nilai Piksel *blue* Gambar Yang Disisipkan Pesan

	1	2	3	4	5	6	7	8	9	10	…	500
1	20	19	18	17	18	19	18	18	18	18	…	8
2	20	20	19	19	20	21	21	20	20	19	…	9
3	19	18	17	17	18	19	19	18	17	16	…	10
4	20	19	18	18	19	20	20	18	18	17	…	11
5	22	22	20	20	21	22	23	22	23	22	…	11
6	22	23	21	19	20	21	22	22	22	22	…	11
7	20	23	22	19	19	20	21	21	21	21	…	12
8	18	20	19	18	18	20	21	21	21	21	…	13
9	16	18	17	18	18	20	21	21	21	21	…	13
10	16	19	19	19	20	21	22	21	21	21	…	14
…	…	…	…	…	…	…	…	…	…	…	…	…
500	6	9	7	26	81	133	138	139	150	144	…	165

Pada tabel di atas matrik nilai B berukuran 500x500 piksel. Pada piksel (1,1) nilaiB = 20 dan pada piksel (500x500) nilai B = 165

Kemudian mengkonversi nilai piksel *red* ke dalam bentuk biner dan mengganti nilai akhir tiap nilai biner *red* dengan satu persatu nilai biner pesan yang disisipkan dimulai dari kiri ke kanan. Berikut adalah proses penyisipan pesan :

25 = 00011001 menjadi 00011000
24 = 00011000 menjadi 00011000
23 = 00010111 menjadi 00010110
22 = 00010110 menjadi 00010110
23 = 00010111 menjadi 00010111
24 = 00011000 menjadi 00011000

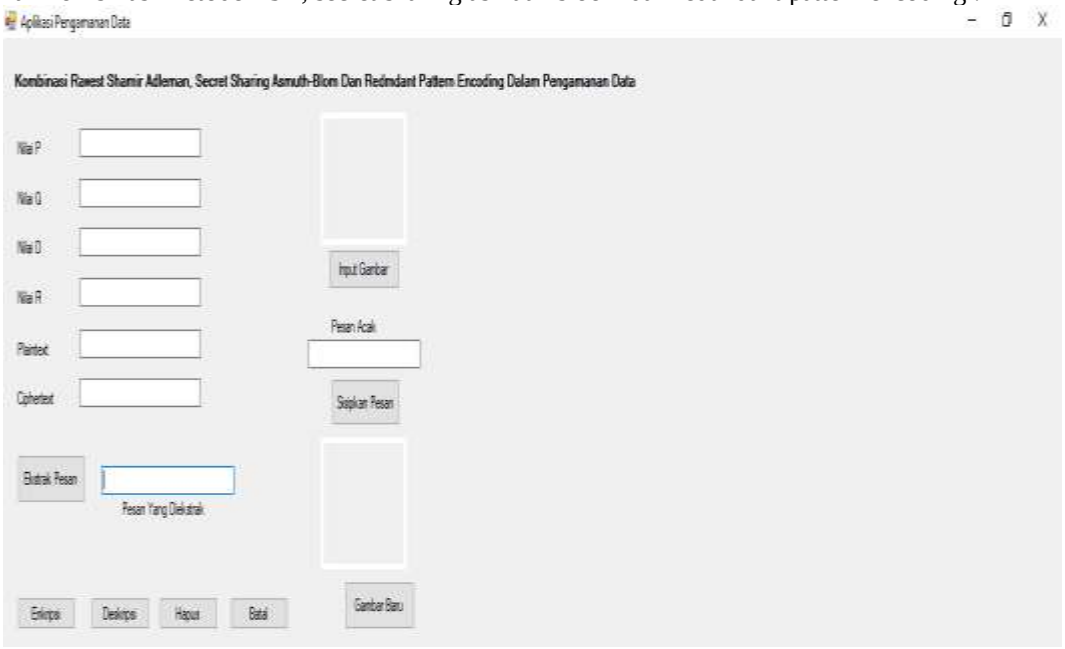
Management of Information System Journal
Vol 1, No 1, November, Hal 29 - 36
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

23 = 00010111 menjadi 0001011<u>0</u>
23 = 00010111 menjadi 0001011<u>1</u>
Proses di atas dilakukan sampai pesan tersebut selesai disisipkan.

3.2 Hasil Implementasi dan Pengujian

1. Tampilan Input

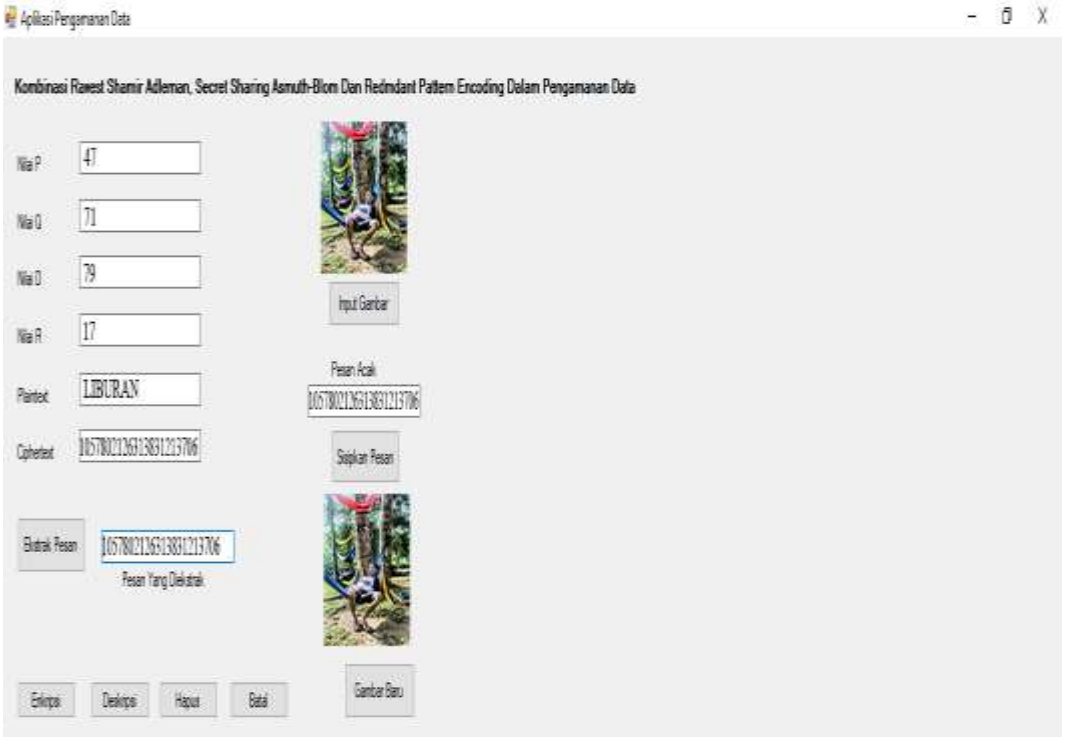
Tampilan input merupakan tampilan yang digunakan untuk memasukan data yang hendak diproses. Tampilan ini akan memperlihatkan desain komponen yang diperlukan. Berikut adalah tampilan input aplikasi pengamanan data menggunakan kombinasi metode RSA, secret sharing asmuth-bloom dan redundant pattern encoding :



Gambar 3. *Input* Aplikasi Pengamanan Data

2. Tampilan Output

Tampilan output merupakan halaman yang manampilkan hasil dari data yang telah diproses Berikut adalah tampilan input aplikasi pengamanan data menggunakan kombinasi metode RSA, secret sharing asmuth-bloom dan redundant pattern encoding :



Management of Information System Journal
Vol 1, No 1, November, Hal 29 - 36
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Gambar 4. *Output* Aplikasi Pengamanan

Tabel 5. Hasil Pengujian

Kombinasi Metode RSA, *Secret Sharing Asmuth-Bloom* Dan *Redundant Pattern Encoding*							
P	Q	D	R	Plaintext	Ciphertext	Gambar	Hasil
47	71	79	17	LIBURAN	1057 802 1263 1383 1213 706		

4. KESIMPULAN

Kesimpulan yang dapat diambil dari hasil penelitian modifikasi vigenere cipher dengan pembangkit kunci blum blum shup, yaitu Prosedur pengamanan pesan dimulai dari tahapan penggunaan metode pengamanan yang sesuai agar objek dan metode yang digunakan singkron. Sehingga masalah tentang keamanan dapat diselesaikan. Proses kombinasi algoritma revest shamir adleman (RSA), secret sharing asmuth-bloom dan redundant Pattern encoding dalam mengamankan pesan dilakukan secara bertahap, dimana tahap pertama yang dilakukan adalah tahapan pengaman menggunakan revest shamir adleman (RSA) dan kemudian hasil dari proses tersebut dilakukan pengaman lagi menggunakan secret sharing asmuth-bloom. Setelah didapatkan ciphertext dari proses tersebut, maka dilakukan penyisipan menggunakan redundant Pattern encoding. Aplikasi pengamanan data menggunakan kombinasi algoritma revest shamir adleman (RSA), secret sharing asmuth-bloom dan redundant Pattern encoding dirancang untuk membantu dan mempermudah pengguna dalam mengamankan data penting atau data yang bersifat rahasia.

REFERENCES

[1] K. dan A. Kinoyo, *Tuntutan Praktis Membangun Sistem Informasi Akutansi dengan Mikrosoft Visual Basic & SQL, Server*. Andi, 2007.
[2] H. Mukhtar, *Kriptografi untuk Keamanan Data*, 1st ed. Yogyakarta: CV Budi Utama, 2018.
[3] T. D. U. M. Buana, "Kriptografi," *Pus. Bahan Ajar dan Learn.*, vol. 2, no. 5, p. 206, 2010.
[4] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher dengan PHP," *J. Teknol. Inf.*, vol. 1, no. 1, p. 11, 2017, doi: 10.36294/jurti.v1i1.21.
[5] I. M. Arrijal, R. Efendi, and B. Susilo, "Penerapan Algoritma Kriptografi Kunci Simetris dengan Modifikasi Vigenere Cipher dalam Aplikasi Kriptografi Teks," *J. Pseudocode*, vol. 3, no. 1, pp. 69–82, 2016, doi: 10.33369/pseudocode.3.1.69-82.
[6] F. R. Andhika, "Modifikasi Vigenere Cipher dengan Menggunakan Caesar Cipher dan Enkripsi Berlanjut untuk Pembentukan Key," *Pelita Inform. Intstitut Teknol. Bandung*, vol. 4, no. 5, pp. 1–8, 2011.
[7] A. E. Putra, "Fungsi Hash pada Kriptografi," *J. Inform. Inst. Teknol. Bandung*, vol. 1, no. 1, pp. 1–6, 2009.
[8] A. R. C, *Algoritma dan Pemrograman dengan Bahasa C*, I. Yogyakarta: ANDI Yogyakarta, 2010.
[9] M. Pratama *et al.*, "PENERAPAN METODE SECRET SHARING ASMUTH-BLOOM UNTUK PENGAMANAN DATA TEKS," vol. 6, pp. 4–7, 2017.
[10] I. Saputra and N. Manalu, "Pengamanan Transfer File Menggunakan Secret Sharing Asmuth-Bloom," vol. 1, pp. 426–428, 2020.
[11] M. K. Stefanus Yerian Elandha, Magdalena A. Ineke Pakereng, "Perancangan dan Implementasi Steganografi Menggunakan Metode Redundant Pattern Encoding dengan Algoritma AES (Advanced Encryption Standard) Artikel Ilmiah Perancangan dan Implementasi Steganografi Menggunakan Metode Redundant Pattern Encoding dengan Alg," *Kumpul. J. TI*, vol. 1, no. 1, 2016.
[12] E. F. Nugraha, I. T. Bandung, and J. G. Bandung, "Meningkatkan Kapasistas Pesan yang disisipkan dengan Metode Redundant Pattern Encoding," *J. Inst. Teknol. Bandung*, vol. 1, no. 11, 2011.
[13] M. Z. Riyanto, "Bilangan Prima dan Teorema Fundamental Aritmatika Bilangan Prima," no. 5, pp. 1–8, 2017.
[14] F. Zunaidi, "Buku Pintar Aritmatika Modular," *J. Ilmu Mat.*, vol. 3, no. 7, 2006.
[15] T. Sutabri, *Konsep Sistem Informasi*, I. Yogyakarta: ANDI Yogyakarta, 2012.
[16] H. E. Dwiyanto, "Format File," *Teknol. J.*, vol. 1, no. 2, pp. 1–5, 2020.
[17] M. S. Rossa A. S, *Rekayasa Perangkat Lunak*, I. Bandung: Informatika Bandung, 2013.
[18] A. Nugoro, *Rekayasa Perangakat Lunak Menggnakan UML dan Java*, 1st ed. Yogyakarta: ANDI, 2009.
[19] J. HM., *Analisa dan Desain Sistem Informasi*, 5th ed. Yogyakarta: ANDI, 2005.
[20] I Ketut Darmayuda, Pemrograman Aplikasi Database Microsoft Visual Basic.Net, Bandung, Informatika, 2010.