BAB IV HASIL DAN PEMBAHASAN

4.1 Analisis Penerapan Metode

File teks menjadi salah satu bentuk dokumen yang umum digunakan untuk menyimpan informasi yang sifatnya pribadi atau rahasia, sehingga perlu dilakukan tindakan untuk tetap menjaga informasi tersebut hanya dapat diakses oleh pemilik data, baik pada saat disimpan atau pada saat ditransmisikan. Teknik kriptografi merupakan salah satu alternatif solusi yang dapat diterapkan untuk menjaga keamanan data, yaitu dengan cara memanipulasi pesan ke dalam bentuk yang tidak dimengerti oleh banyak orang.

Selain menerapkan algoritma kriptografi yang baru, biasanya banyak peneliti memodifikasi suatu algoritma kriptografi, namun hal ini bukanlah suatu pekerjaan yang mudah. Oleh karena itu, salah satu cara yang dapat diterapkan dalam meningkatkan keamanan pesan dengan menggunakan teknik kriptografi dengan cara mengkombinasikan dua buah algoritma kedalam satu proses. Pada penelitan ini akan mengimplementasikan perpaduan algoritma kriptografi simetris *Beaufort Cipher* dan algoritma kriptografi asimetris RSA guna meningkatkan keamaman pesan pada *file* teks. Metode pengkombinasian antara kedua algoritma yang bertujuan untuk mendapatkan hasil enkripsi (*ciphertext*) yang lebih kuat sehingga sulit untuk dipecahkan, dan juga untuk mengatasi penggunaan *ciphertext* tunggal yang secara komparatif lemah (Syahputra et al., 2021) karena hanya menggunakan satu algoritma kriptografi. Sistem yang dibangun pada penelitian ini adalah berupa aplikasi berbasis *web* untuk menyelesaikan permasalahan keamanan pesan pada *file* teks.

4.1.1 Analisis Proses Enkripsi

Proses enkripsi merupakan tahap untuk mentransformasi data ke dalam bentuk yang tidak dimengerti oleh banyak orang. Dalam penelitian ini data yang akan di enkripsi adalah berupa pesan yang terdapat dalam *file* teks dengan menerapkan perpaduan algoritma kriptografi simetris *Beaufort Cipher* dan algoritma asimetris RSA dalam skema super enkripsi. Gambar 4.1 berikut menjelaskan secara umum mengenai proses enkripsi yang diterapkan dalam penelitian ini.



Gambar 4.1 Skema Proses Enkripsi

Sesuai gambar 4.1 terdapat dua proses utama yang dilakukan dalam mengamankan data berupa *file* teks dalam skema super enkripsi, proses pertama yaitu melakukan enkripsi menggunakan kunci algoritma *Beaufort Cipher* sehingga menghasilkan *ciphertext*1, lalu hasil dari proses tersebut akan di enkripsi lagi dengan menggunakan kunci publik algoritma RSA sehingga menghasilkan *ciphertext*2 sebagai hasil akhir dari proses enkripsi. Pesan yang terdapat dalam *file* teks yang akan di enkripsi hanya menggunakan penyandian karakter A-Z dan karakter a-z yang terdapat dalam tabel ASCII dengan *modulo* 26 untuk algoritma *Beaufort Cipher* dan hanya menggunakan kunci dengan karakter *alphabet*. Sedangkan hasil enkripsi algoritma RSA akan dikonversi kedalam nilai desimal. Berikut ditampilkan contoh sampel data dengan format *file* teks.

		UNIVE	👔 🕼 file ujil - Notepad	- 🗆 X
file uji'l Pe Gereral Sect	opertiec arty Details Previous Versons	*ED	File Edit Format View Help kriptografi merupakan studi terhada	ap teknik matematis yang ter
Type of file. Opens with: Location: Size:	Tes ul 1 Test Document (Jit) Notopiad Notopiad Crivalenge/Holdoce*vea/best/fort 31.5 KBI (J2:251 bytes)		sia dan tidak boleh diberitahukan k ripsi dan dekripsi. Kedua proses te ipsi dapat dihitung dari kunci dek kunci enkripsi dapat dibuat publik gan menggunakan dua jenis kunci yar	<pre>cepada orang lain yang tida) wrsebut tentunya membutuhkan vipsi dan sebaliknya, artin yaitu pihak luar dapat men g berbeda untuk tiap-tiap</pre>
Size on dak: Created Modified Accessed	22.0 KB (32.758 bytes) 31 October 2032, 14:07:22 08 December 2022, 16:43:21 05 December 2022, 16:43:21		rtext diseout dengan proses enkrip: ffusion (peleburan) yaitu harus man rbasis kunci, yaitu sistem kriptop oritma dimana kunci yang digunakan	il sedangkan proses yang di ipu menyembunyikan pola dar grafi simetris (Symmetric Ci untuk enkripsi berbeda denj
Attibutes	OK Care	Adverset	bertujuan untuk mendapatkan cipheri but tidak dapat dibaca oleh orang y a untuk keamanan informasi, seperti kriptografi (cryptosystem) sering o	<pre>:ext yang lebih kuat sehing 'ang tidak berkepentingan. privasi dan autentikasi. disebut juga dengan sistem ></pre>
			Ln 1, Col 29748 100%	Windows (CRLF) UTF-8

Gambar 4.2 Potongan Sampel Data

Sesuai gambar 4.2, sampel data mempunyai *size* sebesar 32 KB (*kilo bytes*) dengan jumlah karakter sebanyak 28.272 karakter. Oleh karena itu, untuk mempermudah perhitungan dalam proses enkripsi maka hanya mengambil 11 huruf pertama sebagai inputan dalam melakukan proses perhitungan enkripsi secara manual.

Sebelum melakukan proses enkripsi menggunakan algoritma *Beaufort Cipher*, maka terlebih dahulu pesan yang terdapat dalam *file* teks dikonversi kedalam bentuk desimal dalam tabel ASCII. Proses konversi teks kedalam bentuk desimal pada penelitian ini dengan memanfaatkan tools yang dapat diakses secara *online* melalui alamat *https://onlinetexttools.com/*. Adapun hasil konversinya dapat disajikan pada gambar 4.3.



Gambar 4.3 Potongan Sampel Data (a) Karakter (b) Nilai Desimal

UNIVERSITAS ISLAM NEGERI

Gambar 4.3 menampilkan nilai desimal dari sampel data yang diperoleh dengan menggunakan alat bantu (*tools*) dari *https://onlinetexttools.com/*. Setelah nilai desimal dari pesan yang terdapat dalam *file* teks didapatkan, maka proses enkripsi dengan algoritma *Beaufort Cipher* dapat dilakukan. Dengan mengambil 11 huruf pertama dari *file* teks serta menentukan kunci enkripsi dan dekripsi sebagai berikut:

Plaintext: kriptografi Kunci : mahyudi Berdasarkan skema enkripsi pada gambar 4.1 maka tahap pertama yang dilakukan yaitu mengenkripsi pesan dengan menggunakan algoritma *Beaufort Cipher*. Enkripsi *Beaufort Cipher* merupakan teknik substitusi kriptografi yang menggunakan operasi *modulo* bilangan bulat sebagai proses utama. Kunci (K) pada *Beaufort Cipher* adalah urutan karakter-karakter $K = k_1, ..., k_n$ dimana k_1 didapat dari banyaknya pergeseran dari karakter ke-i. Artinya bahwa jumlah kunci yang digunakan harus sama dengan jumlah karakter *plaintext* yang diamankan. Algoritma ini melakukan proses enkripsi secara *stream* (masing-masing karakter *plaintext* harus memiliki pasangan kunci).

Dapat diketahui bahwa panjang *plaintext* = 11, sedangkan panjang kunci = 7, karena panjang kunci algoritma *Beaufort Cipher <* panjang *plaintext*, maka kunci algoritma *Beaufort Cipher* tersebut akan diulang secara periodik sehingga panjang kunci tersebut sama dengan panjang *plaintext*-nya, yaitu sebagai berikut:

Plaintex	t:	k	r	i	р	t	0	g	r	а	f	i
Kunci	:	m	a	h	у	u	d	i	m	a	h	у

Pada contoh diatas kunci algoritma *Beaufort Cipher* "mahyudi" diulang sedemikian rupa hingga panjang kunci sama dengan panjang *plaintext*-nya. Kemudian setelah panjang kunci sama dengan panjang *plaintext*, proses enkripsi dilakukan terlebih dahulu akan dikonversi ke desimal pada tabel ASCII sehingga hasilnya dapat disajikan pada tabel 4.1.

		LVE	LCNL	LAN.	\mathbb{N}	M	<u>N MC i</u>	H.K.L			
Plaintext (M_i)	k,	r	j ⁱ	р	TAT	-9	g	r	a	f	i
Nilai Desimal	107	114	105	112	116	-111	103	114	97	102	105
Kunci (Ki)	m	а	h	у	u	d	i	m	а	h	у
Nilai Desimal	109	97	104	121	117	100	105	109	97	104	121

Tabel 4.1 Proses Mengubah Plaintext Menjadi Desimal

Setelah *plaintext* dikonversi menjadi desimal, maka proses enkripsi algoritma *Beaufort Cipher* dapat dilakukan dengan menggunakan rumus pada persamaan (2.1) sehingga diperoeleh hasilnya sebgai berikut:

Untuk karakter $(M_1) = k$ dan kunci $(K_1) = m$ $C_1 = (K_1 - M_1) \mod 26 = (m - k) \mod 26 + 97$ $= (109 - 107) \mod 26 + 97$ = 99 (huruf "c" dalam tabel ASCII) Untuk karakter $(M_2) = r$ dan kunci $(K_2) = a$ $C_2 = (K_2 - M_2) \mod 26 = (a - r) \mod 26 + 97$ $= (97 - 114) \mod 26 + 97$ = 106 (huruf "j" dalam tabel ASCII) Untuk karakter $(M_3) = i$ dan kunci $(K_3) = h$ $C_3 = (K_3 - M_3) \mod 26 = (h - i) \mod 26 + 97$ $= (104 - 105) \mod 26 + 97$ = 122 (huruf "z" dalam tabel ASCII) Untuk karakter $(M_4) = p$ dan kunci $(K_4) = y$ $C_4 = (K_4 - M_4) \mod 26 = (y - p) \mod 26 + 97$ $= (121 - 112) \mod 26 + 97$ = 106 (huruf "j" dalam tabel ASCII) Untuk karakter $(M_5) = t$ dan kunci $(K_5) = u$ $C_5 = (K_5 - M_5) \mod 26 = (u - t) \mod 26 + 97$ $= (117 - 116) \mod 26 + 97$ = 98 (huruf "b" dalam tabel ASCII) Untuk karakter $(M_6) = o \text{ dan kunci} (K_6) = d$ $C_6 = (K_6 - M_6) \mod 26 = (d - o) \mod 26 + 97_{GERI}$ SUMATER = (100 - 111) mod 26 + 97= 112 (huruf "p" dalam tabel ASCII)Untuk karakter $(M_7) = g$ dan kunci $(K_7) = i$ $C_7 = (K_7 - M_7) \mod 26 = (i - g) \mod 26 + 97$ $= (105 - 103) \mod 26 + 97$ = 99 (huruf "c" dalam tabel ASCII) Untuk karakter $(M_8) = r \text{ dan kunci} (K_8) = m$ $C_8 = (K_8 - M_8) \mod 26 = (m - r) \mod 26 + 97$

 $= (109 - 114) \mod 26 + 97$ = 118 (huruf "v" dalam tabel ASCII)Untuk karakter (M₉) = a dan kunci (K₉) = a C₉ = (K₉ - M₉) mod 26 = (a - a) mod 26 + 97 $= (97 - 97) \mod 26 + 97$ = 97 (huruf "a" dalam tabel ASCII)Untuk karakter (M₁₀) = f dan kunci (K₁₀) = h C₁₀ = (K₁₀ - M₁₀) mod 26 = (h - f) mod 26 + 97 $= (104 - 102) \mod 26 + 97$ = 99 (huruf "c" dalam tabel ASCII)Untuk karakter (M₁₁) = i dan kunci (K₁₁) = y C₁₁ = (K₁₁ - M₁₁) mod 26 = (y - i) mod 26 + 97 $= (121 - 105) \mod 26 + 97$ = 113 (huruf "q" dalam tabel ASCII)

Berdasarkan hasil perhitungan diatas maka diperoleh hasil enkripsi pertama (*ciphertext*1) dengan menggunakan algoritma *Beaufort Ciphert* yaitu:

Plaintext (M _i)	k	r	i	p	t	0	g	r	а	f	i
Kunci Beaufort (K _i)	m	а	h	у	u	d	i	m	а	h	y
Ciphertext1 (C _i)	c	j	z	j	b	p	c	v	a	c	q

Hasil dari proses enkripsi (*ciphertext*1) kemudian akan di enkripsi lagi dengan menggunakan algoritma kriptografi RSA. Algoritma RSA merupakan algoritma kriptografi asimetris dimana kunci enkripsi tidak sama dengan kunci dekripsinya. Untuk mengenkripsi dan dekripsi dengan menggunakan algoritma RSA, maka terlebih dahulu membangkitkan sepasang kunci, yaitu kunci publik (*public key*) dan kunci privat (*private key*). Adapun algoritma untuk membangkitkan kunci publik (*public key*) dan kunci privat (*private key*) algoritma RSA yaitu sebagai berikut:

- Pilih dua buah bilangan prima sembarang untuk p dan q, misalkan p = 11 dan q = 23.
- 2. Hitung nilai *n* sehingga diperoleh hasilnya:

n = p * qn = 11 * 23 = 253

3. Hitung nilai *totient* (φ) sehingga diperoleh hasilnya yaitu:

 $\varphi(n) = (p-1)(q-1)$ $\varphi(n) = (11-1)(23-1)$ $\varphi(n) = 10 * 22 = 220$

4. Pilih sembarang bilangan e sebagai kunci publik yang relatif prima terhadap φ(n) yaitu 1 > e < φ(n) dan gcd(e,φ(n)) = 1. Karena e mempunyai ketentuan e > 1 dan e < φ(n), maka e dimulai dari e = 2,3,...,n

Misalkan dipilih e = 3 karena relatif prima dengan $\varphi(n) = 220$. Pembuktian, gcd(3, 220) = 1 sehingga nlai e yang digunakan yaitu e = 3

5. Hitung kunci privat, disebut namanya *d* sedemikian agar $d * e \mod \varphi(n) = 1$ Dengan mencoba nilai-nilai d = 1, 2, 3, ..., n

Misalkan dipilih nilai d = 147 yang memenuhi syarat $d * e \mod \varphi(n) = 1$ Pembuktian, $d * e \mod \varphi(n) = 147 * 3 \mod 220 = 1$ sehingga nlai d yang digunakan yaitu d = 147.

Berdasarkan hasil perhitungan diatas maka diperoleh pasangan kunci publik dan kunci privat algoritma RSA sebagai berikut:

- 1. Kunci enkripsi (*public key*) adalah pasangan (n, e) = (253, 3)
- 2. Kunci dekripsi (*private key*) adalah pasangan (n, d) = (253, 147)

Dengan mengambil hasil enkripsi *Beaufort Cipher (ciphertext1)* maka proses enkripsi dengan menggunakan kunci publik algoritma RSA dapat dilakukan dengan menggunakan persamaan (2.4) adalah sebagai berikut:

- 1. Ambil kunci publik (*public key*) algoritma RSA yang telah dibangkitkan sebelumnya, yaitu pasangan (n, e) = (253, 3).
- 2. Ambil *plaintext* (m_i) yang merupakan hasil enkripsi *Beaufort Cipher (ciphertext1)* kemudian susun menjadi blok-blok $m_1, m_2, m_3, ..., m_n$, lalu konversi bentuk desimal dalam tabel ASCII sehingga:

 $m_1 = c = 99$

$$m_{2} = j = 106$$

$$m_{3} = z = 122$$

$$m_{4} = j = 106$$

$$m_{5} = b = 98$$

$$m_{6} = p = 112$$

$$m_{7} = c = 99$$

$$m_{8} = v = 118$$

$$m_{9} = a = 97$$

$$m_{10} = c = 99$$

$$m_{11} = q = 113$$

3. Enkripsi *plaintext* (m_i) menggunakan persamaan (2.4), sehingga hasilnya:

$$c_i = m_i^e \mod n$$

 $c_1 = 99^3 \mod 253 = 44$
 $c_2 = 106^3 \mod 253 = 145$
 $c_3 = 122^3 \mod 253 = 67$
 $c_4 = 106^3 \mod 253 = 145$
 $c_5 = 98^3 \mod 253 = 32$
 $c_6 = 112^3 \mod 253 = 19$
 $c_7 = 99^3 \mod 253 = 44$
 $c_8 = 118^3 \mod 253 = 50$
 $c_9 = 97^3 \mod 253 = 102$
 $c_{10} = 99^3 \mod 253 = 44$
 $c_{11} = 113^3 \mod 253 = 38$
Berdasarkan hasil perhitungan diatas maka diperoleh hasil enkripsi

(*ciphertext*2) dengan menggunakan kunci publik algoritma RSA dalam bentuk bilangan desimal yang masing-masing hasil enkripsi akan disipsahkan dengan tanda titik adalah 44.145.67.145.32.19.44.50.102.44.38.

Adapun perbandingan pesan teks sebelum dan setelah di enkripsi dengan menggunakan algoritma *Beaufort Cipher* dan algoritma RSA dapat disajikan pada tabel 4.2.

File Teks	Plaintext	kriptografi
	Size	11 * 8 = 88 bit
Hasil Enkrinsi <i>Regufort</i>	Ciphertext	cjzjbpcvacq
nush Elixipsi Deuajori	Size	11 * 8 = 88 bit
Hasil Enkrinsi RSA	Ciphertext	44.145.67.145.32.19.44.50.102.44.38
	Size	25 * 8 = 200 bit

Tabel 4.2 Perbandingan Hasil Enkripsi

Sesuai tabel 4.2, maka dapat disimpulkan bahwa setelah di enkripsi melalui dua tahapan proses enkripsi maka diperoleh *ciphertext* yang lebih acak serta tidak memperlihatkan hubungan antara *plaintext* dengan *ciphertext*, karena hasil enkripsi kedua dengan algoritma RSA akan dikodekan kedalam nilai desimal sehingga tingkat keamanan pesan dapat ditingkatkan, akan tetapi akan menghasilkan *ciphertext* yang lebih besar dari teks aslinya, yaitu 200 *bit* (25 karakter), oleh karena itu perlu dikompresi untuk memperkecil ukurannya.

4.1.2 Analisis Proses Dekripsi

Setelah *ciphertext* diperoleh, maka selanjutnya akan dilakukan proses dekripsi yang bertujuan untuk mengembalikan pesan sudah di enkripsi pada langkah sebelumnya. Proses dekripsi merupakan kebalikan dari proses enkripsi yaitu untuk mentransformasi *ciphertext* ke dalam bentuk yang dapat dimengerti



Gambar 4.4 Skema Proses Dekripsi

Sesuai gambar 4.4 terdapat dua proses utama yang dilakukan dalam melakukan proses dekripsi. Proses pertama yaitu melakukan dekripsi menggunakan kunci privat algoritma RSA sehingga menghasilkan *ciphertext*1, lalu hasil dari proses tersebut akan di dekripsi lagi dengan menggunakan kunci algoritma *Beaufort Cipher* sehingga menghasilkan *plaintext* sebagai hasil akhir dari proses dekripsi.

Proses dekripsi dengan menggunakan kunci privat algoritma RSA dapat dilakukan dengan menggunakan persamaan (2.5) yaitu sebagai berikut:

- 1. Ambil kunci privat (*private key*) algoritma RSA yaitu (n, d) = (253, 147).
- 2. Ambil *ciphertext* (c_i) yang akan didekripsi (dalam hal ini *ciphertext* merupakan hasil dari proses enkripsi sebelumnya yaitu *ciphertext*2) kemudian nyatakan menjadi blok-blok $c_1, c_2, c_3, \dots, c_n$.

	$c_1 = 44$				
	$c_2 = 145$				
	$c_3 = 67$				
4) -	$c_4 = 145$				
	$c_{5} = 32$				
	$c_{6} = 19$				
	$c_7 = 44$				
	$c_8 = 50$				1
	$c_9 = 102$				P.
	$c_{10} = 44$	UNIVERSIT	AS ISLAM NEG	ERI	
3.	$c_{11} = 38$ Setiap blok c	i akan didekrips	i menjadi blok m	i dengan menggunaka	n
	persamaan (2.5), sehingga hasilny	ya:		
	$m_i = c_i^d mod$	n			
	$m_1 = 44^{147} m$	10d 253 = 99			
	$m_2 = 145^{147}$	$mod \ 253 = 106$			

- $m_3 = 67^{147} \mod 253 = 122$
- $m_4 = 145^{147} \mod 253 = 106$

$$\begin{split} m_5 &= 32^{147} \mod 253 = 98 \\ m_6 &= 19^{147} \mod 253 = 112 \\ m_7 &= 44^{147} \mod 253 = 99 \\ m_8 &= 50^{147} \mod 253 = 118 \\ m_9 &= 102^{147} \mod 253 = 97 \\ m_{10} &= 44^{147} \mod 253 = 99 \\ m_{11} &= 38^{147} \mod 253 = 113 \end{split}$$

Berdasarkan hasil perhitungan diatas maka diperoleh hasil dekripsi (*ciphertext*) algoritmaRSA yang jika dikonversi kedalam karakter pada tabel ASCII akan diperoleh hasil seperti pada tabel 4.3.

Tabel 4.3 Konversi Desimal Kedalam T	abel ASCII
--------------------------------------	------------

	Desimal	Karakter ASCII	
	99	с	
	106	j	
	122	Z	
	106	j	
	98	b	
	112	р	
	99	с	
	118	V	
	97	а	
U	NIVE99SITA!	S ISLAM NEGE	RI
SUMA	TE 113	JTARA M	EDAN

Berdasarkan tabel 4.3 maka diperoleh hasil dekripsi pertama dengan algoritma RSA yaitu "cjzjbpcvacq" yang merupakan hasil enkripsi algoritma *Beaufort Cipher (ciphertext1)*. Hasil dari proses dekripsi pertama (*ciphertext1*) kemudian akan di dekripsi lagi dengan menggunakan algoritma kriptografi *Beaufort Cipher* untuk mendapatkan kembali *file* teks aslinya (*plaintext*). Adapun *ciphertext1* dan kunci *Beaufort Cipher* untuk proses dekripsi tahap kedua yaitu:

Panjang *ciphertext*1 = 11, sedangkan panjang kunci = 7, karena panjang kunci *Beaufort Cipher* < panjang *ciphertext*1, maka kunci *Beaufort Cipher* tersebut akan diulang secara periodik hingga panjang kunci tersebut sama dengan panjang *ciphertext*1, yaitu:

Ciphertext1 (C_i) c j z j b p c v a c q Kunci Beaufort (K_i) m a h y u d i m a h y

Pada contoh diatas kunci *Beaufort Cipher* "mahyudi" diulang sedemikian rupa hingga panjang kunci sama dengan panjang *ciphertext*1. Kemudian setelah panjang kunci sama dengan panjang *ciphertext*1, proses enkripsi dilakukan terlebih dahulu akan dikonversi ke desimal pada tabel ASCII sehingga hasilnya dapat disajikan pada tabel 4.4.

<i>Ciphertext</i> 1 (C _i)	с	j	Z	j	b	p	с	v	a	с	q
Nilai Desimal	99	106	122	106	98	112	99	118	97	99	113
Kunci (Ki)	m	a	h	у	u	d	i	m	a	h	у
Nilai Desimal	109	97	104	121	117	100	105	109	97	104	121

Tabel 4.4 Proses Mengubah Ciphertext1 Menjadi Desimal

Setelah *ciphertext*1 dikonversi menjadi desimal, maka proses dekripsi algoritma *Beaufort Cipher* dapat dilakukan dengan menggunakan rumus pada persamaan (2.2) sehingga diperoeleh hasilnya sebgai berikut:

Untuk karakter $(C_1) = c$ dan kunci $(K_1) = m$

 $M_1 = (K_1 - C_1) \mod 26 = (m - c) \mod 26 + 97$

= (109 - 99) mod 26 + 97

= 107 (huruf "k" dalam tabel ASCII)

Untuk karakter $(C_2) = j$ dan kunci $(K_2) = a$

 $M_2 = (K_2 - C_2) \mod 26 = (a - j) \mod 26 + 97$

 $= (97 - 106) \mod 26 + 97$

= 114 (huruf "r" dalam tabel ASCII) Untuk karakter $(C_3) = z$ dan kunci $(K_3) = h$ $M_3 = (K_3 - C_3) \mod 26 = (h - z) \mod 26 + 97$ $= (104 - 122) \mod 26 + 97$ = 105 (huruf "i" dalam tabel ASCII) Untuk karakter $(C_4) = j$ dan kunci $(K_4) = y$ $M_4 = (K_4 - C_4) \mod 26 = (y - j) \mod 26 + 97$ $= (121 - 106) \mod 26 + 97$ = 112 (huruf "p" dalam tabel ASCII) Untuk karakter (C₅) = b dan kunci (K₅) = u $M_5 = (K_5 - C_5) \mod 26 = (u - b) \mod 26 + 97$ $= (117 - 98) \mod 26 + 97$ = 116 (huruf "t" dalam tabel ASCII) Untuk karakter $(C_6) = p$ dan kunci $(K_6) = d$ $M_6 = (K_6 - C_6) \mod 26 = (d - p) \mod 26 + 97$ $= (100 - 112) \mod 26 + 97$ = 111 (huruf "o" dalam tabel ASCII) Untuk karakter $(C_7) = c$ dan kunci $(K_7) = i$ $M_7 = (K_7 - C_7) \mod 26 = (i - c) \mod 26 + 97$ $= (105 - 99) \mod 26 + 97$ = 103 (huruf "g" dalam tabel ASCII) Untuk karakter (C_8) = v dan kunci (K_8) = m $M_8 = (K_8 - C_8) \mod 26 = (m - v) \mod 26 + 97$ $= (109 - 118) \mod 26 + 97$ = 114 (huruf "r" dalam tabel ASCII) Untuk karakter $(C_9) = a$ dan kunci $(K_9) = a$ $M_9 = (K_9 - C_9) \mod 26 = (a - a) \mod 26 + 97$ $= (97 - 97) \mod 26 + 97$ = 97 (huruf "a" dalam tabel ASCII) Untuk karakter $(C_{10}) = c$ dan kunci $(K_{10}) = h$

 $M_{10} = (K_{10} - C_{10}) \mod 26 = (h - c) \mod 26 + 97$ = (104 - 99) mod 26 + 97 = 102 (huruf "f" dalam tabel ASCII) Untuk karakter (C_{11}) = q dan kunci (K_{11}) = y $M_{11} = (K_{11} - C_{11}) \mod 26 = (y - q) \mod 26 + 97$ = (121 - 113) mod 26 + 97 = 105 (huruf "i" dalam tabel ASCII)

Berdasarkan hasil perhitungan diatas seteleh melakukan proses dekripsi dengan menggunakan algoritma *Beaufort Cipher* untuk tahap kedua maka diperoleh kembali *plaintext* aslinya yaitu "kriptografi".

4.2 Perancangan Sistem

Perancangan *interface* atau tampilan antarmuka pengguna sistem pada aplikasi ini berguna sebagai perantara komunikasi pengguna dengan sistem. Sistem dibangun berbasis *web* dengan menggunakan bahasa pemrograman *php*. *Interface* yang akan dirancang pada sistem ini memiliki enam bagian utama, yaitu halaman utama (*home*), halaman bangkitkan kunci, halaman enkripsi, halaman dekripsi, halaman *help*, dan halaman *about*.

4.2.1 Perancangan Halaman Utama

Halaman utama merupakan halaman pembuka yang akan ditampilkan pertama kali saat aplikasi dijalankan. Gambar 4.5 merupakan rancangan *interface* dari halaman utama sistem.



Gambar 4.5 Rancangan Interface Halaman Utama

4.2.2 Perancangan Halaman Bangkitkan Kunci

Halaman bangkitkan kunci merupakan sebuah *form* yang dirancang untuk membangkitkan kunci publik (*public key*) dan kunci privat (*private key*) dari algoritma RSA. Kunci publik digunakan untuk mengenkripsi pesan teks, sedangkan kunci privat digunakan untuk mendekripsi pesan teks. Rancangan *interface* dari halaman bangkitkan kunci dapat disajikan pada gambar 4.6.

Home	Generate Key Home-Banykovan Kuno	
Bangkilkan Kunci	Bangkilkan Kunci Publik dan Kunci Privat Algoritma RSA	Cek Bilangan Prima
Enkripsi	Bilangan Prima p Bilangan Prima g	Masukkan Angka
Dekripsi		
Help	Auto Generate Key Generale Key Save Public Key Save Private Key	Cek Angke
About	Nilai n = ip * q) Nilai Tuluent = (p-1)(q-1)	
	Nılşi ç Nılşi (l	
	Vurse Buddik in al Kurse Buddin al	

Gambar 4.6 Rancangan Interface Halaman Bangkitkan Kunci

4.2.3 Perancangan Halaman Enkripsi

Halaman enkripsi merupakan sebuah *form* yang dirancang untuk melakukan proses enkripsi pesan dalam *file* teks (*plaintext*) dengan menggunakan kombinasi algoritma kriptografi simetris *Beaufort Cipher* dan algoritma kriptografi asimetris RSA dalam skema super enkripsi. Adapun rancangan *interface* dari halaman enkripsi dapat disajikan pada gambar 4.7.

Home	Enknpsi Holle: Frans
Bangkitkan Kunci	Enkripsi Plainteks Dengan Algoritma Beaufort Cipher dan RSA
Enkripsi	Read Kunci Puplik RSA
Dekripsi	Masukkan File Teks (Planteks)
Help	Chocse File
About	
	Masukkan Kunci Beaufort Cipher
	Enkripsi Beaufori Enkripsi RSA Simpan Cipherleks
	Hasil Enkripsi (Cipherteks) Beaufori Cipher Hasil Enkripsi (Cipherteks) RSA
_	Footer

Gambar 4.7 Rancangan Interface Halaman Enkripsi UNIVERSITAS ISLAM NEGERI

4.2.4 Perancangan Halaman Dekripsi

Halaman dekripsi dirancang untuk melakukan proses dekripsi *file* teks (*ciphertext*) dengan menggunakan kombinasi algoritma kriptografi *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi. Adapun rancangan *interface* dari halaman dekripsi dapat disajikan pada gambar 4.8.

	E (100) Mahyudi
Home	Dekripsi Home: Dekrips
Bangkilkan Kunci	Dekripsi Cipherteks Dengan Algoritma Beaufort Cipher dan RSA
Enknipsi	Road Kund Privet RSA
Dekripsi	Masukkan File Teks (Ciphonets)
Help	Choose File
About	
	Masuktan Kunci Beaufort Cipher
	Dokrips/Beaufort Simpan Plainteks
	Haşil Dekirçisi (Plumtoks) RSA Haşil Dekirçisi (Plumtoks) Beavfort Cipher
	Footer

Gambar 4.8 Rancangan Interface Halaman Dekripsi

4.2.5 Perancangan Halaman Help

Halaman *help* dirancang untuk menampilkan informasi mengenai proses bangkitkan kunci, proses enkripsi dan proses dekripsi yang terdapat pada aplikasi yang dibuat. Adapun rancangan *interface* dari halaman *help* dapat dilihat pada gmbar 4.9.

	Ξ			(lcai)	Mahyudi
Ноте	Help Heme/Use:/Help				
Bangkitkan Kunci	Bangkitkan Kunci	Enkripsi	Dekripsi		
Enkripsi		1			
Deknipsi					
Неір			content		
About					
	L				
			Fooler		

Gambar 4.9 Rancangan Interface Halaman Help

4.2.6 Perancangan Halaman About

Halaman *about* dirancang untuk menampilkan informasi singkat mengenai *profile user* pada aplikasi yang dibuat. Adapun rancangan *interface* dari halaman *about* dapat dilihat pada gmbar 4.10.

(laga) UINSU	Ξ	(icon) Mahyudi
Home Bangkitkan Kunci Enkripsi Dekripsi Help About	Profile Home/User/Abot: icon Mahyudi 0701152115	Overview content
		Footer

Gambar 4.10 Rancangan Interface Halaman About

4.3 Implementasi Program

Implementasi program merupakan tahapan yang dilakukan setelah perancangan sistem dan pembuatan *flowchart* sistem. Setelah selesai menganalisis dan membuat rancangan dari sistem yang akan dibangun, selanjutnya adalah mengimplementasikan hasil analisis dan perancangan ke dalam bentuk aplikasi dengan menggunakan bahasa pemrograman. Implementasi program dalam penelitian dibuat berbasis *web* yang terdiri dari enam buah halaman, yaitu halaman utama, halaman bagkitkan kunci, halaman enkripsi, halaman dekripsi, halaman *help*, dan halaman *about*. Adapun ruang lingkup spesifikasi kebutuhan perangkat lunak dan perangkat keras yang digunakan saat membangun dan menjalankan aplikasi ini dapat dilihat penjelasannya pada bab tiga.

4.3.1 Implementasi Halaman Utama

Halaman utama atau halaman *home* berfungsi sebagai tampilan utama pada saat aplikasi dijalankan. Pada halaman utama terdapat lima buah menu yang yang dapat diakses oleh *user* yaitu terdiri dari menu bangkitkan kunci, menu enkripsi, menu dekripsi, menu *help*, dan menu *about*. Gambar 4.11 merupakan tampilan dari halaman utama.

uin UINSU	=	Mahyud
88 Home	Dashboard Home / Dashboard	
🗁 Bangkitkan Kunci		
Enkripsi	Implementasi Kombinasi Algoritma Beaufo Dalam Skema Super Enkripsi Untuk	ort Cipher dan Algoritrma RSA Pengamanan File Teks
Dekripsi		
PAGES		
() Help		
About		
	Mahyudi 0701162010	
	Program Studi Ilmu K Fakultas Sains dan Te Universitas Islam Negeri St Medan - 2022	fomputer oknologi umatera Utara 2
	¥ 000	
	© Copyrght NiceAdmin. All Rig Decimed by Bostorius	ihis Reserved
W.	Gambar 4.11 Tampilan Halamar	n Utama

4.3.2 Implementasi Halaman Bangkitkan Kunci

Halaman bangkitkan kunci berfungsi untuk membangkitkan kunci publik (*public key*) dan kunci privat (*private key*) dari algoritma RSA. Kunci publik digunakan untuk mengenkripsi pesan (*plaintext*) yang terdapat dalam *file* teks dengan format *.*txt*, sedangkan kunci privat digunakan untuk mendekripsi pesan (*ciphertext*) yang terdapat dalam *file* teks dengan format *.*txt*. Gambar 4.12 merupakan tampilan dari halaman bangkitkan kunci.

88 Home	Generate Key Home / Bangkitkan Kunel RBA		
 Bangkitkan Kunci Eskrinei 	Bangkilkan Kanci Publik dan Ka	anci Privat Algoritma RSA	Cek Bilangan Prima
Enknpsi	Bilangan Prima p	Bilangan Prima q	Masukkan Angka
d Dekripsi	Nilai p	Nilmi q	
D Help	CAulti Generate Key	Senerale Key	🛞 Celt Angka
About	Nitai $n = (p * q)$	Nilai Totient = (p - 1)(q - 1)	
	Nilai e	Nilar d	
	Kunci Publik (n, e)	Kunci Privat (n, d)	
	0	0	

Gambar 4.12 Tampilan Halaman Bangkitkan Kunci

4.3.3 Implementasi Halaman Enkripsi

Halaman enkripsi berfungsi untuk melakukan proses enkripsi pesan (*plaintext*) yang terdapat dalam *file* teks dengan format *.*txt* dengan menggunakan kombinasi algoritma kriptografi *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi. Gambar 4.13 merupakan tampilan dari halaman enkripsi.

	Home / Enkripsi			
ingkitkan Kunci	Enkripsi Plainteks Dengan Algoritma I	Jeaufort Cipher dan RSA		
kripsi	Design of the second			
kripsi	C Read Kunca Putaik RSA	Kunci Publik RSA (n)	Kunci Publik RSA (e)	
	Masukkan File Teks (Plainteks)			
lp	Choose File No file chosen			
put	Diaintale			
	Masukkan Kunci Beautort Cipher			
	Masukkan Kunci Beaufort Cipher			
	Masukkan Kunci Beaufort Cipher Kunci Beaufort Cipher			
	Masukkan Kunci Beautort Cipher Kunci Beautort Cipher	C Envripsi Beautori	6)	
	Masukkan Kunci Beautort Cipher Kunci Beautort Cipher Hasil Enkinpsi (Cipherteks) Beaufort I	Strompsk Beautyri) (Strompsk RS	A) [⊘Sempan Conchens] I Enkripsi (Copherteks) RSA	
	Masukkan Kunci Beaufort Cipher Kunci Beaufort Cipher Hasil Enkingsi (Cipherteks) Beaufort I Cipherteks Beaufort Cipher	C Enropsi Beautor C Enropsi RS	n [⊘senpan conenera] I Enkripsi (Coherteka) RSA polarteka RSA	
	Masukkan Kunci Beaufort Cipher Kunci Beaufort Cipher Hasil Enkripsi (Cipherfeks) Beaufort f Cipherfeks Beaufort Cipher	C Enropsi Beautor C Enropsi RS	n [⊘Senpan Cpherters] # Erkripsi (Cpherteks) RSA abenteks RSA	
	Masukkan Kunci Beaufort Cipher Kunci Beaufort Cipher Hasil Enkirpsi (Cipherfeks) Beaufort f Cipherfeks Beaufort Cipher	(⊘ Enwood Seautor) (⊘ Enwood Has Spiner Has	A Concernant Contentens Il Enkripsi (Contenteks) RSA phanteks RSA	
	Masukkan Kunci Beaufort Cipher Kunci Beaufort Cipher Hasil Enkirgsi (Cipherteks) Beaufort I Cipherteks Beaufort Cipher	(⊘ Envirgiu Seaufor) (⊘ Envirgiu Has Dipher Has	A) Sampan Coheners Il Enforpsi (Cohenteks) RSA pherteks RSA	

Gambar 4.13 Tampilan Halaman Enkripsi

4.3.4 Implementasi Halaman Dekripsi

Halaman dekripsi berfungsi untuk melakukan proses dekripsi pesan (*ciphertext*) yang terdapat dalam *file* teks dengan format *.*txt* dengan menggunakan kombinasi algoritma kriptografi *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi. Gambar 4.14 merupakan tampilan dari halaman dekripsi.

5 Home	Dekripsi Home / Dekripsi
Bangkitkan Kunci	Dekrinsi Cinherteks Densen Altoritma RSA dan Beaufort Cinher
Enkripsi	account from and from the second band of the second s
Dekripsi	Read Kunci Putvit RSA Kunci Putvit RSA (n) Kunci Putvit RSA (d)
ES	Masukkan File Teks (Cipherteks)
Help	Choose File No file chosen
About	Cipherteks
	Kunci Beaufort Cipher
	Plainteks RSA Plainteks Beaufort Cipher
	© Copyright NiceAdmin: A# Rights Reserved

Gambar 4.14 Tampilan Halaman Dekripsi

4.3.5 Implementasi Halaman HelpAS ISLAM NEGERI

Halaman *help* berfungsi untuk menampilkan informasi panduan kepada *user* mengenai proses dalam membangkitkan kunci algoritma RSA, proses enkripsi dan proses dekripsi yang terdapat pada aplikasi yang dibuat. Gambar 4.15 merupakan tampilan dari halaman *help*.



Gambar 4.15 Tampilan Halaman Help

4.3.6 Implementasi Halaman About

Halaman *about* berfungsi untuk menampilkan informasi singkat mengenai *profile* pembuat aplikasi yang berisi mengenai nama lengkap, alamat, nomor telepon, dan alamat email. Gambar 4.16 merupakan tampilan dari halaman *about*.

	-		V •	nyuur
88 Home	Home / Users / About			
Bangkitkan Kunci		Overview		
Dekripsi		About		
PAGES		Lorem (psum dolor si	t amet, consectetur adipisiong elit, sed do eiusmod tempor inciditunt ut labo	re
[] Help	Mahyudi 0701162010	et dolore magna aliqu aliquip ex éa commo	ui. Ut enim ad minim veniam, quis nostrud exercitation ullamod laboris nai u 30	2
About	900	Profile Details		
		Nama Lengkap	Mahyudi	
		Alamat	Medan	
		Phone	08boox	
		Email	mahyudi@gmail.com	
		Copyright NiceAdr Designed by	nin. All Rights Reserved BootstrapMade	Ť

Gambar 4.16 Tampilan Halaman About

4.4 Hasil Pengujian

Hasil pengujian merupakan hasil dari pengujian kemampuan atau keakuratan metode yang digunakan dalam menyelesaikan masalah yang diteliti. Dalam hal ini, penerapan skema super enkripsi dengan menggunakan kombinasi algoritma kriptografi *Beaufort Cipher* dan algoritma RSA yang telah dibangun akan diuji dengan menggunakan sampel data atau *file* uji. Objek yang menjadi inputan data sebagai sampel data pada pengujian ini adalah berupa *file* teks berformat *.*txt* dengan *size* atau ukuran yang beragam.

4.4.1 Hasil Pengujian Bangkitkan Kunci

Setelah memilih menu "Bangkitkan Kunci" yang terdapat pada halaman utama, maka sistem akan menampilkan halaman bangkitkan kunci untuk proses membangkitkan kunci publik (*public key*) dan kunci privat (*private key*) algoritma asimetris RSA. Terdapat dua cara yang dapat dilakukan untuk membangkitkan kunci algoritma RSA pada aplikasi yang dibangun, yaitu dengan membangkitkan kunci secara otomatis atau dengan cara secara manual dengan mengisikan langsung dua buah bilangan prima p dan q pada *textbox* masing-masing yang tersedia pada halaman bangkitkan kunci.

Dalam membangkitkan kunci algoritma RSA secara manual, maka *user* harus menginputkan terlebih dahulu dua buah bilangan prima p dan q, selanjutnya *user* dapat menekan tombol "Generate Key". Jika bilangan yang dimasukkan bukan bilangan prima maka sistem akan menampilkan pesan *error* dan *user* harus memasukkan ulang untuk bilangan prima p dan q. Jika bilangan yang dimasukkan merupakan bilangan prima maka sistem akan menampilkan kunci publik (public key) dan kunci privat (*private key*) algoritma RSA. Adapun cara kedua untuk membangkitkan kunci yaitu dengan menekan tombol "Auto Generate Key" dan sistem akan menampilkan pada masing-masing *textbox* p dan q serta sistem akan menampilkan kunci publik (*public key*) dan kunci privat (*private key*) algoritma RSA seperti terlihat pada gambar 4.17.

Home	Generate Key Home / Bangkitkan Kunci RSA		
- Bangkitkan Kunci	Banekitkan Kunci Publik dan Kunci Pri	val Algoritma RSA	Cek Bilangan Prima
Enkripsi	plangradan ranka s sank alan nama i n	Val Puger and Tearly	oon coungains minit.
Dekripsi	Bilangan Prima p	Bilangan Prima q	Masukkan Angka
GE1	11	23	
Help	🕑 Auto Generale Key 🖉 Generate	Key Save Public Key Save Private Key	🕑 Cak Angka
About	Nitai n = (p * q)	Nilai Totient = (p - 1)(q - 1)	
	253	220	
	Nilai e	Nilai d	
	3	147	
	Kunci Publik (n, e)	Kunci Privat (n, d)	
	253, 3	253, 147	
	Running Time	0.00011110305786123 Delik	
		Copyright NiceAdmin, All Rights Reserved Designed by BoststrapMade	

Gambar 4.17 Hasil Pengujian Bangkitkan Kunci

Sesuai gambar 4.17, nilai bilangan prima yang dihasilkan untuk p = 11dan q = 23. Sedangkan untuk nilai n = 253 yang merupakan hasil dari p * q. Adapun kunci publik yang dihasilkan yaitu pasangan n dan e (253, 3) dan kunci privat yang dihasilkan yaitu pasangan n dan d (253, 147). Pasangan kunci yang berhasil dibangkitkan selanjutnya akan disimpan untuk keperluan proses enkripsi dan dekripsi. Untuk menyimpan pasangan kunci dapat dilakukan dengan memilih tombol "Save Public Key" untuk menyimpan kunci publik dan tombol "Save Private Key" untuk menyimpan kunci privat. Adapun tampilan dari pasangan kunci publik dan kunci privat algoritma RSA setelah berhasil disimpan dapat dilihat pada gambar 4.18.

KunciPublik - Notepad	_		<	💭 KunciPrivat - Notepad 🛛 🗖 🗆	\times	
File Edit Format View Help				File Edit Format View Help		
253 3			•	253 147		~
<		3		<	>	
Ln 2, Cc 100% Windows (CRLF)	UTF-8			Ln 2, Cc 100% Windows (CRLF) UTF-8		
(a)				(b)		

Gambar 4.18 Hasil Kunci Algoritma RSA (a) Kunci Publik (b) Kunci Privat

4.4.2 Hasil Pengujian Enkripsi

Setelah memilih menu "Enkripsi" yang terdapat pada halaman utama, maka sistem akan menampilkan halaman enkripsi untuk melakukan proses enkripsi pesan (*plaintext*) yang terdapat dalam *file* teks dengan menggunakan kombinasi algoritma *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi. Untuk memulai proses enkripsi, maka *user* terlebih dahulu memasukkan *file* kunci publik (*public key*) algoritma RSA yang telah dibangkitkan sebelumnya, yaitu dengan memilih tombol "*Read* Kunci Publik RSA" dan sistem akan menampilkan kunci publik pada masing-masing *textbox* yang terdapat pada halaman enkripsi. Tahap selanjutya memasukkan *file* teks yang akan di enkripsi dengan memilih tombol "*Choose File*" dan sistem akan menampilkan *preview* isi dari *file* teks yang dimasukkan pada *textbox plaintext*. Setelah itu dilanjutkan dengan memasukkan kunci algoritma *Beaufort Cipher* dan dilanjutkan dengan memilih tombol "Enkripsi Beaufort" dan sistem akan menampilkan hasil enkripsi pertama (*ciphertext*1) algoritma *Beaufort Cipher* seperti terlihat pada gambar 4.19.

UINSU	🚍 🕘 Mahyudi -
88 Home	Enkripsi Homa / Enkripsi
P Bangkitkan Kunci	Enlinesi Blaidhle: Donan Abasilon Donaled Fishte dan DCA
Enkripsi	Envirger Mannaks Derigen Adorante Dealmon Clover aun richt.
Dekripsi	Read Kunci Publik RSA 253 3
PAGES	Masukkan File Teks (Plainteks)
() Help	Choose File dil tut
	keranasaan, megritas dain, auerinkasi dari ketuadaan perinyangkalah. Kriptografi (Criptografi) (Criptografi) (Sriptografi) ketualas ruhani, terdiri dari dua suduk kata yalik ketup dari penping ketualasi kripto artinya meneyembunyikan, sedangkan grapha artinya tulisan sehingga , kriptografi dapat diartikan sebagai ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan Masukkan Kunci Beaufort Cipher mahyudi
	Centrops Beauforr Centrops RSA Sempan Cipherteka Hasil Enkiripsi (Cipherteka) RSA cipheneteka brifaed feenars idiologing transit Cipherteka RSA cipheneteka RSA
	(gypy)-two y gypy (gypy) (gypy
	© Copyright NiceAdmin: All Rights Reserved Designed by BootinpMade

Gambar 4.19 Hasil Pengujian Enkripsi Beaufort Cipher

Gambar 4.19 merupakan hasil pengujian enkripsi pada *file* teks dengan format *.*txt* menggunakan kunci algoritma *Beaufort Cipher*. *Input* data yang di uji menggunakan sampel data *file* uji1 dengan *size* 32 KB (*kilo bytes*). Hasil enkripsi pertama dari algoritma *Beaufort Cipher* kemudian akan di enkripsi lagi dengan memilih tombol "Enkripsi RSA" dan sistem akan menampilkan hasil enkripsi kedua (*ciphertext*2) sebagai hasil akhir dari proses enkripsi dalam skema super enkripsi. Adapun hasil enkripsinya dapat dilihat pada gambar 4.20.

88 Home	Enkripsi	
🖙 Bangkitkan Kunci	House I Elimited	
Enkripsi	Enlorpsi Plainteks Dangan Algoritma Beautort Cipher dan RSA	
Dekripsi	@ Read Kunci Publik RSA Kunci Publik RSA	SA (n) Kunci Publik RSA (e)
PAGER	Masukkan File Teks (Plaintieks)	
() Help	Choose File No file chosen	
3. About	Plainteks	
	Masukkan Kunci Beaufort Cipher	
	Kunci Beaufort Cipher	
	(2) Entempsi Bestufort	Enkripsi RSA Simpan Ciphetteks
	Hasil Enkripsi (Cipherteks) Beaufort Cipher	Hasi Enkripsi (Cipherteks) RSA
	Cipherteks Beaufort Cipiter	44 145 67 145 32 19 44 50 102 44 38 131 150 67 229 92 25 26 166 123 38 131 36 139 20 65 38 131 32 67 229 126 102 85 55 126 131 17 85 44 220 67 168 131 150 144 19 150 166
	Ranning Tim	n (d.S7423550746663) Dulix

Gambar 4.20 Hasil Pengujian Enkripsi RSA

Gambar 4.20 merupakan hasil pengujian enkripsi kedua dengan menggunakan kunci publik algoritma RSA. Karakter (*string*) yang terdapat pada *file* teks yang telah di enkripsi akan menghasilkan *ciphertext* dalam bentuk bilangan desimal dengan estimasi waktu enkripsi selama 0.579 ms (*millisecond*). *Ciphertext* yang dihasilkan dari proses enkripsi kedua dengan menggunakan algoritma RSA akan terlihat acak dan tidak memiliki makna karena hasil enkripsi dalam bentuk bilangan desimal, sehingga keamanan dan kerahasiaan sebuah informasi pada *file* teks dapat terjaga karena tidak memperlihatkan korelasi antara *plaintext* dengan *ciphertext*.

4.4.3 Hasil Pengujian Dekripsi

Setelah memilih menu "Dekripsi" yang terdapat pada halaman utama, maka sistem akan menampilkan halaman dekripsi untuk melakukan proses dekripsi pesan (*ciphertext*) yang terdapat dalam *file* teks dengan menggunakan kombinasi algoritma *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi. Untuk memulai proses dekripsi, maka *user* terlebih dahulu memasukkan *fîle* kunci privat (*private key*) algortima RSA yang telah dibangkitkan sebelumnya, yaitu dengan memilih tombol "*Read* Kunci Privat RSA" dan sistem akan menampilkan kunci privat pada masing-masing *textbox* yang terdapat pada halaman dekripsi. Tahap selanjutya memasukkan *file* teks (*ciphertext*) yang akan di dekripsi dengan memilih tombol "*Choose File*" dan sistem akan menampilkan *preview* isi dari *fîle* teks yang dimasukkan pada *textbox ciphertext*. Setelah itu dilanjutkan dengan memasukkan kunci algoritma *Beaufort Cipher* dan dilanjutkan dengan memilih tombol "Dekripsi RSA" dan sistem akan menampilkan hasil dekripsi pertama algoritma RSA seperti terlihat pada gambar 4.21.

招 Home	Dekripsi Rome / Dekripsi	
- Bangkitkan Kunci	Dekripsi Cipherteks Dengan Algoritma RSA dan Beaufort Cipher	
Enkripsi		
Dekripsi	© Reat: Kunci Publik RSA (n) Kunci Publik RSA (d)	
NGES	Masukkan File Teks (Cipherteks)	
) Help	Choose File No file chosen	
& About	Cipherteks	
		1
	Masukkan Kunci Beaufort Cipher	
	Kunci Beaufort Cipher	
	O Bennpsi HSA	
	Hasil Dekripsi (Plainteks) RSA Hasil Dekripsi (Plainteks) Beaufort Cipher	
	cjzjbpcvacq izrsthoug gtgeg bzrfaeyf kecnzo idpiohfml kmnb	
	cjzjbpcvacg izrsthoug gługed bzrfaeyt kecnzo idpiołnimi knnub (gmymso vągomn hgtzy cwhmugiz inyb) geioui wyhmgmula uwsudka cwgyndgeahl, mgiugąbdą jacy, ujpinocąkdę xhl	
	cjzippovacq izrsihoug qtgeq bzrfaeyt kecnzo idpiohfmi knnb fqmymso vqqcmin hgfzy cwhmuqiz inyb) qeioui wyhmqmula uwsudka cwyndgeahl, mgiuqqbdq jaoy, ujpincqkdqe xhl kzpeaeyuq tinyhxymphi. Kmaxhtsddde (yqafkugjhjinf)	
	cizipbocvacq izisihouq qitgeq berfaeyi kecizi idpiotifmi kinni fiqmymiso vqqcmn hgtzy civihmuqiz iniyoji qeioui vikmiqmula uwsadka cwqyndpeahl, mghuqabda jagov, ujpiinoqkdge xhi kzpeaeyuq tiniytxymphi. Kmaxtitisidde (yqafkugihini)	

Gambar 4.21 Hasil Pengujian Dekripsi RSA

Gambar 4.21 merupakan hasil pengujian dekripsi pada *file* teks (*ciphertext*) dengan menggunakan kunci privat algoritma RSA. Hasil dekripsi pertama dari algoritma RSA kemudian akan di dekripsi lagi dengan memilih tombol "Dekripsi *Beaufort*" dan sistem akan menampilkan hasil dekripsi kedua (*plaintext*) sebagai hasil akhir dari proses dekripsi dalam skema super enkripsi. Adapun hasil dekripsinya dapat dilihat pada gambar 4.22.

Home	Dekripsi Home / Dekrosi
Bangkitkan Kunci	Dekrossi Coherteks Densen Alsonitma RSA des Resultert Circher
Enkripsi	 Wondolise Schutzetande ender allerite allerite and a new statement of history.
Dekripsi	(2) Read Kunci Privat RSA Kunci Publik RSA (n) Kunci Publik RSA (d)
GES	Masukkan File Teks (Cipherteks)
Help	Choose File No file chosen
About	Cipbedeks
	Masukkan Kunci Beaufort Cipher
	mahyudi
	C Dekripsi RSA
	manyud:
	manyud: (C) Dekripsi IRSA (C) Dekripsi Beautori (C) Simpan Plainteks Hasil Dekripsi (Plainteks) RSA ojzjópcvacq izrsihouq qigeq bzrfaeyf kecnzo idpiohtmi kmbi famymso vąqemi hgfzy cwhnugiz intycj ąeiou wyhngmula wsucka cwqyndqeahl, mgbiuqdbq jaoy, upincqdkdg xhl kzpeaeyuq thyltxymphi Kmaartisddia (yqdkugnjint) Hasil Dekripsi (Plainteks) Beaufort Cipher kriptografi merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan sudu isistem informasi kezpedayuq thyltysymphi (Kmaartisddia (yqdkugnjint)

Gambar 4.22 Hasil Pengujian Dekripsi Beaufort Cipher

Gambar 4.22 merupakan hasil pengujian dekripsi kedua dengan menggunakan kunci *Beaufort Cipher*. Karakter (*string*) yang terdapat pada *file* teks yang telah di dekripsi akan menghasilkan *plaintext* yang sama persis dengan *file* teks aslinya dengan estimasi waktu enkripsi selama 0.433 ms (*millisecond*).

4.4.4 Hasil Pengujian Black box Testing

Pengujian *black box (black box testing)* adalah salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas, khususnya pada *input* dan *output* aplikasi (apakah sudah sesuai dengan apa yang diharapkan atau belum). Pengujian dengan metode *black box testing* dilakukan dengan cara memberikan sejumlah *input* pada program. *Input* tersebut kemudian diproses sesuai dengan kebutuhan fungsionalnya untuk melihat apakah program aplikasi dapat menghasilkan *output* yang sesuai dengan yang diinginkan dan sesuai pula dengan fungsi dasar dari program tersebut. Apabila dari *input* yang diberikan, proses dapat menghasilkan *output* yang sesuai dengan kebutuhan fungsionalnya, maka program yang dibuat sudah benar, tetapi apabila *output* yang dihasilkan tidak sesuai dengan kebutuhan fungsionalnya, maka program tersebut, dan selanjutnya dilakukan penelusuran perbaikan untuk memperbaiki kesalahan yang terjadi.

Adapun hasil pengujian *black box testing* sistem dapat diuraikan sebagai berikut:

1. Black box Testing Bangkitkan Kunci

Berikut adalah hasil *black box testing* pada proses bangkitkan kunci publik (*public key*) dan kunci privat (*private key*) algoritma RSA yang dapat disajikan pada tabel 4.5.

No.	Kasus Uji	Langkah Uji	Hasil	Status
1.	Bangkitkan Kunci SUMA	Membangkitkan kunci dengan memilih tombol "Auto Generate Key" atau memilih tombol "Generate Key"	Sistem dapat membangkitkan kunci secara otomatis atau dengan menentukan sendiri bilangan prima untuk membangkitkan kunci	N
2.	Simpan Kunci	Menyimpan kunci dengan memilih tombol " <i>Save</i> <i>Public Key</i> " dan tombol " <i>Save</i> <i>Private Key</i> "	Sistem dapat menyimpan kunci publik dan kunci privat kedalam <i>file</i> teks dengan format *. <i>txt</i>	

Tabel 4.5 Black box Testing Bangkitkan Kunci

Tabel 4.5 pengujian *black box testing* dalam proses bangkitkan kunci, kasus pengujian yang dilakukan antara lain "Bangkitkan Kunci" dan "Simpan Kunci" dengan status hasil pengujian berhasil.

2. Black box Testing Enkripsi

Berikut adalah hasil *black box testing* pada proses enkripsi yang dapat disajikan pada tabel 4.6.

No.	Kasus Uji	Langkah Uji	Hasil	Status
1.	<i>Input</i> Kunci Publik RSA	Mengimport <i>file</i> kunci publik RSA dengan memilih tombol " <i>Read</i> Kunci Publik RSA"	Sistem dapat membaca dan menampilkan isi dari <i>file</i> kunci publik algoritma RSA	
2.	<i>Input File</i> Teks	Mengimport <i>file</i> teks dengan memilih tombol " <i>Choose</i> <i>File</i> "	Sistem hanya dapat menerima format <i>file</i> . <i>txt</i> dan sistem dapat menampilkan isi dari <i>file</i> teks	
3.	Input Kunci Beaufort Cipher	Memasukkan kunci Beaufort Cipher	Sistem dapat menerima kunci	5
4.	Enkripsi Beaufort Cipher	Mengenkripsi <i>file</i> teks dengan memilih tombol "Enkripsi <i>Beaufort</i> "	Sistem dapat menampilkan hasil enkripsi algoritma Beaufort Cipher	Ν
5.	Enkripsi RSA	Mengenkripsi hasil Beaufort Cipher dengan memilih tombol "Enkripsi RSA"	Sistem dapat menampilkan hasil enkripsi algoritma RSA	

Tabel 4.6 Black box Testing Enkripsi

Simpan		Menyimnan hasil	Sistem dapat
	enkripsi dengan	menyimpan hasil	
6.	Ciphertext	memilih tombol "Simpan <i>Cipherteks</i> "	enkripsi (ciphertext)
			kedalam <i>file</i> baru
			dengan format *. <i>txt</i>

Tabel 4.6 pengujian *black box testing* dalam proses enkripsi, kasus pengujian yang dilakukan antara lain "*Input* Kunci Publik RSA", "*Input File* Teks", "*Input* Kunci *Beaufort Cipher*", "Enkripsi *Beaufort Cipher*", "Enkripsi RSA", dan "Simpan *Ciphertext*".

3. Black box Testing Dekripsi

Berikut adalah hasil *black box testing* pada proses dekripsi yang dapat disajikan pada tabel 4.7.

No.	Kasus Uji	Langkah Uji	Hasil Sta	tus
1.	<i>Input</i> Kunci Privat RSA	Mengimport <i>file</i> kunci privat RSA dengan memilih tombol " <i>Read</i> Kunci Privat RSA"	Sistem dapat membaca dan menampilkan isi dari <i>file</i> kunci privat algoritma RSA	
2.	Input File Teks	Mengimport <i>file</i> teks (<i>ciphertext</i>) dengan memilih tombol " <i>Choose File</i> "	Sistem hanya dapat menerima format <i>file</i> *. <i>txt</i> dan sistem dapat menampilkan isi dari <i>file</i> teks	
3.	Input Kunci Beaufort Cipher	Memasukkan kunci Beaufort Cipher	Sistem dapat menerima kunci	

Tabel 4.7	Black box	Testing	Dekripsi

4.	Dekripsi RSA	Mendekripsi <i>file</i> <i>ciphertext</i> dengan memilih tombol "Dekripsi RSA"	Sistem dapat menampilkan hasil dekripsi algoritma RSA
5.	Dekripsi Beaufort Cipher	Mendekripsi <i>file</i> <i>ciphertext</i> dengan memilih tombol "Dekripsi <i>Beaufort</i> "	Sistem dapat menampilkan hasil dekripsi algoritma <i>Beaufort Cipher</i>
6.	Simpan <i>Plaintext</i>	Menyimpan hasil dekripsi dengan memilih tombol "Simpan <i>Plaintext</i> "	Sistem dapat menyimpan hasil dekripsi (<i>plaintext</i>) kedalam <i>file</i> baru dengan format *. <i>txt</i>

Tabel 4.7 pengujian *black box testing* dalam proses dekripsi, kasus pengujian yang dilakukan antara lain "*Input* Kunci Privat RSA", "*Input File* Teks", "*Input* Kunci *Beaufort Cipher*", "Dekripsi RSA", "Dekripsi *Beaufort Cipher*", dan "Simpan *Plaintext*".

UNIVERSITAS ISLAM NECPenguji, SUMATERA UTARA MEDAN