Jurnal CyberTech

Vol.4. No.6, Juni 2021, pp. xx~xx
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Implementasi Algoritma Rsa Untuk Keamanan Data Mutasi Pada PT. SSSS Kuala Tanjung

Dalia *, Badrul Anwar **, Dedi Setiawan***

* Program Studi Sistem Informasi, STMIK Triguna Dharma
** Program Studi Sistem Komputer, STMIK Triguna Dharma
*** Program Studi Teknik Komputer, STMIK Triguna Dharma

Article Info

Article history:
Received Jun 12th, 201x

Keyword:
Mutasi, Kriptografi, Metode RSA

ABSTRACT

Data mutasi merupakan salah satu data yang bersifat rahasia pada PT.SSSS Kuala Tanjung. Belum adannya pengamanan pada data saat proses pengiriman data mutasi tersebut, sehingga menyebabkan tingginnya ancaman terhadap data-data penting dan rahasia tersebut. Untuk mengatasi masalah pengamanan data pada PT.SSSS tersebut dibutuhkan ilmu kriptografi. Kriptografi merupakan salah satu ilmu dalam pengamanan data, banyak metode yang digunakan didalamnya salah satunya ialah metode RSA (Rivest Shamir Adlemen). Algoritma ini termasuk ke dalam algoritma kriptografi asimetris (Asymetric Cryptography), yaitu algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi yaitu dengan menggunakan public key dan private key. Public key digunakan untuk mengenkripsi pesan dan didekripsi dengan menggunakan private key. RSA merupakan algoritma kriptografi yang paling sering digunakan karena sangat sulit untuk dipecahkan. Maka dalam pengamanan data mutasi pegawai pada PT.SSSS Kuala Tanjung digunakan kriptografi dengan metode RSA (Rivest Shamir Adlemen). Penelitian ini menghasilkan aplikasi sistem yang dapat membantu manager KSA di PT.SSSS Kuala Tanjung didalam penanganan masalah pengamanan dan pengarsipan pada data mutasi karyawan. Dengan konsep kriptografi yang merupakan sebuah program yang mampu mengamankan dan mengarsipkan data mutasi sehingga dapat mengurangi ancaman terhadap penyalahgunaan data.

First Author
Nama : Dalia
Program Studi : Sistem Informasi
Kampus : STMIK Triguna Dharma
Email : daliakhan890@gmail.com

1. PENDAHULUAN

Karyawan merupakan aset terpenting dalam sebuah perusahaan ataupun organisasi yang memiliki pengaruh sangat besar terhadap kesuksesan sebuah perusahaan ataupun organisasi tersebut. karyawan juga dapat diartikan sebagai setiap orang yang memberikan jasa kepada perusahaan ataupun organisasi yang membutuhkan jasa ataupun tenaga kerja, yang mana dari jasa tersebut, karyawan akan mendapatkan balas jasa berupa gaji dan kompensasi-kompensasi lainnya. PT.SSSS (Sumatra Sarana Sekar Sakti) Kuala Tanjung merupakan perusahaan Nasional yang bergerak dibidang usaha jasa pengangkutan. Didalam perusahan tersebut sering terjadi perputaran karyawan ataupun mutasi karyawan. Mutasi karyawan dapat terlaksana apabila

PT.SSSS (Sumatra Sarana Sekar Sakti) Kuala Tanjung sudah mengirimkan data karyawan yang akan dimutasi dan mendapat persetujuan ataupun perintah langsung dari kantor pusat di Medan.

Mutasi adalah suatu unsur yang sering terjadi di dalam suatu perusahaan dan organisasi. Seperti diketahui, mutasi adalah suatu perubahan posisi/ jabatan/ tempat/ pekerjaan yang dilakukan oleh pimpinan pusat kepada seseorang yaitu karyawan (manajemen dan non-manajemen) baik secara promosi (kenaikan pangkat) / demosi (pemindahan suatu jabatan ke jabatan yang lebih rendah) di dalam suatu perusahaan ataupun organisasi hal ini merupakan salah satu bagian dari pengembangan sumber daya manusia (SDM)[1].

Data mutasi pada PT. SSSS (Sumatera Sarana Sekar Sakti) Kuala Tanjung adalah salah satu data yang bersifat rahasia, hanya pihak-pihak tertentu saja yang dapat menerima dan membaca data mutasi itu, sehingga pentingnya pengamanan pada data mutasi tersebut. Dalam hal ini PT.SSSS (Sumatra Sarana Sekar Sakti) Kuala Tanjung belum memiliki pengamanan pada data mutasi sehingga data mutasi tersebut rentan terhadap pencurian dan manipulasi data.

Untuk mengatasi permasalahan diatas dapat memanfaatkan ilmu dan perkembangan teknologi saat ini, khususnya dalam bidang pendidikan. Informasi dan data dapat dengan mudah dan cepat untuk dikirim melalui jaringan komputer. Hal ini tentu saja dapat menimbulkan risiko jika informasi dan data yang dikirim dapat diakses oleh pihak-pihak yang tidak berhak sehingga mengakibatkan kebocoran data. Salah satu teknologi yang dapat mengatasi permasalahan diatas adalah ilmu kriptografi.

Dalam kriptografi terdapat beberapa metode dalam proses mengamankan data atau informasi. Untuk penyelesaian kasus atau permasalahan yang telah dijelaskan di atas maka dapat menggunakan algoritma RSA untuk mengamankan data mutasi tersebut.

2. KAJIAN PUSTAKA

2.1 Mutasi

Mutasi adalah suatu perubahan posisi/ jabatan/ tempat/ pekerjaan yang dilakukan baik secara horizontal maupun vertikal di dalam suatu organisasi. Pada dasarnya mutasi termasuk dalam fungsi pengembangan karyawan, karena tujuannya untuk meningkatkan efisiensi dan efektivitas kerja dalam perusahaan tersebut[2]. Mutasi dibagi menjadi 2 bagian yaitu, mutasi horizontal dan mutasi vertical. Mutasi horizontal adalah mutasi tempat dan mutasi jabatan. Mutasi tempat *(tour of area)* adalah perubahan tempat kerja, tetapi tanpa perubahan jabatan, posisi, ataupun golongannya. Mutasi jabatan *(tour of duty)* adalah perubahan jabatan pada posisi semula, sedangkan mutasi vertikal adalah perubahan posisi, jabatan dan pekerjaan. Terjadinya mutasi disebabkan oleh dua hal utama yaitu mutasi karena permintaan dari diri pegawai yang bersangkutan ataupun permintaan perusahaan dengan persetujuan pimpinan perusahaan untuk meningkatkan produktifitas perusahaan[3].

2.2 *Kriptografi*

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan, tanda tangan digital dan keaslian pesan dengan sidik jari digital[4].

Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti pihak lain[5].

Untuk dapat menjalankan dengan baik pada proses kriptografi haruslah terdapat empat elemen utama didalamnya, yang paling berkait satu sama lain. Yaitu :

1. *PlainText* merupakan sebagai pesan awal atau pesan asli yang dikirim pada proses komunikasi. *PlainText* inilah yang kemudian di *enkripsi* dan *deskripsi*.
2. *CipherText* merupakan pesan yang tersembunyi, yaitu pesan asli (*PlainText*) yang telah di *enkripsi* dengan proses kriptografi. *CipherText* ini dapat diubah kembali kebentuk aslinya (*PlainText*) memanfaatkan *Key* yang telah di sediakan.
3. *Cryptography Key* merupakan kunci yang digunakan untuk melakukan *enkripsi* dan *deskripsi* pada proses kriptografi. Tanpa adanya kunci (*key*) yang sama maka proses *enkripsi* dan *deskripsi* tidak dapat dilakukan dengan baik. Kunci (*key*) merupakan informasi yang dapat menjadi kendali terhadap proses terjadinya kriptografi.

4. *Encryption Decryption Algorithm* merupakan komponen terakhir yang juga sama pentingnya dalam proses kriptografi adalah algoritma yang di gunakan untuk *enkripsi* dan *dekripsi*. *Enkripsi* adalah proses mengubah *plaintext* menjadi *chipertext*. Sedangkan *dekripsi* adalah proses mengubah *chipertext* menjadi *plaintext.*

2.3 *Algoritma RSA (Rivest Shamir Adleman)*

Algoritma kriptografi RSA atau singkatan dari Ron Rivest, Adi Shamir and Leonard Adleman. Algoritma ini termasuk ke dalam algoritma kriptografi asimetris (*Asymetric Cryptography*), yaitu algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi yaitu dengan menggunakan *public key* dan *private key*. *Public key* digunakan untuk mengenkripsi pesan dan didekripsi dengan menggunakan *private key*. Prosesnya, pengirim (*sender*) mengenkripsi pesan dengan menggunakan *public key* milik penerima pesan (*receiver*) dan hanya penerima pesanlah yang dapat mendekripsi pesan karena hanya penerima yang mengetahui *private key* nya sendiri[6].

Pada algoritma RSA terdapat tiga proses yaitu, pembangkitan kunci, proses enkripsi dan proses dekripsi. Letak kesulitan pada algoritma RSA 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 $p \neq q$[7].

Teknik operasi pembangkitan kunci pada RSA adalah sebagai berikut:

1. Memilih dua bilangan prima berbeda p dan q.
   - Untuk alasan keamanan, bilangan p dan q dipilih secara random.
2. Compute $n = pq$. Hitung n = p . q
   - n digunakan sebagai modulus kunci publik dan kunci privat.
3. Hitung $\varphi(n) = (p - 1)(q - 1)$, dimana φ is fungsi euler tosien
4. Pilih sebuah bilangan bulat e sehingga $1 < e < \varphi(n)$ dan faktor pembagi terbesar dari $(e, \varphi(n)) = 1$; i.e., e dan $\varphi(n)$ are relatif prima.
   - e digunakan sebagai eksponen kunci publik.
   - e mempunyai panjang bit yang pendek dan berat Hamming yang ringan menghasilkan hasil yang lebih efisien dalam enkripsi - umumnya 0x10001 = 65,537. Namun demikian, semakin kecil nilai e (such as 3) semakin kecil pula tingkat keamanan di hal– hal tertentu.
5. Berdasar technet.microsoft.com, pene-rapan RSA di dalam pertukaran kunci adalah dengan cara mengenkripsi kun-ci privat dari pesan dengan mengguna-kan kunci publik hasil pembang-kitan dari RSA dan pesan berisi kunci itu dapat dibuka hanya dengan kunci privat hasil pembangkitan RSA yang dimiliki oleh penerima pesan[7].

3. METODOLOGI PENELITIAN

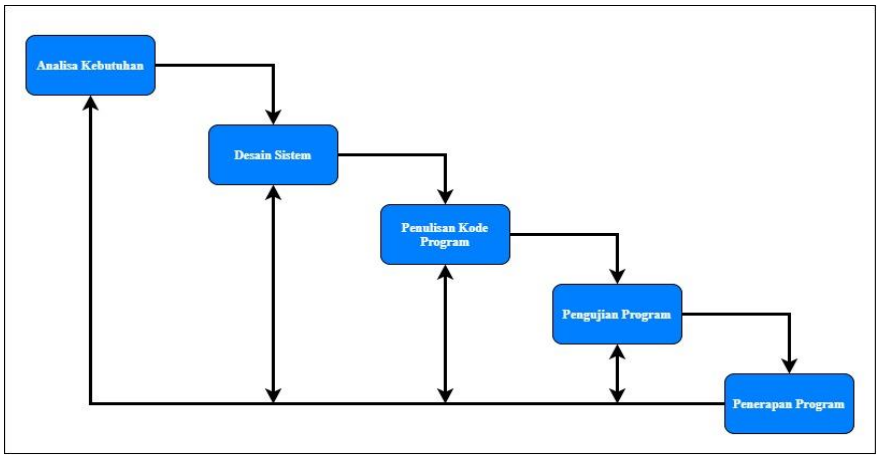
3.1 Metode Penelitian

Motode penelitian adalah salah satu cara yang digunakan untuk mengumpulkan data. Metode penelitian merupakan cara yang digunakan untuk memperoleh data menjadi informasi akurat dengan masalah yang diteliti.

1. Observasi, Adalah teknik pengumpulan informasi atau data dengan melakukan tinjauan langsung ketempat studi kasus dimana akan dilakukan penelitian. Oleh sebab itu, peneliti melakukan tinjauan langsung ke PT. SSSS Kuala Tanjung untuk mengetahui masalah yang terjadi dan apa solusi untuk kendala yang dihadapi mengenai keamanan data mutasi Karyawan pada PT. SSSS Kuala Tanjung.
2. Wawancara, Adalah kegiatan Tanya jawab secara lisan untuk memperoleh suatu informasi. Oleh sebab itu peneliti melakukan wawancara langsung dengan Ka.PGA/Hrd Dept (*Human Resource Department)* suatu bagian yang mempunyai wewenang dalam mengatur sumber daya Manusia (SDM).

3.2 Model Pengembangan Sistem

Model pengembangan sistem merupakan salah satu unsur penting dalam penelitian. Dalam model pengembangan sistem, yang paling khusus adalah *software* atau perangkat lunak, tetapi dapat juga diadopsi beberapa metode diantaranya algoritma *waterfall* atau algoritma air terjun.



Gambar 3.1 Metode *Waterfall*

3.3 Algoritma Sistem

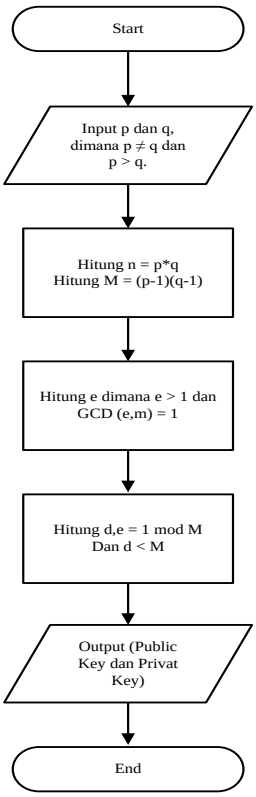
Algoritma sistem merupakan urutan langkah-langkah yang dilakukan dalam penyelesaian suatu masalah berdasarkan elemen-elemen yang saling integrasi dengan dituangkan kedalam bentuk kalimat untuk mencapai tujuan yang telah ditetapkan. Sehingga algoritma sistem yang jelas dan teratur sangat diperlukan dalam penyelesaian perancangan perangkat lunakAlgoritma

3.3.1 *Flowchart* Metode RSA

Flowchart merupakan keterangan yang lebih rinci tentang bagaimana prosedur sesungguhnya yang dilakukan pada suatu program. Berikut ini adalah *Flowchart* metode RSA:

1. Proses Pembangkitan Kunci

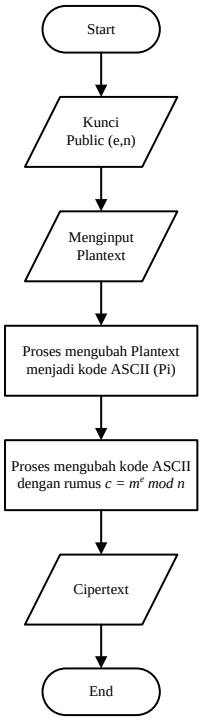
Dalam tahap ini adalah proses pembangkitan kunci. Dalam algorima RSA terdapat dua buah kunci berbeda yaitu *public key* dan *privat key*. Berikut *Flowchart* dari proses pembangkitan kunci



Gambar 3.2 *Flowchart* Proses Pembangkitan Kunci

2. Proses Enkripsi

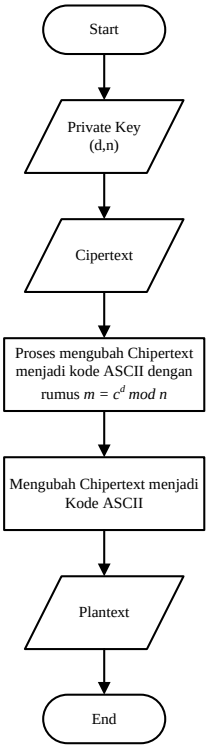
Proses enkripsi merupakan proses untuk mengubah data sumber menjadi file ciphertext dengan menggunakan nilai-nilai kunci enkripsi dan kunci publik yang telah dihasilkan sebelumnya. Berikut *Flowchart* dari proses *enkripsi*



Gambar 3.3 *Flowchart enkripsi*

3. Proses Dekripsi

Proses dekripsi adalah proses untuk mengembalikan ciphertext kedalam bentuk plaintext, dengan menggunakan kunci pribadi dekripsi dan kunci public. Berikut *Flowchart* dari proses *dekripsi*



Gambar 3.4 *Flowchart dekripsi*

3.3.2 Perhitungan Metode RSA

Perhitungan Metode RSA ini merupakan penjelasan langkah – langkah penyelesaian masalah dalam penerapan *Security* Sistem untuk keamanan data mutasi karyawan pada PT.SSSS. Berikut ini langkah yang dilakukan dalam perhitungan:

1. Proses Pembangkit Kunci RSA

Proses enkripsi algoritma Rivest Shamir Adleman (RSA) adalah sebagai berikut:

a. Pilih dua bilangan prima sembarang *p* dan *q* , $p \neq q$.
Nilai (*p*) = 17 dan
nilai (*q*) = 11.

b. Hitung *n* = *p*q*. Bilangan *n* disebut *parameter*.
*P * q = n*
*17 * 11 = 187*

c. Hitung Hitung $\varphi(n)$ = (p - 1)(q – 1).
$(p-1)(q-1) = \varphi(n)$
(17-1)(11-1) = $\varphi(n)$
(16)(10) = 160

d. Pilih nilai *e* dengan syarat *e* > 1 dan *greatest comman divisior* (*e,160*) = 1
Nilai *e* yang di ambil adalah 7.

e. Hitung *d* hingga *d,e* = 1 (mod 160) dan *d* < 160
d * 7 = 1 mod 160
d * 7 mod 160 =1
d = 23
jadi 23 * 7 mod 160 = 1
Sehingga pasangan kunci yang didapat adalah :
Kunci *enkripsi* (*public key*) (*e,n*) = (7, 187) dan
Kunci *dekripsi* (*private key*) (*d,n*) = (23, 187)

2. Proses *Enkripsi*

Proses enkripsi adalah suatu proses yang mengubah plainteks (kode sesungguhnya) menjadi ciperteks (kode rahasia). Untuk merubah plainteks ke ciperteks digunakan fungsi matematika dan kunci. Pada proses enkripsi ini, penulis menggunakan nomor surat keputusan mutasi sebagai *plaintext*. Sebagai contoh kode surat yaitu: 0001/SPT/SSSS/HRD-HO/I/2021.

Langkah pertama yang harus dilakukan adalah merubah *plaintext* menjadi format ASCII. berikut ini adalah penyelesaiannya:

ASCII table

Char	Dec	Oct	Hex	Char	Dec	Oct	Hex	Char	Dec	Oct	Hex	Char	Dec	Oct	Hex
(nul)	0	0000	0x00	(sp)	32	0040	0x20	@	64	0100	0x40	`	96	0140	0x60
(soh)	1	0001	0x01	!	33	0041	0x21	A	65	0101	0x41	a	97	0141	0x61
(stx)	2	0002	0x02	"	34	0042	0x22	B	66	0102	0x42	b	98	0142	0x62
(etx)	3	0003	0x03	#	35	0043	0x23	C	67	0103	0x43	c	99	0143	0x63
(eot)	4	0004	0x04	$	36	0044	0x24	D	68	0104	0x44	d	100	0144	0x64
(enq)	5	0005	0x05	%	37	0045	0x25	E	69	0105	0x45	e	101	0145	0x65
(ack)	6	0006	0x06	&	38	0046	0x26	F	70	0106	0x46	f	102	0146	0x66
(bel)	7	0007	0x07	'	39	0047	0x27	G	71	0107	0x47	g	103	0147	0x67
(bs)	8	0010	0x08	(	40	0050	0x28	H	72	0110	0x48	h	104	0150	0x68
(ht)	9	0011	0x09	)	41	0051	0x29	I	73	0111	0x49	i	105	0151	0x69
(nl)	10	0012	0x0a	*	42	0052	0x2a	J	74	0112	0x4a	j	106	0152	0x6a
(vt)	11	0013	0x0b	+	43	0053	0x2b	K	75	0113	0x4b	k	107	0153	0x6b
(np)	12	0014	0x0c	,	44	0054	0x2c	L	76	0114	0x4c	l	108	0154	0x6c
(cr)	13	0015	0x0d	-	45	0055	0x2d	M	77	0115	0x4d	m	109	0155	0x6d
(so)	14	0016	0x0e	.	46	0056	0x2e	N	78	0116	0x4e	n	110	0156	0x6e
(si)	15	0017	0x0f	/	47	0057	0x2f	O	79	0117	0x4f	o	111	0157	0x6f
(dle)	16	0020	0x10	0	48	0060	0x30	P	80	0120	0x50	p	112	0160	0x70
(dc1)	17	0021	0x11	1	49	0061	0x31	Q	81	0121	0x51	q	113	0161	0x71
(dc2)	18	0022	0x12	2	50	0062	0x32	R	82	0122	0x52	r	114	0162	0x72
(dc3)	19	0023	0x13	3	51	0063	0x33	S	83	0123	0x53	s	115	0163	0x73
(dc4)	20	0024	0x14	4	52	0064	0x34	T	84	0124	0x54	t	116	0164	0x74
(nak)	21	0025	0x15	5	53	0065	0x35	U	85	0125	0x55	u	117	0165	0x75
(syn)	22	0026	0x16	6	54	0066	0x36	V	86	0126	0x56	v	118	0166	0x76
(etb)	23	0027	0x17	7	55	0067	0x37	W	87	0127	0x57	w	119	0167	0x77
(can)	24	0030	0x18	8	56	0070	0x38	X	88	0130	0x58	x	120	0170	0x78
(em)	25	0031	0x19	9	57	0071	0x39	Y	89	0131	0x59	y	121	0171	0x79
(sub)	26	0032	0x1a	:	58	0072	0x3a	Z	90	0132	0x5a	z	122	0172	0x7a
(esc)	27	0033	0x1b	;	59	0073	0x3b	[	91	0133	0x5b	{	123	0173	0x7b
(fs)	28	0034	0x1c	<	60	0074	0x3c	\	92	0134	0x5c	|	124	0174	0x7c
(gs)	29	0035	0x1d	=	61	0075	0x3d	]	93	0135	0x5d	}	125	0175	0x7d
(rs)	30	0036	0x1e	>	62	0076	0x3e	^	94	0136	0x5e	~	126	0176	0x7e
(us)	31	0037	0x1f	?	63	0077	0x3f	_	95	0137	0x5f	(del)	127	0177	0x7f

Gambar 3.5 Table ASCII

Tabel 3.1 Tabel Karakter untuk di Encrypt

Plaintext	Kode ASCII	*Plaintext*	Kode ASCII
0	48	H	72
0	48	R	82
0	48	D	68
1	49	-	45
/	47	H	72
S	83	O	79
P	80	/	47
T	84	I	73
/	47	/	47
S	83	2	50
S	83	0	48
S	83	2	50
S	83	1	49
/	47		

Selanjutnya di*enkripsi* dengan rumus $c_i = m_i^e \ mod \ n$, yaitu sebagai berikut:

$C_1 = 48^7 \bmod 187$
$= 587.068.342.272 \bmod 187$
$= 159$
$C_2 = 48^7 \bmod 187$
$= 587.068.342.272 \bmod 187$
159
$C_3 = 48^7 \bmod 187$
$= 587.068.342.272 \bmod 187$
159
$C_4 = 49^7 \bmod 187$
$= 678.223.072.849 \bmod 187$
25
$C_5 = 47^7 \bmod 187$
$= 506.623.120.463 \bmod 187$
174
$C_6 = 83^7 \bmod 187$
$= 27.136.050.989.627 \bmod 187$
8
$C_7 = 80^7 \bmod 187$
$= 20.971.520.000.000 \bmod 187$
75
$C_8 = 84^7 \bmod 187$
$= 29.509.034.655.744 \bmod 187$
50
$C_9 = 47^7 \bmod 187$
$= 506.623.120.463 \bmod 187$
174
$C_{10} = 83^7 \bmod 187$
$= 27.136.050.989.627 \bmod 187$
8
$C_{11} = 83^7 \bmod 187$
$= 27.136.050.989.627 \bmod 187$
8
$C_{12} = 83^7 \bmod 187$
$= 27.136.050.989.627 \bmod 187$

8
$C_{13} = 83^7 \bmod 187$
$= 27.136.050.989.627 \bmod 187$
8
$C_{14} = 47^7 \bmod 187$
$= 506.623.120.463 \bmod 187$
174
$C_{15} = 72^7 \bmod 187$
$= 10.030.613.004.288 \bmod 187$
30
$C_{16} = 82^7 \bmod 187$
$= 24.928.547.056.768 \bmod 187$
91
$C_{17} = 68^7 \bmod 187$
$= 6.722.988.818.432 \bmod 187$
51
$C_{18} = 45^7 \bmod 187$
$= 373.669.453.125 \bmod 187$
122
$C_{19} = 72^7 \bmod 187$
$= 10.030.613.004.288 \bmod 187$
30
$C_{20} = 79^7 \bmod 187$
$= 19.203.908.986.159 \bmod 187$
139
$C_{21} = 47^7 \bmod 187$
$= 506.623.120.463 \bmod 187$
174
$C_{22} = 73^7 \bmod 187$
$= 11.047.398.519.097 \bmod 187$
61
$C_{23} = 47^7 \bmod 187$
$= 506.623.120.463 \bmod 187$
174
$C_{24} = 50^7 \bmod 187$
$= 781.250.000.000 \bmod 187$
118
$C_{25} = 48^7 \bmod 187$
$= 587.068.342.272 \bmod 187$
159
$C_{26} = 50^7 \bmod 187$
$= 781.250.000.000 \bmod 187$
118
$C_{27} = 49^7 \bmod 187$
$= 678.223.072.849 \bmod 187$
25

Maka, didapat hasil dari enkripsi sebagai berikut: 159, 159, 159, 25, 174, 8, 75, 50, 174, 8, 8, 8, 8, 174, 30, 91, 51, 122, 30, 139, 174, 61, 174, 118, 159, 118, 25.

Tabel 3.2 Hasil Encrypt

Plaintext	Kode ASCII	***Encrypt***	*Plaintext*	Kode ASCII	***Encrypt***
0	48	159	H	72	30
0	48	159	R	82	91

0	48	159	D	68	51
1	49	25	-	45	122
/	47	174	H	72	30
S	83	8	O	79	139
P	80	75	/	47	174
T	84	50	I	73	61
/	47	174	/	47	174
S	83	8	2	50	118
S	83	8	0	48	159
S	83	8	2	50	118
S	83	8	1	49	25
/	47	174			

Dari penjelasan diatas bahwasanya proses perhitungan Encrypt Metode RSA sudah dilakukan, dengan kata lain setelah Enkripsi dilakukan maka kebalikannya yaitu melakukan proses Deskripsi.

3. Proses Dekripsi

Proses dekripsi merupakan proses untuk mengembalikan kembali kalimat yang telah disandikan sebelumnya menjadi kalimat dalam bentuk yang dapat dipahami.

Selanjutnya yang harus dilakukan adalah merubah *ciphertext* menjadi format ASCII, didekripsi kembali dengan rumus $m_i = c_i^d \ mod \ n$, yaitu sebagai berikut:

$M_1 = 159^{23} \bmod 187$
$= 4{,}28680629091077690129220680975 05e+50$
$= 48$
$M_2 = 159^{23} \bmod 187$
$= 4{,}28680629091077690129220680975 05e+50$
$= 48$
$M_3 = 159^{23} \bmod 187$
$= 4{,}28680629091077690129220680975 05e+50$
$= 48$
$M_4 = 25^{23} \bmod 187$
$= 1{,}42108547152020037174224853515 63e+32$
$= 49$
$M_5 = 174^{23} \bmod 187$
$= 3{,}40904481528835456110377323637 3e+51$
$= 47$
$M_6 = 8^{23} \bmod 187$
$= 590.295.810.358.705.651.712$
$= 83$
$M_7 = 75^{23} \bmod 187$
$= 1{,}33785503673777839139802381396 29e+43$
$= 80$
$M_8 = 50^{23} \bmod 187$
$= 1{,}1920928955078125e+39$
$= 84$
$M_9 = 174^{23} \bmod 187$
$= 3{,}40904481528835456110377323637 3e+51$
$= 47$
$M_{10} = 8^{23} \bmod 187$
$= 590.295.810.358.705.651.712$
$= 83$
$M_{11} = 8^{23} \bmod 187$
$= 590.295.810.358.705.651.712$
$= 83$
$M_{12} = 8^{23} \bmod 187$
$= 590.295.810.358.705.651.712$

= 83
$M_{13} = 8^{23} \bmod 187$
= 590.295.810.358.705.651.712
= 83
$M_{14} = 174^{23} \bmod 187$
= 3,4090448152883545611037732363 73e+51
= 47
$M_{15} = 30^{23} \bmod 187$
= 9,4143178827e+33
= 72
$M_{16} = 91^{23} \bmod 187$
= 1,1427520877213404022237164128266e+45
= 82
$M_{17} = 51^{23} \bmod 187$
= 1,8798104097740619833503811636 49e+39
= 68
$M_{18} = 122^{23} \bmod 187$
= 9,6889364088008223881912242474922e+47
= 45
$M_{19} = 30^{23} \bmod 187$
= 9,4143178827e+33
= 72
$M_{20} = 139^{23} \bmod 187$
= 1,9468854787012822037132952643844e+49
= 79
$M_{21} = 174^{23} \bmod 187$
= 3,4090448152883545611037732363 73e+51
= 47
$M_{22} = 61^{23} \bmod 187$
= 1,1550122257958438859213857945791e+41
= 73
$M_{23} = 174^{23} \bmod 187$
= 3,4090448152883545611037732363 73e+51
= 47
$M_{24} = 118^{23} \bmod 187$
= 4,5007632431817730857819618235933e+47
= 50
$M_{25} = 159^{23} \bmod 187$
= 4,2868062909107769012922068097505e+50
= 48
$M_{26} = 118^{23} \bmod 187$
= 4,5007632431817730857819618235933e+47
= 50
$M_{27} = 25^{23} \bmod 187$
= 1,4210854715202003717422485351563e+32
= 49

Maka, didapat hasil dari dekripsi sebagai berikut: 48, 48, 48, 49, 47, 83, 80, 84, 47, 83, 83, 83, 83, 47, 72, 82, 68, 45, 72, 79, 47, 73, 47, 50, 48, 50, 49 dalam karakter ASCII adalah:

Tabel 3.3 Hasil *Decrypt*

Decrypt	Kode ASCII	*Decrypt*	Kode ASCII
48	0	72	H
48	0	82	R
48	0	68	D

49	1	45	-
47	/	72	H
83	S	79	O
80	P	47	/
84	T	73	I
47	/	47	/
83	S	50	2
83	S	48	0
83	S	50	2
83	S	49	1
47	/		

4. PEMODELAN DAN PERANCANGAN SISTEM

Pemodelan sistem merupakan sebuah gambaran perancangan dari sistem yang akan dibangun nantinya. Adapun diagram yang digunakan menggunakan pemodelan sistem dari UML (*Unified Modeling* Language) dengan diagram yang digunakan yaitu: *use case diagram, activity diagram* dan *class diagram.*

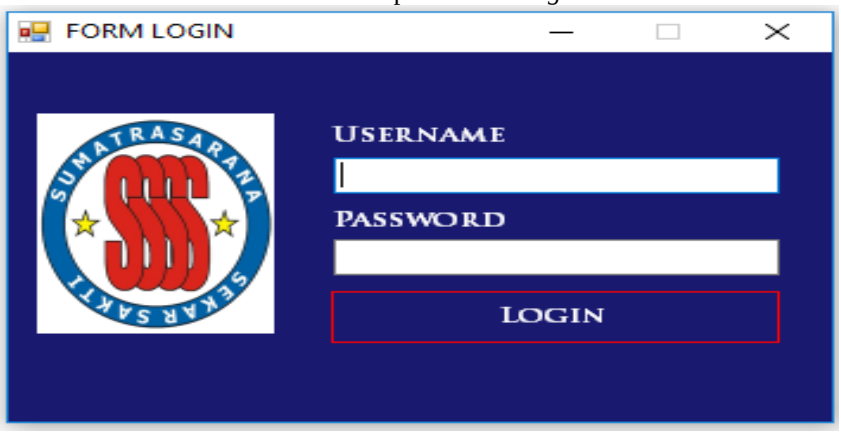
5. HASIL DAN PEMBAHASAN

Hasil Tampilan Antarmuka adalah tahapan dimana sistem atau aplikasi siap untuk dioperasikan pada keadaan yang sebenarnya sesuai dari hasil analisis dan perancangan yang dilakukan, sehingga akan diketahui apakah sistem atau aplikasi yang dirancang benar-benar dapat menghasilkan tujuan yang dicapai.

Aplikasi Sistem pengamanan data mutasi ini dilengkapi dengan tampilan yang bertujuan untuk memudahkan penggunanya. Pada aplikasi ini memiliki *interface* yang terdiri dari *Form Login, Form* Menu Utama, *Form* Kirim Data, *Form* Terima Data, *Form User, dan Form Logout.*

5.1 *Form Login*

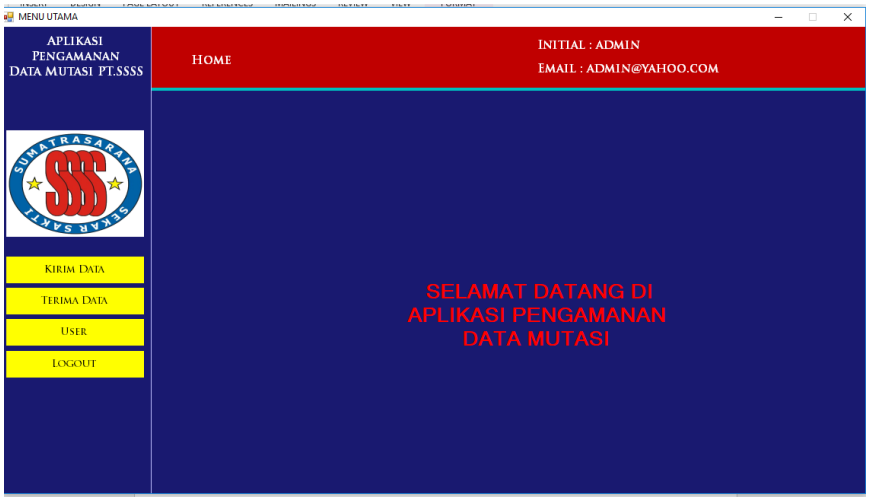
Form Login digunakan untuk mengamankan sistem dari *user-user* yang tidak bertanggung jawab sebelum masuk ke Menu Utama. Berikut adalah tampilan *Form Login* :



Gambar 5.1 *Form Login*

5.2 *Form* Menu Utama

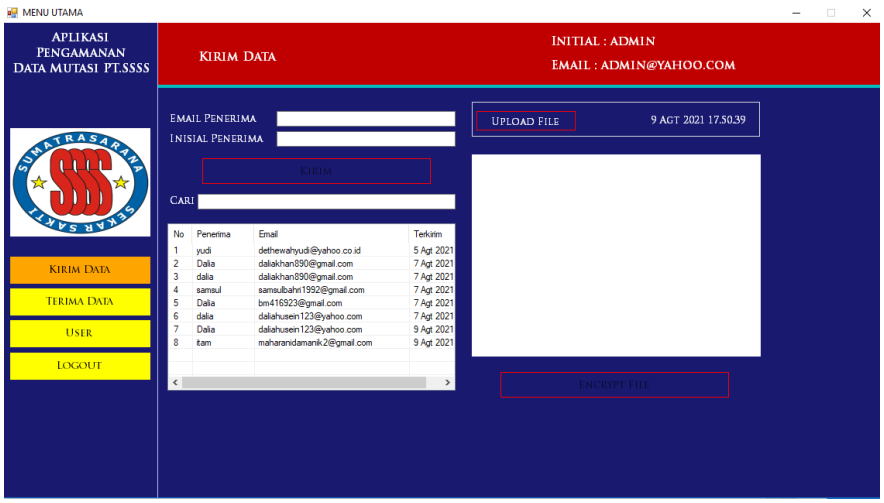
Form Menu Utama digunakan sebagai penghubung untuk *Form* Kirim Data, *Form* Terima Data, *Form User*, dan *Form Logout.* Berikut adalah tampilan *Form* Menu Utama :



Gambar 5.2 *Form* Menu Utama

5.3 *Form* Kirim Data

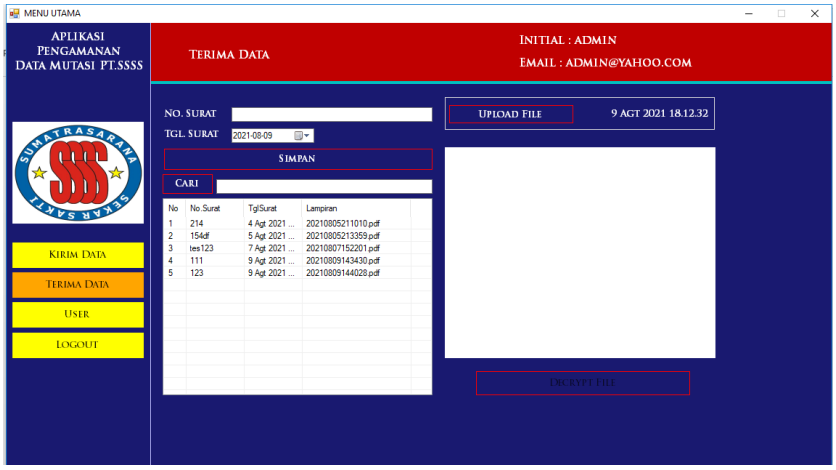
Form Kirim Data ini digunakan untuk melakukan *enkripsi* dan mengirim data. Berikut adalah tampilan *Form* Kirim Data :



Gambar 5.3 *Form* Kirim Data

5.4 *Form* Terima Data

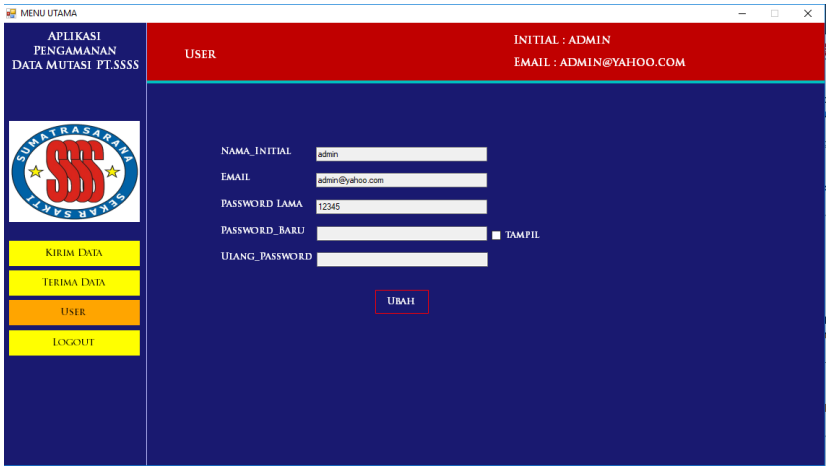
Form Terima Data ini digunakan untuk menerima data yang telah di *enkripsi*, kemudian di *dekripsi* sebelum di simpan. Berikut adalah tampilan *Form* Terima Data :



Gambar 5.4 *Form* Terima Data

5.5 Form User

Form user ini digunakan untuk memperbaiki data user. Berikut tampilan halaman *Form user* dapat dilihat pada gambar dibawah:



Gambar 5.5 *Form User*

6. KESIMPULAN DAN SARAN

Berdasarkan analisis pembahasan hasil penelitian tentang Implementasi Algoritma RSA Untuk Kamanan Data Mutasi Pada PT.SSSS Kuala Tanjung, maka dapat disimpulkan bahwa:

1. Sisitem pengamanan data yang dibangun dengan menggunakan metode *Rivest Shamir Adleman* (RSA) ternyata dapat memenyelesaikan masalah pengamanan data mutasi pada PT. SSSS Kuala Tanjung.
2. Sistem yang dirancang dalam pengamanan data dapat menyelesaikan masalah yang ada pada PT. SSSS Kuala Tanjung dan menjadi referensi penyelesaian masalah pengamanan data mutasi karyawan.
3. Dalam pengamanan data dapat meminimalisir terjadinya penyalahgunaan dan pencurian data serta dapat melindungi data pada saat proses pengiriman.

UCAPAN TERIMA KASIH

Puji syukur kehadirat Allah Subhanahu Wa Ta'ala atas izin-Nya yang telah melimpahkan karunia-Nya sehingga dapat menyelesaikan jurnal ilmiah ini dengan baik. Ucapan terima kasih teristimewa ditujukan untuk kepada Kedua orang tua yang selalu memberikan kasih sayang, doa, nasehat, serta atas kesabarannya yang luar biasa dalam setiap langkah hidup penulis, yang merupakan anugrah terbesar dalam hidup. Ucapan terima kasih

yang sebesar-besarnya kepada ketua yayasan STMIK Triguna Dharma, kepada Bapak Badrul Anwar, S.E, S.Kom, M.Kom selaku Dosen Pembimbing I (Satu) yang membimbing penulis selama melakukan penulisan Skripsi ini. Bapak Dedi Setiawan, S.Kom, M.Kom selaku Dosen Pembimbing II (Dua) yang membimbing penulis selama melakukan penulisan Skripsi ini. Seluruh Staff dan Karyawan/Karyawati STMIK Triguna Dharma. Bapak Harijanto Harun selaku PGA/HRD Dept PT.SSSS yang telah mengizinkan melakukan riset guna memenuhi data dan bahan yang dibutuhkan dalam menyelesaikan kasus yang diangkat dan seluruh teman-teman di STMIK Triguna Dharma yang telah berbagi dalam suka maupun duka dan membantu hingga terselesaikannya penelitian ini.

.

REFERENSI

[1] P. P. Kerja, M. D. A. N. Beban, P. T. Bank, S. Manado, J. Manajemen, and F. Ekonomi, "Kerja Terhadap Kinerja Karyawan Pada Effect of Job Placement , Mutation and Workload on Employee," vol. 16, no. 01, pp. 269–279, 2016.

[2] N. Ellyzar, "Konflik Interpersonal Terhadap Stress Kerja," *Magister Manaj. ISSN 2302-0199*, vol. 1, no. 1, pp. 35–45, 2017.

[3] E. Indrayuni, "Analisis Kepuasan Pelayanan Mutasi Pegawai Menggunakan Metode Fuzzy Service Quality (Servqual)," *Pilar Nusa Mandiri*, vol. 13, no. 2, pp. 157–166, 2017.

[4] A. Pradipta, "Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi," *Indones. J. Netw. Secur.*, vol. 5, no. 3, pp. 3–6, 2016.

[5] M. M. Amin, "Komunikasi Berbasis Teks," *J. Pseudocode*, vol. III, no. September, pp. 129–136, 2016.

[6] A. S. Indrawanti, A. W. Azinar, and M. A. Firdiansyah, "Secure E-Voting Menggunakan Metode Rsa Dan Autentikasi Rfid," *Netw. Eng. Res. Oper.*, vol. 4, no. 1, pp. 67–75, 2018, doi: 10.21107/nero.v4i1.113.

[7] L. Benny, "Analisis Dan Perancangan Aplikasi Kriptografi Keamanan File Berbasis Teks Dengan Menggunakan Metode Rsa," vol. 1, no. April P-ISSN : 2541-1322, pp. 15–23, 2017, [Online]. Available: http://jurnal.polgan.ac.id/index.php/remik/article/view/10116.

BIOGRAFI PENULIS

	Nama : Dalia Nirm : 2017021129 Program Studi : Sistem Informasi STMIK Triguna Dharma Deskripsi : Saat ini menempuh pendidikan Strata Satu (S-1) di STMIK Triguna Dharma Medan mengambil jurusan Program Studi Sistem Informasi E-mail : daliakhan890@gmail.com
	NIDN : 0126017501 Nama : Badrul Anwar, S.E., S.Kom.,M.Kom Program Studi : Sistem Kompter Deskripsi : Beliau merupakan Dosen tetap dan aktif sebagai pengajar di SRMIK Triguna Dharma E-mail : badrul.anwar@yahoo.com
	NIDN : 0118058901 Nama : Dedi Setiawan, S.Kom., M.Kom Program Studi : Teknik Kompter Deskripsi : Beliau merupakan Dosen tetap dan aktif sebagai pengajar di SRMIK Triguna Dharma E-mail : I.info@trigunadharma.ac.id