Jurnal Elektronik Ilmu Komputer Udayana
Volume 11, No 4. Mei 2023

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Sistem Pengamanan Lukisan Digital Menggunakan Metode Rivest Shamir Adleman (RSA)

I Dewa Gde Putra Anga Biara[a1], I Putu Gede Hendra Suputra[a2]

[a]Program Studi Informatika, Fakultas Matermatika dan Ilmu Pengetahuan Alam
Universitas Udayana
Jalan Raya Kampus Unud, Badung, 08361, Bali, Indonesia
[1]angabiara@gmail.com
[2]hendra.suputra@unud.ac.id

Abstract

Digital painting is a result of the process of making digital images/paintings using digital brushes that can produce lines. This painting has become a modern art that can be disseminated through the internet. However, with the ease of disseminating information, digital artwork on the internet is very easy to fake or steal. To solve this problem, a system was created to secure digital painting files using the Rivest Shamir Adleman (RSA) encryption and decryption method. RSA has the basis for encryption and decryption, namely the concepts of prime numbers and modulo arithmetic. Both keys are integers. Based on the research conducted, digital painting files are converted into text and then will go through an encryption process by RSA into text files. Furthermore, to restore the encryption results, the decryption process is carried out with the private key. The weakness of the current system is its inability to process large image files.

Keywords: *Security System, Rivest Shamir Adleman, Digital Painting, Cryptography, Asymmetric*

1. Pendahuluan

Kriptografi merupakan suatu metode dalam mengamankan data yang dapat diterapkan untuk menjaga kerahasiaan data, serta keaslian data dan pengirim. Kriptografi memiliki arti “secret writing” (Tulisan Rahasia). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan yang dikirim dari satu tempat ke tempat lain. Dalam perkembangannya kriptografi dipergunakan untuk menandai berbagai aktifitas rahasia yang berkaitan dengan pertukaran informasi rahasia. Proses mengacak pesan disebut dengan encryption dan proses untuk mengembalikan pesan yang sudah teracak disebut dengan decryption (Harun Mukhtar, 2018).

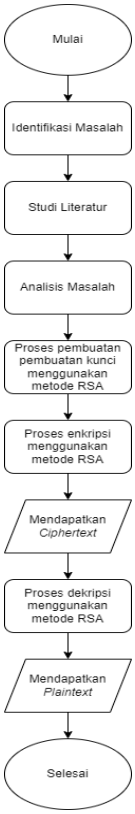
Kemajuan perkembangan teknologi telah memberikan dampak pada kehidupan manusia. Dengan adanya internet penyebaran informasi menjadi semakin mudah dan cepat. Informasi yang dapat disebarkan ini tidak hanya berupa text, namun dapat berupa file dengan beragam format yang telah tersedia. Informasi yang dikirimkan melalui internet sangatlah rentan untuk dapat diakses oleh orang – orang yang tidak berkepentingan yang ingin mensabotase informasi tersebut. Untuk itu keamanan dari informasi tersebut haruslah terjamin. Kriptografi merupakan salah satu metode yang dapat diterapkan untuk mengatasi permasalahan tersebut.

Rivest Shamir Adleman (RSA) adalah penerapan dari metode kriptografi asimetris yang menggunakan 2 pasang kunci, yaitu kunci privat dan kunci publik. RSA memiliki mekanisme kerja yang sederhana, mudah dimengerti dan kokoh. Untuk bisa mendobrak enkripsi dari RSA saat ini hanya bisa dilakukan dengan menggunakan metode *brute force*, dimana metode brute force tersebut akan mencoba satu persatu kombinasi dari kunci enkripsi tersebut. Perbandingan metode RSA dengan metode lainnya seperti AES, metode RSA jauh lebih unggul dalam hal keamanan data jika dibandingkan dengan AES. Namun yang menjadi kompensasi atas keamanan tersebut adalah kecepatan metode RSA dalam melakukan enkripsi dan dekripsi. Hal tersebut menjadikan RSA sebagai salah satu enkripsi yang sangat sesuai jika digunakan dengan tujuan untuk mementingkan keamanan data serta informasi yang dikirimkan.

Lukisan merupakan sebuah karya seni yang dalam proses pembuatannya memerlukan keahlian dalam memulaskan kuas dan cat, serta alat sebagainya dan dapat memakai berbagai warna serta gradasi untuk mengekspresikan sebuah gambaran dari si pelukis. Lukisan merupakan salah satu seni yang sangat berharga dan memiliki nilai nya tersendiri. Dengan kemajuan teknologi lukisan kini tidak hanya dapat dibuat dengan cara memulaskan kuas dan cat, akan tetapi sudah dapat menggunakan aplikasi yang tersedia dalam komputer untuk menghasilkan sebuah lukisan digital. Lukisan digital sangat mudah ditiru dan dipalsukan sehingga membuat keaslian dari lukisan tersebut diragukan sehingga penulis berinisiatif untuk menciptakan sebuah system pengamanan file lukisan digital sehingga hanya dapat dilihat oleh orang yang bersangkutan dengan menggunakan metode kriptografi RSA.

2. Metode Penelitian

Metode yang akan digunakan oleh penulis untuk mengamankan data adalah metode RSA. Penelitian ini dilakukan sesuai dengan tahapan dalam diagram flowchart untuk makalah ini. Identifikasi masalah merupakan tahap pengamatan dalam proses pengiriman lukisan digital. Fokus penelitian ini adalah masalah keamanan dari pengiriman lukisan digital itu sendiri. Tujuan dari observasi ini adalah untuk melakukan identifikasi masalah sesuai dengan masalah yang ada. Studi literatur merupakan tahap pengumpulan bahan dari berbagai referensi serta jurnal yang sesuai dengan topik permasalahan yaitu penggunaan metode RSA dalam pengamanan lukisan digital. Analisis masalah merupakan tahapan analisis terhadap masalah keamanan pada saat proses pengiriman lukisan digital terjadi. Dalam analisis ini, diasumsikan bahwa pengirim dan penerima tidak mengetahui apakah data yang dikirim dapat dirahasiakan atau tidak. Solusi dari permasalahan tersebut adalah dengan melakukan proses enkripsi dan dekripsi terhadap data tersebut menggunakan metode RSA.



Gambar 1. Flowchart penelitian

2.1. Lukisan Digital

Lukisan digital atau biasa disebut *digital painting* adalah proses pembuatan gambar/lukisan secara digital dengan menggunakan kuas digital yang dapat menghasilkan garis, gambar, dan warna yang dibentuk oleh titik – titik digital monitor. Lukisan digital juga merupakan sebuah seni

p-ISSN: 2301-5373
e-ISSN: 2654-5101

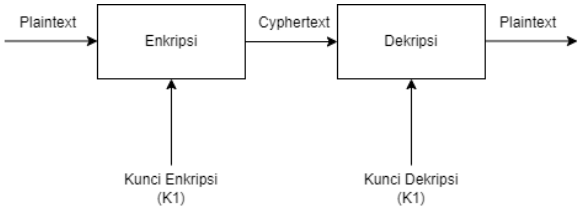
modern dimana seniman membuat karya dengan memanfaatkan media komputer maupun media elektronik lainnya sebagai pengganti kuas (Berri Oktariza Sandra, 2012) .

2.2. Kriptografi

Kriptografi merupakan sebuah seni dalam menjaga keamanan informasi data ketika dipindahkan ke tempat lain dan diterima oleh pihak lain. Kriptografi memiliki arti “secret writing” (Tulisan Rahasia). Kriptografi juga merupakan sebuah ilmu merumuskan metode yang dapat memungkinkan informasi yang dikirimkan hanya dapat dipahami oleh pihak pengirim dan penerima saja. Kriptografi bekerja dengan cara mengganti pesan atau data yang ingin dikirimkan menjadi suatu baris kode yang ditentukan oleh si pengirim yang selanjutnya akan dikirimkan ke si penerima dan untuk memecahkan kode tersebut si penerima harus memiliki sebuah kunci untuk mengubah baris kode tersebut menjadi pesan seperti semula.

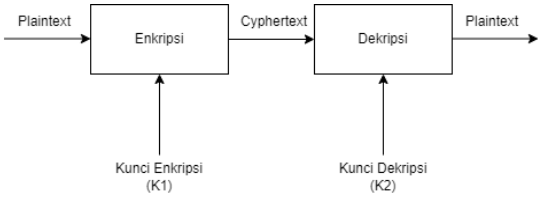
2.3. Algoritma Simetris dan Asimetris

Algoritma simetris adalah algoritma yang dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi yang digunakan. Sebelum mengirim data, pengirim dan penerima harus memilih sebuah kunci yang sama untuk dibagikan dan kunci ini harus dirahasiakan untuk menjaga keamanan algoritma ini. Algoritma ini biasa disebut dengan algoritma kunci rahasia.



Gambar 2. Algoritma simetris

Algoritma asimetris adalah algoritma yang berkebalikan dengan algoritma simetris, dimana pada algoritma asimetris kunci enkripsi yang digunakan berbeda dengan kunci dekripsi. Dalam algoritma ini mengharuskan menggunakan dua buah kunci, yaitu *public key* (kunci publik) dan *private key* (kunci pribadi). *Public key* dapat dibagikan secara publik sedangkan *private key* harus dirahasiakan. *Public key* digunakan pada proses enkripsi sedangkan *private key* digunakan dalam proses dekripsi.



Gambar 3. Algoritma simetris

2.4. Rivest Shamir Adleman (RSA)

Rivest Shamir Adleman (RSA) adalah sebuah algortima kriptografi asimetris yang menggunakan 2 pasang kunci, yaitu kunci privat dan kunci public. RSA ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman dan juga nama RSA diambil dari nama ketiga penemunya tersebut. RSA memiliki 2 kunci yaitu kunci publik dan kunci privat(rahasia). RSA memiliki dasar enkripsi dan dekripsinya yaitu pada konsep bilangan prima dan aritmatika modulo. Kedua kunci tersebut merupakan bilangan bulat. RSA memiliki mekanisme kerja yang sederhana, mudah dimengerti dan kokoh. Untuk bisa mendobrak enkripsi dari RSA saat ini hanya bisa dilakukan dengan menggunakan metode brute force, dimana metode brute force tersebut akan mencoba satu persatu kombinasi dari kunci enkripsi tersebut. Hal tersebut menjadikan RSA

sebagai salah satu enkripsi yang masih sering digunakan untuk saat ini. Berikut merupakan proses dari algoritma RSA :

2.4.1. Proses Pembuatan Kunci

Besaran yang digunakan dalam algoritma RSA:

1. p dan q bilangan prima (rahasia)
2. n = p × q (tidak rahasia)
3. $\varphi(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plaintext) (rahasia)
7. c (chipertext) (tidak rahasia)

Proses pembuatan kunci untuk algoritma RSA memiliki dua kunci yang berbeda untuk proses enkripsi dan dekripsi. Adapun Langkah-langkah yang berkaitan dengan perhitungan pembuatan kunci, enkripsi dan dekripsi adalah sebagai berikut :

1. Tentukan 2 bilangan prima, dengan nama p dan q.
2. Hitung nilai modulus (n) dengan rumus n = p × q.
3. Hitung nilai total atau phi (φ) dari n.
4. Tentukan nilai e dimana nilai e adalah bilangan prima dan nilai e harus sesuai dengan suku 1 < e < φ (n). Untuk membuktikan nilai e dapat dihitung menggunakan rumus gcd (e, (n)) = 1.
5. Mencari nilai eksponen pengurai (d) dengan rumus e x d mod $\varphi(n)$
6. Setelah menemukan nilai n, e, dan d, pasangan kuncinya adalah pasangan kunci publik dan pasangan kunci rahasia. Pasangan kunci publik (n, e) dan pasangan kunci rahasia (n, d).

2.4.2. Proses Enkripsi

Pada proses enkripsi ini, sebuah pesan dalam bentuk plaintext diubah menjadi kode ASCII dengan menggunakan tabel ASCII untuk melihat kode yang sesuai dengan plaintext yang ada. Selanjutnya adalah mencari nilai C dengan menggunakan rumus. Kunci yang digunakan dalam proses ini adalah kunci publik (n, e). Dari rumus perhitungan tersebut, akan ditemukan nilai c (cyphertext). Berikut ini adalah gambar dari tabel ASCII.

Hex	Dec	Char		Hex	Dec	Char	Hex	Dec	Char	Hex	Dec	Char
0x00	0	NULL	null	0x20	32	Space	0x40	64	@	0x60	96	`
0x01	1	SOH	Start of heading	0x21	33	!	0x41	65	A	0x61	97	a
0x02	2	STX	Start of text	0x22	34	"	0x42	66	B	0x62	98	b
0x03	3	ETX	End of text	0x23	35	#	0x43	67	C	0x63	99	c
0x04	4	EOT	End of transmission	0x24	36	$	0x44	68	D	0x64	100	d
0x05	5	ENQ	Enquiry	0x25	37	%	0x45	69	E	0x65	101	e
0x06	6	ACK	Acknowledge	0x26	38	&	0x46	70	F	0x66	102	f
0x07	7	BELL	Bell	0x27	39	'	0x47	71	G	0x67	103	g
0x08	8	BS	Backspace	0x28	40	(	0x48	72	H	0x68	104	h
0x09	9	TAB	Horizontal tab	0x29	41	)	0x49	73	I	0x69	105	i
0x0A	10	LF	New line	0x2A	42	*	0x4A	74	J	0x6A	106	j
0x0B	11	VT	Vertical tab	0x2B	43	+	0x4B	75	K	0x6B	107	k
0x0C	12	FF	Form Feed	0x2C	44	,	0x4C	76	L	0x6C	108	l
0x0D	13	CR	Carriage return	0x2D	45	-	0x4D	77	M	0x6D	109	m
0x0E	14	SO	Shift out	0x2E	46	.	0x4E	78	N	0x6E	110	n
0x0F	15	SI	Shift in	0x2F	47	/	0x4F	79	O	0x6F	111	o
0x10	16	DLE	Data link escape	0x30	48	0	0x50	80	P	0x70	112	p
0x11	17	DC1	Device control 1	0x31	49	1	0x51	81	Q	0x71	113	q
0x12	18	DC2	Device control 2	0x32	50	2	0x52	82	R	0x72	114	r
0x13	19	DC3	Device control 3	0x33	51	3	0x53	83	S	0x73	115	s
0x14	20	DC4	Device control 4	0x34	52	4	0x54	84	T	0x74	116	t
0x15	21	NAK	Negative ack	0x35	53	5	0x55	85	U	0x75	117	u
0x16	22	SYN	Synchronous idle	0x36	54	6	0x56	86	V	0x76	118	v
0x17	23	ETB	End transmission block	0x37	55	7	0x57	87	W	0x77	119	w
0x18	24	CAN	Cancel	0x38	56	8	0x58	88	X	0x78	120	x
0x19	25	EM	End of medium	0x39	57	9	0x59	89	Y	0x79	121	y
0x1A	26	SUB	Substitute	0x3A	58	:	0x5A	90	Z	0x7A	122	z
0x1B	27	FSC	Escape	0x3B	59	;	0x5B	91	[	0x7B	123	{
0x1C	28	FS	File separator	0x3C	60	<	0x5C	92	\	0x7C	124	|
0x1D	29	GS	Group separator	0x3D	61	=	0x5D	93	]	0x7D	125	}
0x1E	30	RS	Record separator	0x3E	62	>	0x5E	94	^	0x7E	126	~
0x1F	31	US	Unit separator	0x3F	63	?	0x5F	95	_	0x7F	127	DEL

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Gambar 4. Tabel ASCII

2.4.3. Proses Dekripsi

Pada proses dekripsi ini, akan merubah ciphertext yang telah didapatkan sebelumnya menjadi data awal berupa plaintext. Proses dekripsi dilakukan dengan menggunakan rumus. Setelah mencari nilai m dengan menggunakan rumus perhitungan dekripsi maka akan dicari juga teks dari pesan yang dikirim.

3. Hasil dan Pembahasan

Pengimplementasian system pengamanan lukisan digital menggunakan perangkat keras dan perangkat lunak. Sistem ini dibangun menggunakan bahasa pemrograman Python. Berikut merupakan spesifikasi dari perangkat keras yang penulis gunakan :

1. Processor AMD Ryzen 5 3,50 Ghz
2. RAM 16 GB
3. SSD 512 GB

Berikut perangkat lunak yang penulis gunakan :

1. Visual Studio Code
2. Sistem Operasi Windows 11

3.1. Implementasi Algoritma RSA

Metode yang digunakan pada implementasi ini adalah metode RSA yang bersifat asimetris. Untuk melakukan enkripsi terhadap gambar atau lukisan digital, lukisan tersebut akan diubah terlebih dahulu kedalam bentuk text agar bisa dienkripsi. Contoh lukisan yang akan dienkripsi :

Gambar 5. Contoh Lukisan Digital

Setelah melalui proses pengubahan menggunakan base64 pada library python. Selanjutnya lukisan tersebut akan menghasilkan teks berupa kumpulan karakter sebanyak 211.377 karakter. Pada penjelasan implementasi ini, penulis akan mengambil 10 karakter pertama (“/9j/4AAQSk”) sebagai contoh kerja algoritma RSA yang dimana gabungan teks ini hanya bisa diubah kembali menjadi gambar oleh pengirim dan penerima.

3.1.1. Proses Penyusunan Kunci

Pada proses penyusunan kunci ini menggunakan metode RSA untuk mendapatkan dua buah kunci yaitu kunci publik dan kunci pribadi, yang dimana kunci pribadi akan disimpan oleh si pengirim dan kunci publik akan disimpan oleh si penerima. Berikut merupakan tahapan dari pembuatan kunci RSA :

1. Tahap pertama adalah memilih dua bilangan prima yang akan digunakan dengan nama p dan q dimana p > q, kali ini p adalah 59 dan q adalah 7.
2. Kemudian hitung nilai n dengan menggunakan rumus n = p × q dimana nilai dari p dan q telah ditentukan pada Langkah pertama
   n = p × q
   n = 59 × 7
   n = 413
3. Kemudian hitung nilai phi dari n dengan menggunakan rumus $\varphi(n) = (p-1)(q-1)$
   $\varphi(n) = (p-1)(q-1)$
   $\varphi(n) = (59-1)(7-1)$
   $\varphi(n) = 58 \times 6$
   $\varphi(n) = 348$
4. Selanjutnya menentukan nilai e dimana nilai e adalah bilangan prima dan nilai e harus sesuai dengan suku 1 < e < φ (n). Untuk membuktikan nilai e dapat dihitung menggunakan rumus gcd (e, (n)) = 1. Setelah melakukan beberapa kali perhitungan, nilai e yang kali ini dipilih adalah 5. Untuk membuktikan 5 memenuhi kondisi adalah sebagai berikut :
   (5, 348) = 1
   348 mod 5 = 3
   5 mod 3 = 2
   2 mod 1 = 0
5. Kemudian mencari nilai eksponen pengurai (d) dengan rumus e x d mod φ (n) .Setelah melakukan beberapa kali percobaan hingga menghasilkan nilai modulo = 1, hasilnya adalah d bernilai 209.
   e x d mod $\varphi(n) = 1$
   5 x (1,2,3,… coba terus hingga menghasilkan 1) mod 348 = 1
   5 x 209 mod 348 = 1
   1045 mod 348 = 1
6. Setelah menemukan nilai dari n, e, dan d, kunci yang telah ditemukan tersebut akan dipasangkan dan dinamai kunci publik dan kunci pribadi.
   Public key (e, n) = (5, 413)
   Private key (d, n) = (209, 413)

3.1.2. Proses Enkripsi

Pada proses enkripsi ini menggunakan metode RSA. Teks yang akan dienkripsi merupakan 10 karakter awal dari total teks hasil konversi gambar menggunakan base64, 10 karakter itu adalah “/9j/4AAQSk” dan kunci yang akan digunakan adalah (5, 413). Teks tersebut kemudian akan diterjemahkan menjadi kode ASCII.

i	karakter	Chipertext (M_i)	ASCII
1	/	M_1	47
2	9	M_2	57
3	j	M_3	106
4	/	M_4	47
5	4	M_5	52
6	A	M_6	65
7	A	M_7	65
8	Q	M_8	81
9	S	M_9	83
10	k	M_{10}	107

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Gambar 6. Tabel konversi karakter kedalam kode ASCII

Kemudian melakukan proses enkripsi menggunakan metode RSA. Untuk melakukan proses ini diperlukan nilai C. Untuk mencari nilai c dengan menggunakan rumus $C = M^e (mod\ n)$.

i	M_i	$C = M^e\ (mod\ n)$	Hex
1	M_1	325	0x145
2	M_2	204	0xcc
3	M_3	148	0x94
4	M_4	325	0x145
5	M_5	362	0x16a
6	M_6	165	0xa5
7	M_7	165	0xa5
8	M_8	100	0x64
9	M_9	279	0x117
10	M_{10}	137	0x89

Gambar 7. Tabel proses enkripsi menggunakan RSA

3.1.3. Proses Dekripsi

Dalam proses ini penerima menerima teks yang sebelumnya telah dienkripsi oleh pengirim dan untuk mengembalikan teks tersebut menjadi teks yang bisa diubah menjadi gambar seperti semula adalah dengan melakukan dekripsi. Proses dekripsi dilakukan dengan menggunakan kunci yang telah didapat sebelumnya. Pada proses ini akan didapatkan hasil berupa karakter yaitu “/9j/4AAQSk”. Berikut merupakan perhitungan untuk proses dekripsi menggunakan metode RSA.

i	Hex	C_i	$M = C^d\ (mod\ n)$	Karakter
1	0x145	325	47	/
2	0xcc	204	57	9
3	0x94	148	106	j
4	0x145	325	47	/
5	0x16a	362	52	4
6	0xa5	165	65	A
7	0xa5	165	65	A
8	0x64	100	81	Q
9	0x117	279	83	S
10	0x89	137	107	k

Gambar 8. Tabel proses dekripsi menggunakan RSA

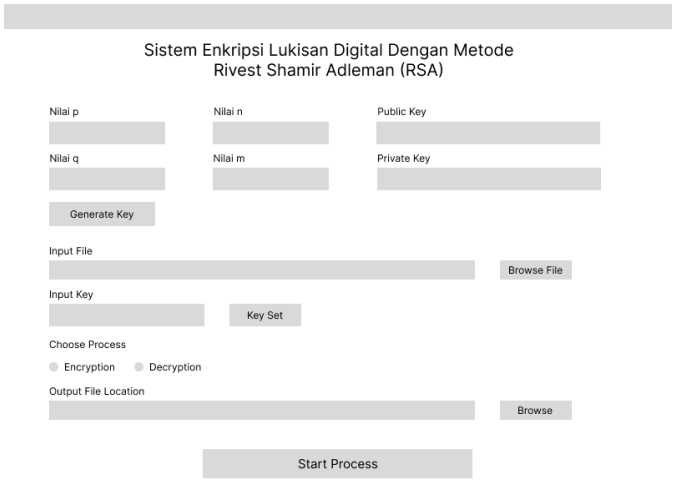
3.2. Tampilan Antarmuka Sistem

Bagian utama terdiri dari beberapa menu yang dapat diakses oleh user sesuai dengan fungsinya masing – masing. Berikut merupakan tampilan beserta keterangan dari menu tersebut :

1. Menu Generate Key

Menu ini berfungsi untuk membuat public serta private key dari nilai – nilai yang telah di inputkan oleh user.

2. Menu Browse File
   Menu ini berfungsi untuk membuka serta memilih file lukisan digital yang akan dienkripsi.
3. Menu Key Set
   Menu ini berfungsi untuk memasukkan kunci baik itu public key maupun private key untuk dua proses yang berbeda.
4. Menu Choose Process
   Menu ini berfungsi untuk memilih proses mana yang akan dijalankan oleh sistem.
5. Menu Browse
   Menu ini berfungsi untuk memilih lokasi penyimpanan file hasil enkripsi atau dekripsi.
6. Menu Start Process
   Menu ini berfungsi untuk memulai proses enkripsi atau dekripsi sesuai dengan pilihan user.



Gambar 9. Tampilan Antarmuka Sistem

4. Kesimpulan

Pada penelitian ini menggunakan metode Rivest Shamir Adleman (RSA). Penerapan metode RSA dalam pengamanan lukisan digital berperan untuk merahasiakan lukisan digital dengan cara mengubahnya menjadi text yang tidak bisa diartikan langsung oleh penerima. Hal ini dapat terjadi karena pada tahap awal lukisan digital diubah menjadi bentuk teks menggunakan base64. Kemudian dengan menggunakan algoritma RSA yang memiliki dua kunci yaitu *public key* (kunci public) yang digunakan untuk melakukan proses enkripsi serta *private key* (kunci pribadi) yang digunakan untuk melakukan proses dekripsi. Pengamanan lukisan digital menggunakan metode RSA memiliki kelebihan dalam hal kecepatan pengolahan data serta kemudahan dalam hal pengamanan data karena untuk dapat menerjemahkan text yang telah di enkripsi menggunakan *public key* (kunci public) diperlukan kunci lainnya yaitu *private key* (kunci pribadi). Selain itu, pada penelitian ini juga terdapat tantangan dalam penggunaan enkripsi RSA yang terletak pada bagian efisiensi serta kecepatan proses enkripsi yang menyebabkan pada beberapa file lukisan digital yang memiliki ukuran besar, proses enkripsi menjadi sangat lama. Dengan melakukan enkripsi pada lukisan digital, kerahasiaan lukisan tersebut dapat terjamin setelah dikirim melalui internet.

Referensi

[1] Handoyo, Antonius Erick, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Christy Atika Sari, and Ajib Susanto. “Message Concealment and Encryption Technique in Digital Image with Combination of LSB and RSA Methods.” Jurnal Teknologi Dan Sistem Komputer 6, no. 1 (2018): 37–43. doi:10.14710/jtsiskom.6.1.2018.37-43.

[2] Harin Noor octafiani and Rosita, A. (2021) 'Implementasi Verifikasi Teks Menggunakan Metode Rivest Shamir Adleman (Rsa)', Jurnal Ilmiah Teknologi Infomasi Terapan, 8(1), pp. 72–77. doi:10.33197/jitter.vol8.iss1.2021.720.

[3] Syahputra, Andika, Implementasi Algoritma, and Freivlds Untuk. "Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video" 10 (2021): 70–77.

[4] Rianty, Winda, and I Ketut Gede Suhartana. "The Security System For Web-Based Lontar Images in JPG Format Using The Rivest Shamir Adleman." JELIKU (Jurnal Elektronik Ilmu Komputer Udayana) 9, no. 4 (2021): 525. doi:10.24843/jlk.2021.v09.i04.p10.

[5] Pamungkas, P.G. and Muhammad, A.H. (2022) 'Modifikasi Algoritma Kriptografi Caesar Chiper pada Deretan Simbol dan Huruf di Smarphone dan Laptop', Journal of Information Technology, 2(1), pp. 1–5. doi:10.46229/jifotech.v2i1.234.

[6] Safira, M.O. and Ari Mogi, I.K. (2020) 'Design Of Hybrid Cryptography With Vigenere Cipher And RSA Algorithm On IOT Data Security', JELIKU (Jurnal Elektronik Ilmu Komputer Udayana), 8(4), p. 475. doi:10.24843/jlk.2020.v08.i04.p14.

[7] Anwar, N. et al. (2018) 'Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA', Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 2(3), pp. 783–791. doi:10.29207/resti.v2i3.606.

[8] Laurentinus, L. et al. (2020) 'Performance comparison of RSA and AES to SMS messages compression using Huffman algorithm', Jurnal Teknologi dan Sistem Komputer, 8(3), pp. 171–177. doi:10.14710/jtsiskom.2020.13468.

[9] Harta, I.G.B.A. et al. (2022) 'Pengamanan Lontar Digital Dengan Tanda Tangan Digital Menggunakan Algoritma RSA', JELIKU (Jurnal Elektronik Ilmu Komputer Udayana), 10(2), p. 199. doi:10.24843/jlk.2021.v10.i02.p02.

This page is intentionally left blank