HYBRID HILL CIPHER ASCII 256 DAN *RSA CIPHER* DALAM MENGAMANKAN PESAN

Skripsi

Oleh

SANDI SAPUTRA
NPM. 2017031054

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2024

ABSTRACT

HYBRID HILL CIPHER ASCII 256 AND RSA CIPHER IN SECURING MESSAGES

By

Sandi Saputra

One of the negative impacts of technological developments in the communications sector is information leakage to third parties. To prevent this, a specific method is needed, namely cryptography. Cryptography can be interpreted as a science that studies how data is converted into a satisfied form that is difficult to understand. Based on the keys used, cryptography can be divisible into two, namely symmetric and asymmetric key cryptography. Symmetric key cryptography has advantages in terms of the speed of the encryption process but has disadvantages in terms of keys security. One example is Hill Cipher. Hill Cipher is a cryptographic algorithm that uses matrix multiplication. The key is a square matrix of size $n \times n$ whose is invertible in modulo p. The lack of this algorithm can be outgrow by combining it with asymmetric key cryptography. One example is RSA Cipher. RSA Cipher uses a public key to encrypt a message and a private key to decrypt the encryption message. Based on the results of combining these two methods, the message encryption results are much more secure and difficult to crack. The encryption process is divisible into two cases based on whether the message length divides the size of the keys matrix used.

Keywords: cryptography, symmetric key, asymmetric key, RSA cipher, Hill cipher, encryption.

ABSTRAK

HYBRID HILL CIPHER ASCII 256 DAN *RSA CIPHER* DALAM MENGAMANKAN PESAN

Oleh

Sandi Saputra

Salah satu dampak negatif dari perkembangan teknologi dalam bidang komunikasi adalah kebocoran informasi ke pihak ketiga. Untuk mencegah hal tersebut diperlukan metode khusus yaitu kriptografi. Kriptografi dapat diartikan sebagai ilmu yang mempelajari bagaimana sebuah data dikonversi ke bentuk tertentu yang sulit untuk dimengerti. Berdasarkan kunci yang digunakan, kriptografi dapat dibedakan menjadi dua, yaitu kriptografi kunci simetris dan asimetris. Kriptografi kunci simetris memiliki kelebihan dalam hal kecepatan proses enkripsinya, namun memiliki kekurangan dalam hal pengamanan kunci. Salah satu contohnya adalah Hill Cipher. Hill Cipher merupakan algoritma kriptografi yang menggunakan perkalian matriks. Kuncinya berupa matriks persegi ukuran $n \times n$ yang bersifat *invertible* dalam modulo p. Kekurangan algoritma ini dapat diatasi dengan menggabungkannya dengan kriptografi kunci asimetris. Salah satu contohnya adalah RSA Cipher. RSA Cipher menggunakan kunci publik untuk mengenkripsi suatu pesan dan menggunakan kunci *private* untuk mendekripsi pesan enkripsi. Berdasarkan hasil dari penggabungan kedua metode tersebut, diperoleh hasil enkripsi pesan menjadi jauh lebih aman dan sulit untuk dipecahkan. Proses enkripsi dibagi menjadi dua kasus berdasarkan habis tidaknya panjang pesan membagi ukuran matriks kunci yang digunakan.

Kata-kata kunci: kriptografi, kunci simetris, kunci asimetris, RSA cipher, Hill cipher, enkripsi.

HYBRID HILL CIPHER ASCII 256 DAN *RSA CIPHER* DALAM MENGAMANKAN PESAN

SANDI SAPUTRA

Skripsi

Sebagai Salah Satu Syarat untuk Memperoleh Gelar
SARJANA MATEMATIKA

Pada

Jurusan Matematika

Fakultas Matematika dan Ilmu Pengetahuan Alam

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2024

Judul Skripsi	:	***HYBRID HILL CIPHER ASCII* 256 DAN *RSA CIPHER* DALAM MENGAMANKAN PESAN**
Nama Mahasiswa	:	Sandi Saputra
Nomor Pokok Mahasiswa	:	**2017031054**
Program Studi	:	**Matematika**
Fakultas	:	**Matematika dan Ilmu Pengetahuan Alam**

MENYETUJUI

1. Komisi Pembimbing

Dr. Fitriani, S.Si.,M.Sc.
NIP 198406272006042001

Dr. Ahmad Faisol, S.Si.,M.Sc.
NIP 198002062003121003

2. Ketua Jurusan Matematika

Dr.Aang Nuryaman, S.Si.,M.Si.
NIP. 197403162005011001

MENGESAHKAN

1. Tim penguji

Ketua : **Dr. Fitriani, S.Si.,M.Sc.** .....

Sekretaris : **Dr. Ahmad Faisol, S.Si.,M.Sc.** .....

Penguji
Bukan Pembimbing : **Prof. Dra. Wamiliana, MA.,Ph.D.** .....

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

Dr. Eng. Heri Satria, S.Si., M.Si.
NIP. 197110012005011002

Tanggal Lulus Ujian Skripsi: **07 Februari 2024**

PERNYATAAN SKRIPSI MAHASISWA

Yang bertanda tangan di bawah ini:

Nama	:	**Sandi Saputra**
Nomor Pokok Mahasiswa	:	**2017031054**
Jurusan	:	**Matematika**
Judul Skripsi	:	***Hybrid Hill Cipher ASCII* 256 dan *RSA Cipher* dalam Mengamankan Pesan**

Dengan ini menyatakan bahwa skripsi ini adalah hasil pekerjaan saya sendiri. Apabila kemudian hari terbukti bahwa skripsi inni merupakan hasil salinan atau dibuat oleh orang lain, maka saya bersedia menerima sanksi sesuai degnan ketentuan akademik yang berlaku.

Bandar Lampung,

Penulis.

Sandi Saputra

RIWAYAT HIDUP

Penulis memiliki nama lengkap Sandi Saputra yang lahir di Teratas pada tanggal 24 Juni 2002. Penulis merupakan anak pertama dari pasangan Bapak Sudaryanto dan Ibu Elyawati.

Penulis menyelesaikan pendidikan Sekolah Dasar di SDN 1 Kembahang pada tahun 2014, pendidikan Sekolah Menengah Pertama di MTSN 1 Lampung Barat yang diselesaikan pada tahun 2017, dan pendidikan Sekolah Menengah Atas di SMA Negeri 1 Liwa yang diselesaikan pada tahun 2020.

Penulis melanjutkan pendidikan Strata Satu (S1) di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam (FMIPA) Universitas Lampung pada tahun 2020 melalui jalur SBMPTN. Sebagai bentuk penerapan ilmu perkuliahan pada tahun 2022 dan 2023, penulis melaksanakan Kerja Praktik (KP) di BUMIDA Lampung dan Kuliah Kerja Nyata (KKN) di Desa Kalidadi, Kecamatan Kalirejo, Kabupaten Lampung Tengah.

Selama menjadi mahasiswa penulis aktif mengikuti organisasi sebagai Anggota Kaderisasi pada periode 2021 dan Reporter Media Dalam Jaringan pada periode 2022 di Unit Kegiatan Mahasiswa Fakultas (UKMF) Natural FMIPA Universitas Lampung dan sebagai Anggota Keilmuan pada periode 2022 di Himpunan Mahasiswa Jurusan Matematika (HIMATIKA) FMIPA Universitas Lampung. Penulis juga aktif dalam beberapa kepanitiaan, diantaranya sebagai Koordinator Kompetisi Matematika Dies Natalis Jurusan Matematika (DINAMIKA) XXIII dan Anggota Sekretariat IndoMS School 2023.

KATA INSPIRASI

"Keberhasilan bukanlah milik orang yang pintar. Keberhasilan adalah kepunyaan mereka yang senantiasa berusaha"
(B.J. Habibie)

"If we think of genius as something magical, we are not obliged to compare ourselves and find ourselves lacking"
(Friedrich Nietzsche)

"Maka sesungguhnya bersama kesulitan itu ada kemudahan"
(QS. Al-Insyirah : 5)

"The only thing i know is that i know nothing"
(Socrates)

"Life is really simple, but we insist on making it complicated"
(Confucius)

PERSEMBAHAN

Dengan mengucap Alhamdulillah dan syukur kepada Allah SWT atas nikmat serta hidayah-Nya sehingga skripsi ini dapat terselesaikan dengan baik dan tepat pada waktunya. Dengan rasa syukur dan Bahagia, saya persembahkan rasa terimakasih saya kepada:

Ayah dan Ibuku Tercinta

Terimakasih kepada orang tuaku atas segala pengorbanan, motivasi, doa dan ridho serta dukungannya selama ini. Terimakasih telah memberikan pelajaran berharga kepada anakmu ini tentang makna perjalanan hidup yang sebenarnya sehingga kelak bisa menjadi orang yang bermanfaat bagi banyak orang.

Dosen Pembimbing dan Pembahas

Terimakasih kepada dosen pembimbing dan pembahas yang sudah sangat membantu, memberikan motivasi, memberikan arahan serta ilmu yang berharga.

Sahabat-sahabatku

Terimakasih kepada semua orang-orang baik yang telah memberikan pengalaman, semangat, motivasinya, serta doa-doanya dan senantiasa memberikan dukungan dalam hal apapun.

Almamater Tercinta
Universitas Lampung

SANWACANA

Alhamdulillah, puji dan syukur penulis panjatkan kepada Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini yang berjudul "*Hybrid Hill Cipher ASCII* 256 dan *RSA Cipher* dalam Mengamankan Pesan" dengan baik dan lancar serta tepat pada waktu yang telah ditentukan. Shalawat serta salam semoga senantiasa tercurahkan kepada Nabi Muhammad SAW.

Dalam proses penyusunan skripsi ini, banyak pihak yang telah membantu memberikan bimbingan, dukungan, arahan, motivasi serta saran sehingga skripsi ini dapat terselesaikan. Oleh karena itu, dalam kesempatan ini penulis mengucapkan terimakasih kepada:

1. Ibu Dr. Fitriani, S.Si.,M.Sc. selaku Pembimbing 1 yang telah banyak meluangkan waktunya untuk memberikan arahan, bimbingan, motivasi, saran serta dukungan kepada penulis sehingga dapat menyelesaikan skripsi ini.
2. Bapak Dr. Ahmad Faisol, S.Si.,M.Sc. selaku Pembimbing II yang telah memberikan arahan, bimbingan dan dukungan kepada penulis sehingga dapat menyelesaikan skripsi ini.
3. Ibu Prof. Dra. Wamiliana, MA.,Ph.D. selaku Penguji yang telah bersedia memberikan kritik dan saran serta evaluasi kepada penulis sehingga dapat menjadi lebih baik lagi.
4. Bapak Dr. Aang Nuryaman, S.Si., M.Si. selaku Ketua Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.
5. Bapak Prof. Dr. La Zakaria, S.SI.,M.SC. selaku dosen pembimbing akademik.
6. Seluruh dosen, staff dan karyawan Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.
7. Ayah dan ibu yang selalu memotivasi, mendukung serta mendoakan penulis.

8. Terimakasih pada diri sendiri karena sudah berjuang dan bertahan hingga tahap ini.
9. Teman-teman satu bimbingan, Bidari, Aira, Lisa, Anggita yang telah memberikan semangat, motivasi maupun saran kepada penulis.
10. Teman-teman KKN Kalidadi, untuk segala kebersamaan dan dukungan selama ini.
11. Teman-teman satu organisasi di UKMF NATURAL dan HIMATIKA FMIPA Unila, terimakasih atas pengalaman dan kebersamaan selama ini.
12. Teman-teman Matematika angkatan 2020 dan semua pihak yang terlibat dalam proses penyusunan skripsi ini.

Semoga skripsi ini dapat bermanfaat bagi kita semua. Penulis menyadari bahwa skripsi ini masih jauh dari sempurna, sehingga penulis mengharapkan kritik dan saran yang membangun untuk menjadikan skripsi ini lebih baik lagi.

Bandar Lampung,

Sandi Saputra

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi tentu berdampak positif terhadap berbagai bidang dalam kehidupan, tidak terkecuali dalam bidang komunikasi. Mudahnya berkomunikasi tanpa terhalang jarak merupakan segelitir dari dampak positif yang ditimbulkan oleh perkembangan teknologi informasi. Namun, dibalik kemudahan tersebut timbul bahaya yang mengancam. Bahaya itu berupa kebocoran informasi terkait pesan yang kita kirimkan ke pihak kedua. Untuk mencegah hal tersebut diperlukan sebuah metode khusus untuk membantu mengamankan pesan yang kita kirimkan ke pihak kedua. Metode ini dikenal dengan istilah kriptografi. Kriptografi dapat diartikan sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data dikonversi ke bentuk tertentu yang sulit untuk dimengerti (Hanafi dan Patombongi, 2016). Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi kriptografi kunci simetris dan kriptografi asimetris (Jamaludin, 2018).

Algoritma simetri merupakan algoritma kriptografi yang memakai satu kunci yang sama untuk melakukan enkripsi dan dekripsi (Cahyanti dkk., 2023). Algoritma ini memiliki kelebihan dalam kecepatan proses enkripsi dan dekripsinya. Namun, memiliki kekurangan dalam hal pengamanan kunci (Jamaludin, 2018). Salah satu contoh dari kriptografi kunci simetris adalah *Hill Cipher*. *Hill Cipher* merupakan algoritma kriptografi yang menggunakan perkalian matriks. Algoritma ini memiliki kelebihan dibandingkan algoritma kunci simetris lainnya dalam hal banyaknya kemungkinan kunci yang dapat diambil (Ulva, 2019). Kunci berupa matriks persegi ukuran $n \times n$ yang bersifat *invertible* dalam modulo p (Wasil, 2023).

Kelemahan algoritma simetris dapat diatasi dengan algoritma kunci asimetris. Algoritma kunci asimetris adalah algoritma yang menggunakan dua kunci berbeda dalam proses enkripsi dan dekripsinya (Cahyanti dkk., 2023). Kelebihan algoritma ini terletak pada lambatnya proses enkripsi dan dekripsi, sehingga lebih aman da-

lam hal keamanan kunci (Jamaludin, 2018). Contoh dari algoritma ini salah satunya adalah *Rivest Shamir Adleman* (*RSA*). Algoritma *RSA* terdiri dari kunci publik dan kunci *private* dimana kunci publik dapat diketahui oleh semua orang, sedangkan kunci *private* hanya diketahui oleh pemilik data (Wahyadyatmika dkk., 2014). Keamanan algoritma *RSA* terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci *private* (Sumarno, 2018).

Berdasarkan alasan tersebut diperlukan penelitian lebih lanjut mengenai penggabungan *Hill Cipher* dan *RSA Cipher*. Penelitian ini sebelumnya sudah pernah dilakukan oleh Jamaludin yang menggabungkan *Hill Cipher* dan *RSA Cipher* dengan kunci *Hill* berupa matriks 2×2 (Jamaludin, 2018). Kemudian, penelitian dilanjutkan oleh Santoso yang memodifikasi ukuran matriks kunci menjadi 3×3 dan menggunakan *RSA* 512 bit (Santoso, 2021). Dari penelitian-penelitian sebelumnya, menimbulkan sebuah peluang untuk melanjutkan penelitian serupa dengan modifikasi pada ukuran matriks kunci *Hill* menjadi $n \times n$ dan digunakan karakter *ASCII* 256. Oleh karena itu, peneliti tertarik untuk mengusulkan penelitian berupa *hybrid Hill Cipher ASCII* 256 dan *RSA Cipher* dalam mengamankan pesan.

1.2 Tujuan Penelitian

Tujuan dari penelitian ini adalah menciptakan sebuah program yang berguna untuk mengamankan pesan dengan menggunakan *hybrid Hill Cipher ASCII* 256 dan *RSA Cipher*.

1.3 Manfaat Penelitian

Adapun manfaat penelitian ini adalah:

1. mengetahui mekanisme enkripsi dan dekripsi *Hill Cipher* dan *RSA Cipher* dalam mengamankan pesan;
2. menambah referensi penelitian selanjutnya mengenai penerapan metode *Hill Cipher* dan *RSA Cipher* dalam mengamankan pesan.

BAB II

TINJAUAN PUSTAKA

2.1 Kriptografi

Kata kriptografi (*Cryptography*) berasal dari bahasa Yunani, yaitu kata *Cryptos* yang artinya tersembunyi dan *Graphein* yang artinya menulis. Kriptografi dapat diartikan sebagai suatu ilmu yang mempelajari bagaimana sebuah data dikonversi ke bentuk tertentu yang sulit untuk dimengerti (Hanafi dan Patombongi, 2016). Untuk menyembunyikan pesan, dilakukan proses mengubah teks pesan (*plaintext*) menjadi teks sandi dengan menggunakan suatu algoritma dan kunci rahasia. Proses menyandikan pesan disebut enkripsi (*encryption*), sedangkan proses mengembalikan teks sandi ke teks asli disebut dengan dekripsi (*decryption*). Pesan awal yang belum diacak disebut dengan teks asli (*plaintext*), sedangkan pesan yang telah diacak disebut dengan teks sandi (*ciphertext*) (Cahyanti dkk., 2023).

Algoritma kriptografi adalah tahapan-tahapan bagaimana cara menyembunyikan isi pesan rahasia dari orang-orang yang tidak berwenang akan pesan tersebut (Cahyanti dkk., 2023). Berdasarkan kunci yang dipakainya, algoritma kriptografi dibagi menjadi tiga, yakni

1. Algoritma Simetri
   Algoritma simetri merupakan algoritma kriptografi yang memakai satu kunci yang sama untuk melakukan enkripsi dan dekripsi. Contohnya *One Time Pad*, *Data Encryptions Standart*, *Advance Encryptions Standart*, *Vigenere Cipher*, dan *Hill Cipher*.

2. Algoritma Asimetri
   Algoritma asimetri memiliki dua kunci yang berbeda pada proses enkripsi dan dekripsinya, yakni kunci publik yang boleh diketahui oleh semua orang dan kunci *private* yang disembunyikan. Contohnya RSA, *Digital Signature Algorithm* (DSA), *Elliptic Curve Crypthography* (ECC), dan lain-lain.

3. Fungsi *Hash*
   Fungsi *Hash* adalah suatu fungsi matematika yang mengambil masukan panjang variabel lalu mengubahnya ke dalam bentuk biner dengan panjang yang tepat. Fungsi ini digunakan pada saat seseorang ingin membuat sidik jari dari suatu pesan. Sidik jari dari pesan itu sendiri bertujuan untuk memberi tanda bahwasanya pesan yang diterima memang benar-benar dari pengirim. Contohnya MD5, SHA-1, SHA-256, dan lain-lain. (Cahyanti dkk., 2023).

2.2 *Hill Cipher*

Hill cipher yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher*, karena teks yang akan dienkripsi dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter-karakter lain dalam proses enkripsi dan dekripsinya (Nasrudin dkk., 2020). Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi. *Hill cipher* ditemukan oleh *Lester S. Hill* pada tahun 1929. *Hill cipher* tidak mengganti setiap abjad *plaintext* yang sama dengan abjad *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya (Rachmawati dkk., 2019). *Hill Cipher* termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext*nya saja (Fauzi dkk., 2017). Namun, teknik ini dapat dipecahkan cukup mudah saat kriptanalis mempunyai *ciphertext* dan potongan *plaintext* (Pangaribuan, 2018). Teknik kriptanalisis ini disebut *known-plaintext attack* (Pawan dkk., 2019).

2.2.1 Dasar Teknik *Hill Cipher*

Dasar dari teknik *Hill Cipher* adalah aritmatika modulo terhadap matriks. Dalam penerapannya, *Hill Cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada *Hill Cipher* adalah matriks $n \times n$ dengan n merupakan ukuran blok (Makhomah dkk., 2021). Jika kunci disebut dengan K, maka K adalah sebagai berikut:

$$K = \begin{bmatrix} k_{11} & \dots & k_{1n} \\ \vdots & \ddots & \vdots \\ k_{n1} & \dots & k_{nn} \end{bmatrix}, \tag{2.2.1}$$

Matriks K yang menjadi kunci harus merupakan matriks yang *invertible*. Sebab, K^{-1} yang merupakan invers matriks kunci digunakan untuk melakukan dekripsi (Wahyadyatmika dkk., 2014).

2.2.2 Teknik Enkripsi *Hill Cipher*

Proses enkripsi pada *Hill Cipher* dilakukan per blok *plaintext*. Ukuran blok tersebut harus sama dengan ukuran matriks kunci (Krisnawanti dkk., 2021). Sebelum membagi teks menjadi deretan blok-blok, *plaintext* terlebih dahulu dikonversi menjadi angka *American Standard Code for Information Interchange* (*ASCII*) 256. Berikut disajikan tabel *ASCII*.

Tabel 2.1 Tabel *ASCII* (0-115)

kode	karakter	kode	karakter	kode	karakter	kode	karakter
0	nul	29	gs	58	:	87	W
1	soh	30	rs	59	;	88	X
2	stx	31	us	60	<	89	Y
3	etx	32	space	61	=	90	Z
4	eot	33	!	62	>	91	[
5	enq	34	"	63	?	92	\
6	ack	35	#	64	@	93	]
7	bel	36	$	65	A	94	^
8	bs	37	%	66	B	95	_
9	tab	38	&	67	C	96	‘
10	lf	39	’	68	D	97	a
11	vt	40	(	69	E	98	b
12	np	41	)	70	F	99	c
13	cr	42	*	71	G	100	d
14	so	43	+	72	H	101	e
15	si	44	,	73	I	102	f
16	dle	45	-	74	J	103	g
17	dc1	46	.	75	K	104	h
18	dc2	47	/	76	L	105	i
19	dc3	48	0	77	M	106	j
20	dc4	49	1	78	N	107	k
21	nak	50	2	79	O	108	l
22	syn	51	3	80	P	109	m
23	etb	52	4	81	Q	110	n
24	can	53	5	82	R	111	o
25	em	54	6	83	S	112	p
26	eof	55	7	84	T	113	q
27	esc	56	8	85	U	114	r
28	fs	57	9	86	V	115	s

Tabel 2.2 Tabel *ASCII* (116-255)

kode	karakter	kode	karakter	kode	karakter	kode	karakter	kode	karakter
116	t	144		172	¬	200	È	228	ä
117	u	145	‘	173		201	É	229	å
118	v	146	’	174	®	202	Ê	230	æ
119	w	147	“	175	¯	203	Ë	231	ç
120	x	148	”	176	°	204	Ì	232	è
121	y	149	•	177	±	205	Í	233	é
122	z	150	–	178	²	206	Î	234	ê
123	{	151	—	179	³	207	Ï	235	ë
124	|	152	~	180	´	208	Ð	236	ì
125	}	153	™	181	µ	209	Ñ	237	í
126	~	154	Š	182	¶	210	Ò	238	î
127	-	155	›	183	·	211	Ó	239	ï
128	€	156	œ	184	¸	212	Ô	240	ð
129		157		185	¹	213	Õ	241	ñ
130	,	158	ž	186	º	214	Ö	242	ò
131	*f*	159	Ÿ	187	»	215	×	243	ó
132	„	160	nbsp	188	¼	216	Ø	244	ô
133	…	161	¡	189	½	217	Ù	245	õ
134	†	162	¢	190	¾	218	Ú	246	ö
135	‡	163	£	191	¿	219	Û	247	÷
136	^	164	¤	192	À	220	Ü	248	ø
137	‰	165	¥	193	Á	221	Ý	249	ù
138	Š	166	¦	194	Â	222	Þ	250	ú
139	‹	167	§	195	Ã	223	ß	251	û
140	Œ	168	¨	196	Ä	224	à	252	ü
141		169	©	197	Å	225	á	253	ý
142	Ž	170	ª	198	Æ	226	â	254	þ
143		171	«	199	Ç	227	ã	255	ß

Secara matematis, proses enkripsi pada *Hill Cipher* adalah:

$$C = K.P, \tag{2.2.2}$$

dengan:
C = *ciphertext*,
K = kunci,
P = plaintext
(Putra dan Ariyus, 2021).

2.2.3 Teknik Dekripsi *Hill Cipher*

Proses dekripsi pada *Hill Cipher* pada dasarnya sama dengan proses enkripsinya. Namun, matriks kunci harus dibalik terlebih dahulu. Secara matematis, proses dekripsi pada *Hill Cipher* adalah:

$$P = K^{-1}.C \tag{2.2.3}$$

(Putra dan Ariyus, 2021).

Contoh 2.2.1 Suatu pesan "Cutalu Aki" akan dienkripsi dengan kunci *Hill*

$$K = \begin{bmatrix} 5 & 1 \\ 11 & 4 \end{bmatrix}.$$

Langkah pertama: bagi pesan menjadi blok-blok matriks dengan ukuran 2×1 lalu ubah setiap karakter ke dalam kode *ASCII* 256.

$$P_1 = \begin{bmatrix} C \\ u \end{bmatrix} = \begin{bmatrix} 67 \\ 117 \end{bmatrix}, P_2 = \begin{bmatrix} t \\ a \end{bmatrix} = \begin{bmatrix} 116 \\ 97 \end{bmatrix}, P_3 = \begin{bmatrix} l \\ u \end{bmatrix} = \begin{bmatrix} 108 \\ 117 \end{bmatrix}$$
$$P_4 = \begin{bmatrix} 'spasi' \\ A \end{bmatrix} = \begin{bmatrix} 32 \\ 65 \end{bmatrix}, P_5 = \begin{bmatrix} k \\ i \end{bmatrix} = \begin{bmatrix} 107 \\ 105 \end{bmatrix}.$$

Langkah kedua: kalikan setiap blok p dengan matriks kunci K dari sebelah kanan. Lalu, dilakukan modulo 256.

$$C_1 = K.P_1 = \begin{bmatrix} 196 \\ 181 \end{bmatrix}, C_2 = K.P_2 = \begin{bmatrix} 165 \\ 128 \end{bmatrix}, C_3 = K.P_3 = \begin{bmatrix} 145 \\ 120 \end{bmatrix}$$
$$C_4 = K.P_4 = \begin{bmatrix} 225 \\ 100 \end{bmatrix}, C_5 = K.P_5 = \begin{bmatrix} 61 \\ 128 \end{bmatrix}.$$

Langkah ketiga: ubah setiap karakter dari langkah kedua ke dalam karakter *ASCII* 256 lalu gabungkan setiap karakter. Diperoleh ciphertext adalah "Äµ¥€'xád=€". Selanjutnya, akan dilakukan proses dekripsi dari *ciphertext*.
Langkah keempat: hitung determinan dari matriks kunci.

$$\det(K) = ad - bc = 20 - 11 = 9$$

Langkah kelima: hitung invers determinan terhadap modulo 256.

$$9x \equiv 1 \text{ (mod 256)}$$
$$57.9x \equiv 57.1 \text{ (mod 256)}$$
$$x \equiv 57 \text{ (mod 256)}$$

Langkah keenam: hitung invers matriks kunci

$$K^{-1} = x. \begin{bmatrix} 4 & -1 \\ -11 & 5 \end{bmatrix} = 57. \begin{bmatrix} 4 & -1 \\ -11 & 5 \end{bmatrix} \mod (256) = \begin{bmatrix} 228 & -57 \\ -627 & 285 \end{bmatrix}$$

Langkah ketujuh: hitung p_i dengan cara kalikan C_i dengan K^{-1} dari kiri untuk $i = 1, 2, 3, 4, 5$. Kemudian, gabungkan p_i setelah diubah ke dalam karakter *ASCII* 256. Dengan demikian, hasil dekripsinya adalah "Cutalu Aki".

2.3 *RSA Cipher*

Algoritma kriptografi RSA merupakan algoritma kriptografi kunci publik. Algoritma ini ditemukan pertama kali pada tahun 1977 oleh R. Rivest, A. Shamir, dan L. Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Algoritma RSA merupakan blok *cipher* dimana semua informasi dipetakan ke sebuah *integer*. Algoritma RSA terdiri dari kunci publik dan kunci *private* dimana kunci publik dapat diketahui oleh semua orang sedangkan kunci *private* hanya diketahui oleh pemilik data. Proses enkripsi menggunakan kunci publik dan proses dekripsi menggunakan kunci *private* pemilik data (Wahyadyatmika dkk., 2014). Algoritma ini mempunyai tingkat reliabilitas keamanan yang tinggi karena menggunakan dua bilangan prima yang besar dalam membangkitkan kuncinya (Suhandinata dkk., 2019). Algoritma ini terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi.

2.3.1 Proses Pembentukan Pasangan Kunci

Berikut ini adalah proses pembentukan kunci dalam algoritma kriptografi RSA:

1. Pilih dua bilangan prima yang diberi simbol sebagai p dan q (nilai $p \neq q$).
2. Hitung nilai $n = p.q$ ($p \neq q$, karena jika $p = q$, maka nilai $n = p^2$ sehingga nilai p dapat diperoleh dengan menarik akar pangkat dua dari n).
3. Hitung nilai $\psi(n) = (p-1).(q-1)$.
4. Pilih kunci publik e yang relatif prima terhadap $\psi(n)$.
5. Bangkitkan kunci *private* dengan persamaan $e.d \equiv 1 \pmod{\psi(n)}$ dimana $1 < d < \psi(n)$. Perhatikan bahwa persamaan $e.d \equiv 1 \pmod{\psi(n)}$ ekuivalen dengan $e.d = 1 + k.\psi(n)$, sehingga untuk mencari nilai d dapat dihitung dengan $s = \frac{1+k.\psi(n)}{e}$.

Hasil dari pembentukan kunci tersebut adalah:

a. kunci publik (e, n);

b. kunci private (d, n).

Nilai n tidak bersifat rahasia karena diperlukan pada saat perhitungan proses enkripsi dan dekripsi (Wahyadyatmika dkk., 2014).

2.3.2 Proses Enkripsi *RSA Cipher*

Berikut ini adalah proses enkripsi dalam algoritma kriptografi RSA:

1. Kunci publik (e, n).
2. Pilih plainteks m dan ubah isi pesan m menjadi pesan dengan nilai *ASCII*.
3. Potong pesan menjadi blok-blok pesan $m_1, m_2, m_3, \ldots$ dengan nilai setiap bloknya adalah $0 \leq m \leq n - 1$.
4. Setiap blok m dihitung dengan rumus $c_i = m_i^e \bmod n$.
5. Susun nilai c hasil enkripsi dengan susunan $c_1, c_2, c_3, \ldots, c_n$ sehingga diperoleh *cipherteks* dari pesan m.

(Wahyadyatmika dkk., 2014).

2.3.3 Proses Dekripsi *RSA Cipher*

Berikut ini adalah proses dekripsi dalam algoritma kriptografi RSA:

1. Ambil pesan (*cipherteks*) yang telah diterima.
2. Kemudian ambil kunci rahasia (d, n).
3. Potong pesan menjadi blok-blok pesan $c_1, c_2, c_3, \ldots$ dengan nilai setiap bloknya adalah $0 \leq c \leq n - 1$.
4. Hitung $m_i = c_i^d \bmod n$.
5. Susun nilai m hasil dekripsi dengan susunan $m_1, m_2, m_3, \ldots, m_n$ sehingga diperoleh *plainteks* (pesan asli) dari *cipherteks* yang diterima.

(Wahyadyatmika dkk., 2014).

Contoh 2.3.1 Sebuah pesan "Suka Aljabar" akan dienkripsi dengan kunci publik (49,1927) dan akan didekripsi dengan kunci *private* (1089, 1927).

Langkah pertama: ubah pesan menjadi blok-blok dan cocokkan karakter dengan kode *ASCII* 256.
Diperoleh:
$m_1 = S = 83, m_2 = u = 117, m_3 = k = 107, m_4 = a = 97, m_5 = `space` = 32, m_6 = A = 65, m_7 = l = 108, m_8 = j = 106, m_9 = a = 97, m_{10} = b = 98, m_{11} = a = 97$, dan $m_{12} = r = 114$.

Langkah kedua: hitung hasil enkripsi tiap karakternya dengan kunci publik.

$$c_1 = m_1^{49} \text{ mod } (1927) = 83^{49} \text{ mod } (1927) = 1395;$$
$$c_2 = m_2^{49} \text{ mod } (1927) = 117^{49} \text{ mod } (1927) = 1498;$$
$$c_3 = m_3^{49} \text{ mod } (1927) = 107^{49} \text{ mod } (1927) = 1868;$$
$$c_4 = m_4^{49} \text{ mod } (1927) = 97^{49} \text{ mod } (1927) = 967;$$
$$c_5 = m_5^{49} \text{ mod } (1927) = 32^{49} \text{ mod } (1927) = 1795;$$
$$c_6 = m_6^{49} \text{ mod } (1927) = 65^{49} \text{ mod } (1927) = 1696;$$
$$c_7 = m_7^{49} \text{ mod } (1927) = 108^{49} \text{ mod } (1927) = 1616;$$
$$c_8 = m_8^{49} \text{ mod } (1927) = 106^{49} \text{ mod } (1927) = 835;$$
$$c_9 = m_9^{49} \text{ mod } (1927) = 97^{49} \text{ mod } (1927) = 967;$$
$$c_{10} = m_{10}^{49} \text{ mod } (1927) = 98^{49} \text{ mod } (1927) = 346;$$
$$c_{11} = m_{11}^{49} \text{ mod } (1927) = 97^{49} \text{ mod } (1927) = 967;$$
$$c_{12} = m_{12}^{49} \text{ mod } (1927) = 114^{49} \text{ mod } (1927) = 1467.$$

Dengan demikian, hasil enkripsinya adalah

$$(1395, 1498, 1868, 967, 1795, 1696, 1616, 835, 967, 346, 967, 1467).$$

Langkah ketiga: dekripsikan langkah kedua dengan kunci *private*.

$$m_1 = c_1^{1089} \text{ mod } (1927) = 1395^{1089} \text{ mod } (1927) = 83;$$
$$m_2 = c_2^{1089} \text{ mod } (1927) = 1498^{1089} \text{ mod } (1927) = 117;$$
$$m_3 = c_3^{1089} \text{ mod } (1927) = 1868^{1089} \text{ mod } (1927) = 107;$$
$$m_4 = c_4^{1089} \text{ mod } (1927) = 967^{1089} \text{ mod } (1927) = 97;$$
$$m_5 = c_5^{1089} \text{ mod } (1927) = 1795^{1089} \text{ mod } (1927) = 32;$$
$$m_6 = c_6^{1089} \text{ mod } (1927) = 1696^{1089} \text{ mod } (1927) = 65;$$
$$m_7 = c_7^{1089} \text{ mod } (1927) = 1616^{1089} \text{ mod } (1927) = 108;$$
$$m_8 = c_8^{1089} \text{ mod } (1927) = 835^{1089} \text{ mod } (1927) = 106;$$
$$m_9 = c_9^{1089} \text{ mod } (1927) = 967^{1089} \text{ mod } (1927) = 97;$$

$$m_{10} = c_{10}^{1089} \text{ mod } (1927) = 346^{1089} \text{ mod } (1927) = 98;$$
$$m_{11} = c_{11}^{1089} \text{ mod } (1927) = 967^{1089} \text{ mod } (1927) = 97;$$
$$m_{12} = c_{12}^{1089} \text{ mod } (1927) = 1467^{1089} \text{ mod } (1927) = 114.$$

Diperoleh, hasil dekripsinya adalah

$$\{83,117,107,97,32,65,108,106,97,98,97,114\}.$$

Langkah keempat: ubah setiap blok hasil dekripsi ke dalam karakter *ASCII* 256. Dengan demikian, hasil dekripsinya adalah “Suka Aljabar”.

2.4 Keterbagian

Sebelum membahas lebih lanjut mengenai keterbagian, terlebih dahulu akan didefinisikan mengenai suatu bilangan dikatakan habis membagi bilangan lainnya. Semua definisi dan teorema pada bagian ini diambil dari buku Hwang dkk. yang berjudul "*Introduction to Number Theory*".

Definisi 2.4.1 Jika m dan n bilangan bulat, m dikatakan habis membagi n (dinotasikan $m|n$) jika terdapat bilangan bulat k sedemikian sehingga $n = km$.

Selanjutnya, akan diberikan contoh mengenai dua bilangan yang dikatakan habis membagi.

Contoh 2.4.2 Bilangan 5 habis membagi bilangan 60 karena terdapat bilangan 12 sedemikian sehingga 60 = 5.12.

Selanjutnya, akan dijelaskan beberapa teorema terkait dengan keterbagian.

Teorema 2.4.3 Jika m, n dan r bilangan bulat, maka berlaku:

a. $n|n$ (setiap bilangan bulat habis membagi dirinya sendiri)

b. $1|m$ (1 habis membagi semua bilangan bulat)

c. Jika $n|m$ dan $m|r$ maka $n|r$

d. Jika $n|m$ dan $n|r$ maka $n|m + r$ dan $n|m - r$

e. Jika $n|1$ maka $n = \pm 1$

f. Jika $n|m$ dan $m|n$ maka $n = \pm m$.

Bilangan bulat a dapat dinyatakan sebagai penjumlahan dari bq dengan r dimana q, r bilangan bulat dan b bulat positif seperti yang tercantum dalam teorema berikut.

Teorema 2.4.4 Jika a dan b bilangan bulat, dengan b positif, maka terdapat tunggal bilangan bulat q dan r sedemikian sehingga $a = bq + r$ dan $0 \leq r < b$.

Selanjutnya, akan dijelaskan mengenai relatif prima antara dua bilangan bulat tak-nol a dan b.

Teorema 2.4.5 Dua bilangan bulat a dan b tak nol, disebut relatif prima jika dan hanya jika persamaan $ax + by = 1$ memiliki solusi pada bilangan bulat x dan y.

2.5 Kongruensi

Sebelum membahas lebih lanjut mengenai kongruensi, terlebih dahulu akan didefinisikan mengenai kongruen. Semua definisi dan teorema pada bagian ini diambil dari buku Hwang dkk. yang berjudul "*Introduction to Number Theory*".

Definisi 2.5.1 Jika a, b dan n bilangan bulat, dengan n positif, dikatakan a kongruen dengan b modulo n (ditulis $a \equiv b$ (mod n)), jika n habis membagi $a - b$.

Contoh 2.5.2 1 kongruen dengan 15 modulo 7 karena 7 habis membagi $(1 - 15 = -14)$ atau dapat ditulis sebagai $1 \equiv 15$ (mod 7).

Teorema 2.5.3 Diberikan a, b, c dan n bilangan bulat, dengan n positif, maka

i) $a \equiv a$ (mod n),

ii) jika $a \equiv b$ (mod n), maka $b \equiv a$ (mod n),

iii) jika $a \equiv b$ (mod n) dan $b \equiv c$ (mod n), maka $a \equiv c$ (mod n).

Teorema 2.5.4 Elemen tak nol $\bar{a}$ pada $\mathbb{Z}_n$ mempunyai invers perkalian jika dan hanya jika a dan n relatif prima.

2.6 Matriks

Sebelum membahas lebih lanjut mengenai matriks, terlebih dahulu akan didefinisikan mengenai matriks. Semua definisi dan teorema pada bagian ini diambil dari buku Anton dan Kaul yang berjudul "*Elementary Linear Algebra* (12 ed.)".

Definisi 2.6.1 Matriks adalah *array* angka berbentuk persegi panjang. Angka pada *array* disebut entri dari matriks.

Contoh 2.6.2 Diberikan matriks

$$A = \begin{bmatrix} 2 & -1 & -1 \\ -2 & 3 & 2 \end{bmatrix}.$$

Ukuran matriks A adalah 2×3.

Definisi 2.6.3 Dua matriks dikatakan sama jika memiliki ukuran yang sama dan entri yang berkorespodensi sama.

Contoh 2.6.4 Diberikan dua matriks

$$A = \begin{bmatrix} 1 & -1 \\ 1 & a \end{bmatrix}, B = \begin{bmatrix} 1 & b \\ 1 & 0 \end{bmatrix}.$$

Matriks A sama dengan matriks B jika $a = 0$ dan $b = -1$.

Definisi 2.6.5 Jika A matriks persegi dan terdapat matriks B dengan ukuran yang sama dimana $AB = BA = I$, maka A dikatakan *invertible* atau nonsingular dan B dikatakan invers dari A. Jika tidak terdapat matriks B, maka A dikatakan singular.

Contoh 2.6.6 Matriks

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

merupakan matriks nonsingular karena terdapat matriks B

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

sehingga

$$AB = BA = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Selanjutnya, akan dibahas mengenai matriks *invertible* dan invers dari matriks ukuran 2×2.

Teorema 2.6.7 Matriks

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

adalah *invertible* jika dan hanya jika $ad - bc \neq 0$, dengan rumus *invers* sebagai berikut:

$$A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Selanjutnya, akan dibahas mengenai pengertian minor dan kofaktor pada sebuah matriks persegi.

Definisi 2.6.8 Jika A adalah matriks persegi, maka minor dari entri a_{ij} dinotasikan dengan M_{ij} adalah determinan dari submatriks tersisa setelah baris ke-i dan kolom ke-j dihapus dari A. Nilai $(-1)^{i+j}M_{ij}$ dinotasikan dengan C_{ij} disebut kofaktor dari entri a_{ij}.

Selanjutnya, akan dibahas mengenai pencarian determinan matriks persegi menggunakan minor dan kofaktor.

Definisi 2.6.9 Jika A adalah matriks $n \times n$, maka nilai yang diperoleh dengan mengalikan entri-entri pada setiap baris dan kolom A dengan kofaktor-kofaktor yang bersesuaian dan menjumlahkan hasil perkaliannya disebut determinan dari A, dan jumlahnya disebut ekspansi kofaktor dari A, yaitu

$$\det(A) = a_{1j}C_{1j} + a_{2j}C_{2j} + \cdots + a_{nj}C_{nj}$$

dan

$$\det(A) = a_{i1}C_{i1} + a_{i2}C_{i2} + \cdots + a_{in}C_{in}.$$

Contoh 2.6.10 Matriks

$$A = \begin{bmatrix} 1 & 4 & 9 \\ 5 & 6 & 8 \\ -1 & 3 & 2 \end{bmatrix}$$

akan ditentukan $\det(A)$ dengan menggunakan ekspansi kofaktor.
Pertama, akan dicari terlebih dahulu minor dari M_{11}, M_{21},dan M_{31}.

$$M_{11} = \begin{vmatrix} 6 & 8 \\ 3 & 2 \end{vmatrix} = 12 - 24 = -12,$$
$$M_{21} = \begin{vmatrix} 4 & 9 \\ 3 & 2 \end{vmatrix} = 8 - 27 = -19,$$
$$M_{31} = \begin{vmatrix} 4 & 9 \\ 6 & 8 \end{vmatrix} = 32 - 54 = -22.$$

Selanjutnya, akan dicari kofaktor dari C_{11}, C_{21}, C_{31}.

$$\begin{aligned} C_{11} &= (-1)^{1+1} M_{11} = -12, \\ C_{21} &= (-1)^{2+1} M_{21} = 19, \\ C_{31} &= (-1)^{3+1} M_{31} = -22. \end{aligned}$$

Lalu, dicari $\det(A)$ dengan menggunakan rumus

$$\det(A) = a_{11}C_{11} + a_{21}C_{21} + a_{31}C_{31}.$$

Kemudian, diperoleh hasil sebagai berikut.

$$\det(A) = -12 + 5.19 + (-22).(-1) = 105.$$

Oleh karena itu, determinan dari matriks A dengan ekspansi kofaktor adalah 105.

BAB III

METODE PENELITIAN

3.1 Waktu dan Tempat Penelitian

Penelitian ini dilakukan pada semester ganjil tahun ajaran 2023/2024 di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung yang beralamatkan di Jalan Prof. Dr. Ir. Soemantri Brojonegoro, Gedong Meneng, Kecamatan Rajabasa, Kota Bandar Lampung, Lampung.

3.2 Metode Penelitian

Langkah-langkah dalam mencapai tujuan penelitian ini adalah sebagai berikut.

1. Mempelajari *Hill Cipher* dan konsep-konsep Aljabar Linear, khususnya matriks, determinan matriks, dan invers matriks dari jurnal, buku, dan artikel ilmiah.
2. Mempelajari *RSA Cipher* dan konsep Teori Bilangan, khususnya keterbagian dan kongruensi dari jurnal, buku, dan artikel ilmiah.
3. Memodifikasi ukuran matriks kunci *Hill Cipher* menjadi $n \times n$ dan menggunakan 256 karakter *ASCII*.
4. Mempelajari penggabungan *Hill Cipher* dengan *RSA Cipher*.
5. Membuat program terkait *Hybrid Hill Cipher* dan *RSA Cipher* dalam mengamankan pesan. Dengan tahapan sebagai berikut:
   (a) menginput dan menghitung panjang pesan yang akan dienkripsi;
   (b) menginput ukuran dan membuat matriks kunci *Hill Cipher*;
   (c) selanjutnya, cek apakah $\det(K) \neq 0$ atau tidak. Jika tidak, maka proses kembali ke langkah b. Jika iya, maka proses dilanjutkan dengan memeriksa FPB$(\det(K), 256) = 1$. Jika iya, maka lanjut ke langkah d. Jika tidak, maka ulangi langkah b hingga dua kondisi sebelumnya terpenuhi;

(d) kemudian, cek apakah panjang ukuran matriks kunci yang digunakan habis membagi panjang pesan. Jika iya, maka langsung lanjut ke langkah e. Jika tidak, maka terlebih dahulu dilakukan penambahan karakter 'nul' ke dalam pesan. Kemudian, dilakukan pengecekan kembali apakah kondisi sudah terpenuhi atau belum. Proses ini akan terus berjalan hingga panjang ukuran matriks kunci habis membagi panjang pesan;

(e) lakukan proses enkripsi dengan menggunakan matriks kunci yang digunakan;

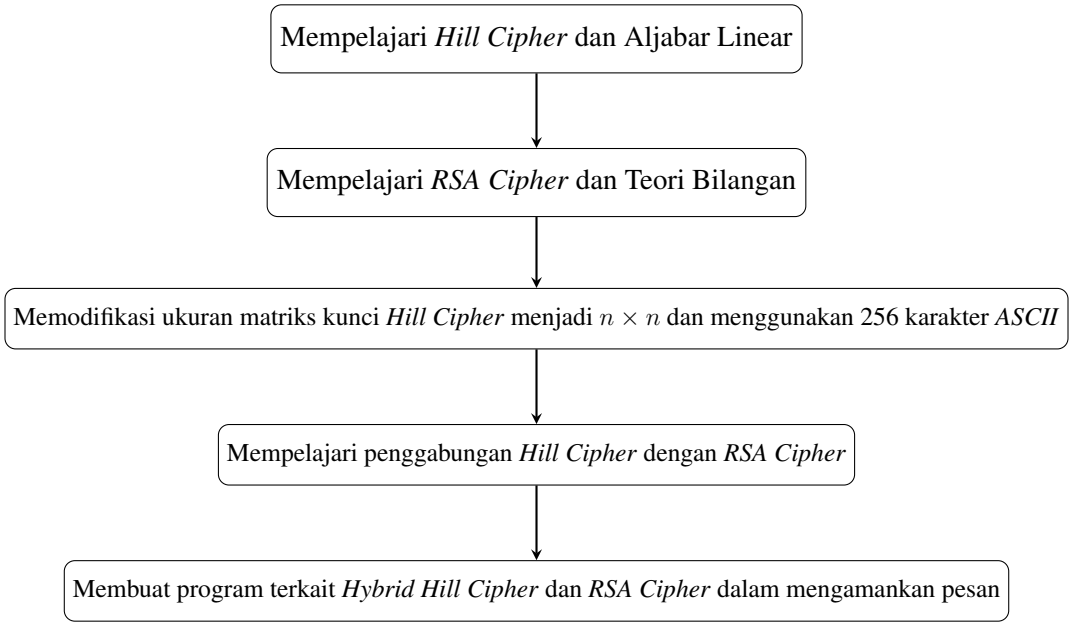
(f) membangun kunci publik dan *private*;

(g) kemudian, lakukan proses enkripsi *RSA Cipher* dengan menggunakan kunci public;

(h) lalu, dekripsi hasil enkripsi *RSA Cipher* dengan kunci *private* yang telah dibangun;

(i) setelah itu, lakukan proses dekripsi *Hill Cipher* dengan invers matriks kunci yang digunakan;

(j) terakhir, cek apakah panjang dekripsi pesan sama dengan pesan awal atau tidak. Jika iya, maka program selesai. Jika tidak, maka program akan menghapus karakter nul dari pesan, hingga kondisi terpenuhi.



Gambar 3.1 Langkah-langkah Penelitian

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan pada Bab IV diperoleh kesimpulan bahwa proses enkripsi pesan menggunakan *hybrid Hill Cipher* dan *RSA Cipher* dapat dibagi berdasarkan panjang pesan dan panjang matriks kunci yang digunakan. Jika panjang pesan tidak habis dibagi oleh panjang matriks kunci, maka perlu dilakukan penambahan karakter "nul" pada pesan hingga panjang pesan habis dibagi oleh panjang matriks kunci. Hal ini berakibat pada proses dekripsi yang mengharuskan pengurangan karakter "nul" hingga panjang *ciphertext* sama dengan panjang pesan awal. Selain itu, dapat disimpulkan juga bahwa semakin besar ukuran matriks kunci dan semakin panjang *bits* yang digunakan, maka hasil enkripsi yang dihasilkan jauh lebih aman dikarenakan jumlah kemungkinan kunci bergantung dengan ukuran matriks kunci dan panjang *bits*. Secara keseluruhan, program yang telah dibuat sudah berjalan dengan baik dari segi ketepatan enkripsi dan dekripsi dengan perhitungan manual, serta seluruh karakter dapat terbaca oleh program dan juga program dapat melakukan eksekusi sesuai dengan pembagian kasus yang dilakukan.

5.2 Saran

Berdasarkan hasil penelitian yang sudah dilakukan, peneliti merasa masih perlu dilakukan analisis lebih mendalam lagi mengenai kriptosistem yang sudah dibuat dan diharapkan dapat dikembangkan lagi sehingga menghasilkan kriptosistem yang jauh lebih aman lagi.

DAFTAR PUSTAKA

Anton, H., dan Kaul, A. (2019). *Elementary Linear Algebra* (12 ed.). Wiley.

Cahyanti, N. D., Turmudi, T., dan Khudzaifah, M. (2023). Modifikasi Vigenere Cipher Menggunakan Grup Simetri untuk Mengamankan Pesan Teks. *Jurnal Riset Mahasiswa Matematika*, 2(5), 173–185.

Fauzi, A., Novriyenni, Maulita, Y., dan Pardede, A. M. (2017). Analisis Hybrid Cryptosystem Algoritma RSA dan Triple DES. *Jurnal Teknik Informatika Kaputama* (JTIK), 1(2), 36–44.

Hanafi, J. I., dan Patombongi, A. (2016). Aplikasi Sms Kriptografi Menggunakan Metode Aes Berbasis Android. *Simtek: jurnal sistem informasi dan teknik komputer*, 1(1), 69–75.

Hwang, S. O., Kim, I., dan Lee, W. K. (2021). Introduction to Number Theory. *In Modern Cryptography with Proof Techniques and Applications*.

Jamaludin. (2018). Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem. *Publikasi Jurnal dan Penelitian Teknik Informatika* , 2(2), 89–93.

Krisnawanti, G., Santoso, K. A., dan Kamsyakawuni, A. (2021). Modifikasi Huffman dengan Hill Cipher pada Pengkodean Data Teks. *PRISMA, Prosiding Seminar Nasional Matematika*, 4, 534–539.

Makhomah, R., Santoso, K. A., dan Kamsyakawuni, A. (2021). Pengkodean Teks Menggunakan Kombinasi Hill Cipher dan Operasi XOR. *PRISMA, Prosiding Seminar Nasional Matematika*, 4, 548–552.

Nasrudin, Pratama, A., Pratama, E., dan Wulandari, E. T. (2020). Implementasi Algoritma Elgamal dan kode HILL Untuk Keamanan Database. *Paper Teknik Informatika*.

Pangaribuan, L. J. (2018). Kriptografi Hybrida Agloritma Hill Cipher Dan Rivest Shamir Adleman (RSA) Sebagai Pengembangan Kriptografi Kunci Simetris (Studi Kasus: Nilai Mahasiswa Amik Mbp). *Jurnal Teknologi Informasi Dan Komunikasi*, 7(1), 11–26.

Pawan, E., Kaharuddin, K., dan Arius, D. (2019). Kombinasi Arnold Cat Map dan Modifikasi Hill Cipher Menggunakan Kode Bunyi Beep Bios Phoenix. *Sisfotenika*, 9(2), 159.

Putra, F. S., dan Ariyus, D. (2021). Enkripsi dan Dekripsi Teks Menggunakan Hill Cipher Dengan Matriks Ordo 3 x 3. *Jurti*, 5(1), 17–22.

Rachmawati, D., Sharif, A., dan Ericko. (2019). Hybrid Cryptosystem Combination Algorithm of Hill Cipher 3x3 and Elgamal to Secure Instant Messaging for Android. *Journal of Physics: Conference Series*, 1235(1).

Santoso, Y. S. (2021). Message Security Using a Combination of Hill Cipher and RSA Algorithms. *Jurnal Matematika Dan Ilmu Pengetahuan Alam LLDikti Wilayah 1 (JUMPA)*, 1(1), 20–28.

Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., dan Srinjiwi. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA. *Jurteksi*, VI(1), 1–10.

Sumarno. (2018). Analisis Kinerja Kombinasi Algoritma Message-Digest Algortihm 5 (MD5), Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) Pada Keamanan E-Dokumen. *Jurnal Sistem Informasi Ilmu Komputer Prima*, 2(1), 1–71.

Ulva, A. F. (2019). Analisis Kinerja Kombinasi Algoritma Affine Chiper, Hill Cipher dan Algoritma El Gamal dalam Pengamanan Data. *Jurnal Sistem Informasi*, 3(1), 63–75.

Wahyadyatmika, A. P., Isnanto, R. R., dan Somantri, M. (2014). Implementasi Algoritma Kriptografi RSA pada Surat Elektronik (E-Mail). *Transient*, 3(4), 1–9.

Wasil, M. (2023). Implementasi Matriks Dalam Kriptografi Hill Cipher Dalam Mengamankan Pesan Rahasia. *Zeta - Math Journal*, 8(2), 71–78.