

**KRIPTOGRAFI HYBRID METODE HILL CIPHER
DAN ELGAMAL DALAM MENINGKATKAN
KEAMANAN PESAN RAHASIA**



JURUSAN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN GANESHA

SINGARAJA

2024

**KRIPTOGRAFI HYBRID METODE HILL CIPHER
DAN ELGAMAL DALAM MENINGKATKAN
KEAMANAN PESAN RAHASIA**

SKRIPSI

**Diajukan kepada
Universitas Pendidikan Ganesha
Untuk Memenuhi Salah Satu Persyaratan dalam menyelesaikan
Program Sarjana Matematika**



**JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN GANESHA
SINGARAJA**

2024

LEMBAR PERSETUJUAN DAN PENGESAHAN PANITIA UJIAN

Diterima oleh Panitia Ujian Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Pendidikan Ganesha
guna memenuhi syarat-syarat untuk mencapai gelar sarjana Matematika

Pada:

Hari : Kamis
Tanggal : 11 Juli 2024



LEMBAR PERSETUJUAN DOSEN PENGUJI

Skripsi oleh Faizar Rusyadi ini
telah dipertahankan di depan dewan penguji
pada tanggal 11 JULI 2024.....

Dewan Penguji,



Dr. I Made Sugiarta, M.Si
NIP. 19671020 199303 1 001

(Ketua)

Dr. I Nyoman Sukajaya, M.T
NIP. 19671115 199303 1 001

(Anggota)

Prof. Dr. I Nengah Suparta, M.Si
NIP. 19650711 199003 1 003

(Anggota)

Dr. Gede Suweken, M.Sc
NIP. 19611111 198702 1 001

(Anggota)

PERNYATAAN

Dengan ini saya menyatakan bahwa karya tulis yang berjudul **“Kriptografi Hybrid Metode Hill Cipher dan ElGamal dalam Meningkatkan Keamanan Pesan Rahasia”** beserta seluruh isinya adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan dan mengutip dengan cara yang tidak sesuai dengan etika yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung resiko/sanksi yang dijatuhkan kepada saya apabila kemudian ditemukan adanya pelanggaran atas etika keilmuan dalam karya ini, atau ada klaim terhadap keaslian karya saya ini.

Singaraja,

Yang membuat pernyataan,



Faizar Rusyadi

NIM. 1813101027



PRAKATA

Dengan mengucapkan puji Syukur ke hadapan ALLAH. S.W.T. Tuhan Yang Maha Esa atas berkat dan rahmatnya, penulis dapat menyelesaikan Skripsi yang baik. Skripsi yang berjudul “**Kriptografi Hybrid Metode Hill Cipher dan ElGamal dalam Meningkatkan Keamanan Pesan Rahasia**”. Skripsi ini disusun untuk memenuhi salah satu persyaratan mencapai gelar Sarjana Sains Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam di Universitas Pendidikan Ganesha

Dalam menyelesaikan skripsi ini, penulis mendapat bimbingan, dorongan, motivasi, serta semangat dari berbagai pihak. Oleh karena itu penulis ingin mengucapkan terima kasih kepada :

1. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam atas Fasilitas yang diberikan selama saya menjalani studi hingga menyelesaikan studi sesuai rencana
2. Ketua Jurusan Matematika atas fasilitas dan waktu yang diberikan dalam Menyusun hingga menyelesaikan skripsi ini
3. Koordinator program Studi Matematika, Universitas Pendidikan Ganesha yang selalu meluangkan waktunya untuk memfasilitasi penulis hingga dapat terselesaikannya skripsi ini
4. Dr. I Made Sugiarta, M.Si yang merupakan dosen pembimbing I dan dosen pembimbing akademik sebagai panutan saya dalam banyak hal dan memberikan bimbingan, arahan, dan petunjuk sehingga dapat belajar banyak kepada beliau, sehingga dapat menyelesaikan skripsi ini dengan baik

5. Dr. I Nyoman Sukajaya, M.T yang merupakan dosen pembimbing II yang selalu memberikan semangat dalam mengerjakan skripsi, serta memberikan arahan dan petunjuk tentang materi perkuliahan matematika komputasi sehingga banyak hal yang saya pelajari dengan beliau.
6. Prof. I Nengah Suparta, M.Si selaku dosen penguji yang menjadi panutan selama saya menempuh perkuliahan dan memberikan motivasi, saran, masukan kepada saya dalam menyelesaikan studi sampai tahap akhir
7. Dr. Gede Suweken, M.Sc selaku dosen penguji yang selalu memberikan semangat dan salah satu dosen yang sangat baik serta mengajari ilmu pemodelan kepada saya dan teman-teman saya
8. Bapak/Ibu Dosen dan Laboran di Jurusan Matematika yang telah memberikan banyak bantuan berupa ilmu dan semangat yang membantu penyusunan skripsi ini terselesaikan dengan baik
9. Keluarga kecil saya, baik bapak, ibu, dan kedua adik saya yang selalu memberikan dukungan penuh selama mengerjakan skripsi dan doa-doa yang dipanjatkan selama ini sangat berarti bagi kehidupan saya khususnya dalam penyusunan skripsi ini.
10. Rekan Kerja, jajaran Staf, dan warga sekolah SMP Firdaus yang selalu memberikan motivasi, semangat dan pengalaman sehingga membantu dalam proses menyelesaikan skripsi ini
11. Keluarga besar Kamariah dan Moh. Sujai yang memberikan semangat dan dukungan penuh serta do'a dalam kehidupan saya yang selalu membantu dalam mengerjakan skripsi ini, sehingga skripsi ini bisa terselesaikan.

12. Orang yang selalu memberikan semangat, berupa hinaan yang menjadi motivasi saya untuk memacu semangat dalam terselesaikannya skripsi ini.
13. Youtube ILKOM UNU BLITAR yang menjadi sumber belajar dalam mengerjakan GUI Interface menggunakan program aplikasi java yang merupakan bagian dari skripsi ini, sehingga skripsi ini terselesaikan.
14. Habib Ja'far yang merupakan pendakwah, sehingga memotivasi saya dan mengajarkan kesabaran, sekaligus menghibur saya dengan candaan
15. Teman kelas saya Prodi Matematika yang selalu menjadi motivasi yang menuntun saya belajar mengenai skripsi dan memberikan banyak masukan, serta selalu memberikan semangat dan support saya.
16. tentunya terhadap diri sendiri, Faizar Rusyadi yang selalu belajar dan bertahan hingga pada tahap ini, terima kasih untuk menyelesaikan segala sesuatu hal dengan sangat baik

Penulis menyadari bahwa dalam penulisan skripsi ini, masih jauh dari kata sempurna dan banyak kekurangan dalam pembahasan materi dikarenakan kemampuan yang penulis miliki. Sehingga penulis mengharapkan kritik dan saran yang bersifat membangun. Penulis berharap skripsi ini dapat bermanfaat dan berguna bagi para pembacanya.

Singaraja,

Penulis

DAFTAR ISI

	HALAMAN
PRAKATA.....	i
ABSTRAK	iv
ABSTRACT	v
DAFTAR ISI	vi
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	4
1.3. Batasan Masalah.....	4
1.4. Tujuan Penelitian.....	4
1.5. Manfaat Penelitian	5
1.5.1. Manfaat Teoritis	5
1.5.2. Manfaat Praktis	5
BAB II KAJIAN TEORI.....	6
2.1. Landasan Matematika	6
2.1.1. Bilangan Prima	6
2.1.2. Matriks.....	8
2.1.3. Aritmatika Modular	13
2.1.4. Invers Modular	14
2.1.5. Masalah Logaritma Diskrit.....	15
2.2. Kriptografi.....	15
2.2.1. Kriptografi Simetris.....	18
2.2.2. Kriptografi Asimetris.....	19
2.3. Kriptosistem	20

2.3.1. Hill Chiper.....	21
2.3.2. Kriptanalisis.....	29
2.3.3. Algoritma ElGamal.....	31
2.3.4. Kriptografi Hybrid.....	36
2.4. Bahasa Pemrograman JAVA.....	45
2.5. Entropi.....	52
2.6. Kerangka Berpikir.....	52
BAB III METODOLOGI PENELITIAN.....	55
3.1. Mengidentifikasi Masalah.....	55
3.2. Mengkaji Model Dasar.....	56
3.3. Mengembangkan Model Dasar.....	58
3.4. Mengkonstruksi Program.....	59
3.4.1. Input atau Output.....	59
3.4.2. Rancangan Interface Program Aplikasi.....	60
3.4.3. Algoritma Penyandian pesan dengan menggunakan Kriptografi Hybrid Hill cipher dengan Algoritma ElGamal.....	65
3.5. Memvalidasi Program.....	66
3.6. Analisis Performa Kriptografi hybrid, ElGamal, dan Hill cipher.....	66
3.7. Kesimpulan.....	66
BAB IV HASIL DAN PEMBAHASAN.....	67
4.1. Skema Penyandian Pesan Teks dengan menggunakan Kriptografi Hybrid Hill Chiper dan Algoritma ElGamal.....	67
4.2. Algoritma Enkripsi dan Dekripsi Teks dengan Menggunakan Kriptografi Hybrid Hill Cipher dan Algoritma ElGamal.....	68
4.3. Program Aplikasi Kriptografi Hybrid Hill cipher dan Algoritma ElGamal.....	74
4.4. Validasi Program Aplikasi.....	81
4.4.1. Contoh Pembangkitan Kunci Menggunakan Program Aplikasi Kriptografi Hybrid Hill cipher dan Algoritma ElGamal.....	81
4.4.2. Contoh Enkripsi dengan menggunakan Program Aplikasi Kriptografi Hybrid Hill Cipher dan ElGamal.....	83
4.4.3. Proses Enkripsi.....	84
4.4.4. Contoh dekripsi menggunakan Program Aplikasi Kriptografi Hybrid Hill Cipher dan ElGamal.....	92

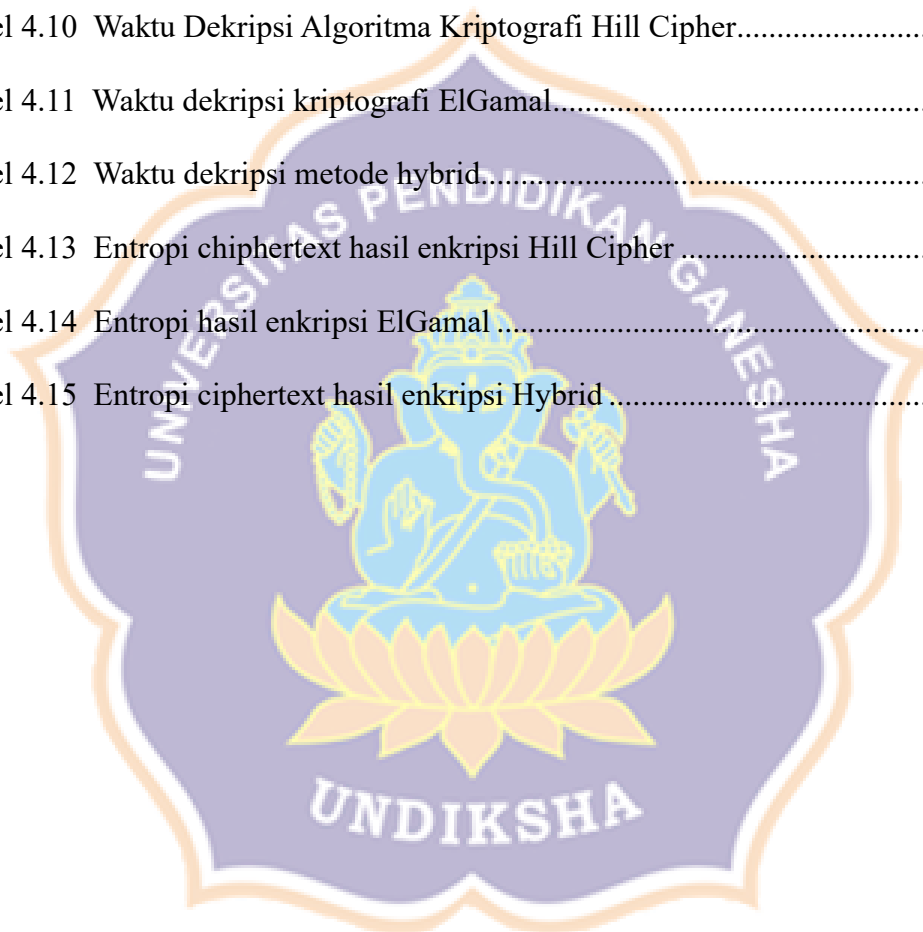
4.4.5. Proses Dekripsi.....	94
4.5. Analisis Algoritma kriptografi Hill Cipher, ElGamal, dan Hybrid	105
4.5.1. Analisis Waktu Enkripsi dan Nilai Entropi Ketiga Metode.....	105
4.5.2. Analisis Waktu Dekripsi Ketiga Metode	114
4.5.3. Analisis Entropi Ketiga Metode	122
BAB V PENUTUP.....	129
5.1. Kesimpulan.....	129
5.2. Saran.....	130
DAFTAR PUSTAKA	132
LAMPIRAN.....	136



DAFTAR TABEL

Tabel	Halaman
Tabel 2.1 Urutan Alfabet	23
Tabel 2.2 Blok – blok Plaintext hill cipher	24
Tabel 2.3 Blok – Blok Hill cipher dengan karakter dummy	24
Tabel 2.4 Ciphertext Hill cipher	26
Tabel 2.5 Memblok ciphertext dan mengubah ke bentuk angka	27
Tabel 2.6 Plaintext yang diubah dari angka ke huruf	29
Tabel 2.7 Menjadikan plaintext menjadi desimal ASCII dan blok	34
Tabel 2.8 Proses enkripsi algoritma kriptografi Elgamal	35
Tabel 2.9 Proses Dekripsi Algoritma kriptografi Elgamal	36
Tabel 2.10 Menjadikan plaintext beberapa blok menurut ukuran matriks kunci ..	38
Tabel 2.11 Mengubah plaintext menjadi angka menurut ASCII	38
Tabel 2.12 Ciphertext1 dari enkripsi hybrid diubah ke ASCII	40
Tabel 2.13 Proses enkripsi ciphertext1 metode hybrid	41
Tabel 2.14 Proses dekripsi ciphertext2 metode hybrid	42
Tabel 2.15 Ciphertext 1 kriptografi hybrid	43
Tabel 2.16 Hasil dekripsi ciphertext 1	45
Tabel 4.1. Proses perubahan plaintext menjadi desimal ASCII	85
Tabel 4.2. Menjadikan Plaintext menjadi blok – blok matriks	85
Tabel 4.3. Enkripsi Ciphertext1 Metode Hybrid	89
Tabel 4.4 Proses Dekripsi Ciphertext2 metode Hybrid	94
Tabel 4.5 Menjadikan bentuk ciphertext kedalam blok	101

Tabel	Halaman
Tabel 4.6 Mengubah Bentuk Desimal ASCII ke Bentuk Karakter	104
Tabel 4.7 Waktu enkripsi Algoritma Hill cipher	105
Tabel 4.8 Waktu Enkripsi Algoritma ElGamal.....	108
Tabel 4.9 Waktu Enkripsi metode Hybrid.....	110
Tabel 4.10 Waktu Dekripsi Algoritma Kriptografi Hill Cipher.....	114
Tabel 4.11 Waktu dekripsi kriptografi ElGamal.....	117
Tabel 4.12 Waktu dekripsi metode hybrid.....	119
Tabel 4.13 Entropi chiphertext hasil enkripsi Hill Cipher.....	122
Tabel 4.14 Entropi hasil enkripsi ElGamal	124
Tabel 4.15 Entropi ciphertext hasil enkripsi Hybrid.....	125

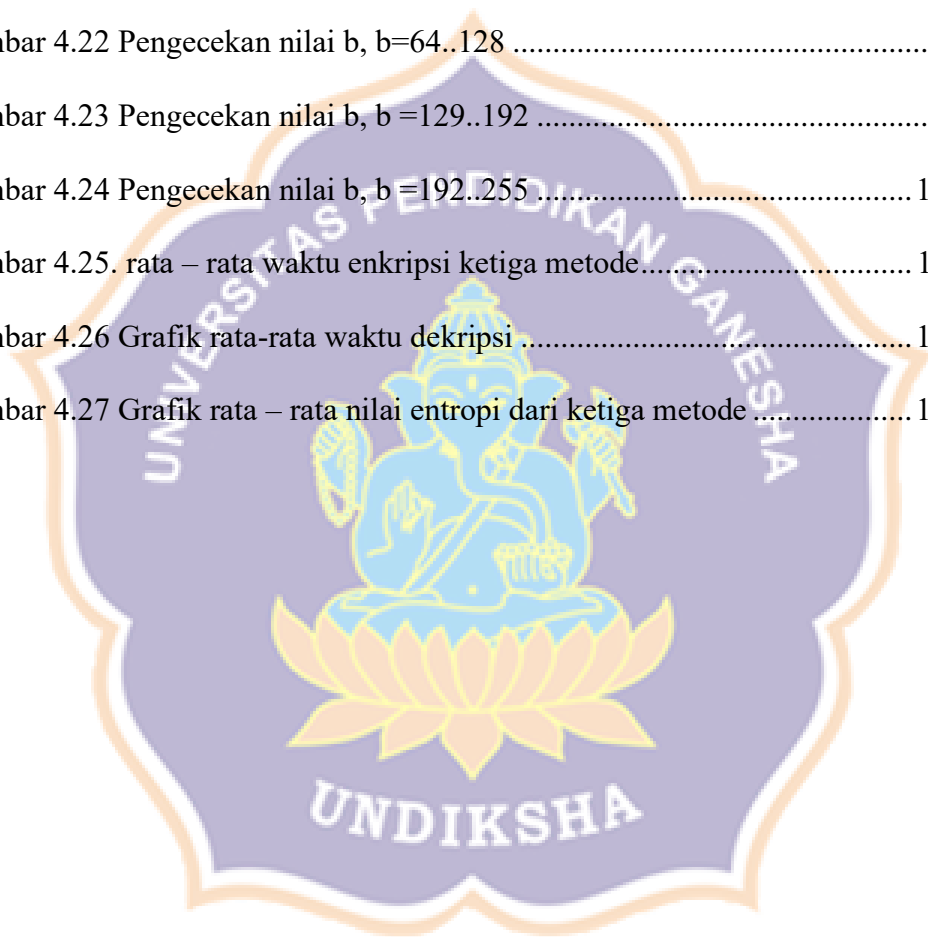


DAFTAR GAMBAR

Gambar	Halaman
Gambar 2.1 Diagram proses enkripsi dan dekripsi	17
Gambar 2.2 Proses Enkripsi dan dekripsi kriptografi simetris	19
Gambar 2.3 Proses Enkripsi dan dekripsi Algoritma asimetris.....	20
Gambar 2.4 Skema Komunikasi Kriptografi	30
Gambar 2.5 Skema Komunikasi Kunci Publik	31
Gambar 2.6 Skema Algoritma kriptografi Hybrid metode pertukaran kunci....	37
Gambar 2.7 Skema algoritma kriptografi Hybrid dua tingkatan kunci.....	37
Gambar 2.8 Keyword Pemrograman Java	48
Gambar 2.9 Tipe data 1 Java.....	51
Gambar 2.10 Tipe data 2 Java.....	51
Gambar 2.11 Bagan kerangka berfikir	53
Gambar 3.1 Skema Kriptografi Hill Cipher.....	56
Gambar 3.2 Skema Algoritma Kriptografi ElGamal.....	57
Gambar 3.3. Skema Algoritma Kriptografi Hybrid pengamanan Kunci dan tingkatan dua kunci	58
Gambar 3.4 Rancangan Homepage.....	60
Gambar 3.5 Rancangan Tampilan Cek Bilangan Prima.....	61
Gambar 3.6 Rancangan Tampilan Generate Kunci	61
Gambar 3.7 Rancangan Tampilan Menu enkripsi Hill cipher.....	62
Gambar 3.8 Rancangan Tampilan Menu dekripsi Hill cipher.....	62
Gambar 3.9 Rancangan Tampilan Menu enkripsi Elgamal.....	63
Gambar 3.10 Rancangan Tampilan Menu dekripsi Elgamal.....	63

Gambar	Halaman
Gambar 3.11 Rancangan Tampilan Menu enkripsi hybrid.....	64
Gambar 3.12 Rancangan Tampilan Menu dekripsi hybrid	64
Gambar 4.1 Diagram alir Pembangkit kunci.....	69
Gambar 4.2 Diagram alir enkripsi hybrid bagian Hill cipher	70
Gambar 4.3 Diagram alir enkripsi hybrid bagian kriptografi ElGamal	71
Gambar 4.4 Diagram Alir Dekripsi Hybrid bagian Kriptografi ElGamal.....	72
Gambar 4.5 Diagram Alir Dekripsi Hybrid bagian Kriptografi Hill cipher.....	73
Gambar 4.6 HomePage aplikasi program aplikasi Kriptografi Hybrid.....	74
Gambar 4.7 Menu Mengecek Bilangan Prima.....	75
Gambar 4.8 Menu Hill Cipher Tab Enkripsi	76
Gambar 4.9 Menu Hill Cipher Tab Dekripsi.....	77
Gambar 4.10 Menu ElGamal Tab Enkripsi.....	78
Gambar 4.11 Menu ElGamal Tab Dekripsi.....	78
Gambar 4.12 Menu Hybrid Tab Enkripsi.....	79
Gambar 4.13 Menu Hybrid Tab Dekripsi.....	80
Gambar 4.14 Pengecekan Bilangan prima	81
Gambar 4.15 Pembangkitan kunci dengan $p = 257$	82
Gambar 4.16 Enkripsi hybrid dengan Program Aplikasi	83
Gambar 4.17 Sesion Key (bilangan acak k) enkripsi teks dari Program Aplikasi Hybrid.....	88
Gambar 4.18 Source code java pengecekan kesamaan ciphertext.....	91

Gambar	Halaman
Gambar 4.19 Output Pengecekan ciphertext melalui program aplikasi dan perhitungan manual	91
Gambar 4.20 Dekripsi dengan menggunakan program aplikasi Hybrid.....	93
Gambar 4.21 Pengecekan nilai b, b = 1..64	98
Gambar 4.22 Pengecekan nilai b, b=64..128	99
Gambar 4.23 Pengecekan nilai b, b =129..192	99
Gambar 4.24 Pengecekan nilai b, b =192..255	100
Gambar 4.25. rata – rata waktu enkripsi ketiga metode.....	113
Gambar 4.26 Grafik rata-rata waktu dekripsi	122
Gambar 4.27 Grafik rata – rata nilai entropi dari ketiga metode	127



DAFTAR LAMPIRAN

Lampiran	Halaman
Lampiran 1. Kode ASCII - 256 Character (American Standard Code for Information Interchange)	136
Lampiran 2. Tampilan JAVA NetBeans18	137
Lampiran 3. Source Code HomePage.java	138
Lampiran 4. Source Code Cek_bil_Prim.java	139
Lampiran 5. Source Code enkripsi Pembangkit_kunci.java	140
Lampiran 6. Source Code dekripsi Hillcipher12.java	141
Lampiran 7. Source Code dekripsi Hillcipher12.java	144
Lampiran 8. Source Code Enkripsi ElGamal.java	148
Lampiran 9. Source Code Dekripsi ElGamal.java	149
Lampiran 10. Source Code Enkripsi Hybrid.java	150
Lampiran 11. Source Code Dekripsi Hybrid.java	153
Lampiran 12. Source Code Menghitung Nilai Entropi	156
Lampiran 13. Source Code Memeriksa Kesamaan Ciphertext Menggunakan Aplikasi dan Perhitungan Manual	157
Lampiran 14. Riwayat Hidup	158