

**ANALISIS KEAMANAN PESAN TERSANDI
MENGUNAKAN KOMBINASI *HILL CIPHER* DAN
CIPHER SUBSTITUSI DENGAN KOSET**

Skripsi

**Disusun untuk memenuhi salah satu syarat
memperoleh gelar Sarjana Matematika**



Khalda Nur Khairun Nisa

1305621027

**PROGRAM STUDI MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS NEGERI JAKARTA**

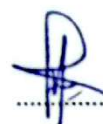
2025

LEMBAR PERSETUJUAN HASIL SIDANG SKRIPSI

ANALISIS KEAMANAN PESAN TERSANDI MENGGUNAKAN KOMBINASI *HILL CIPHER* DAN CIPHER SUBSTITUSI DENGAN KOSET

Nama : Khalda Nur Khairun Nisa

No. Registrasi : 1305621027

	Nama	Tanda Tangan	Tanggal
Penanggung Jawab Dekan	: <u>Dr. Hadi Nasbey, S.Pd., M.Si.</u> NIP. 197909162005011004		30/07/2025
Wakil Penanggung Jawab Dekan I	: <u>Dr. Meiliasari, S.Pd., M.Sc.</u> NIP. 197905042009122002		30/07/2025
Ketua	: <u>Dr. Yudi Mahatma, M.Si.</u> NIP. 197610202008121001		21/07/2025
Sekretaris	: <u>Dr. Eti Dwi Wiraningsih, S.Pd., M.Si.</u> NIP. 198102032006042001		22/07/2025
Penguji Ahli	: <u>Med Irzal, M.Kom.</u> NIP. 197706152003121001		21/07/2025
Pembimbing I	: <u>Ibnu Hadi, M.Si.</u> NIP. 198107182008011017		23/07/2025
Pembimbing II	: <u>Dr. Lukita Ambarwati, S.Pd., M.Si.</u> NIP. 197210262001122001		23/07/2025

Dinyatakan lulus ujian skripsi tanggal 14 Juli 2025

SURAT PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini, mahasiswa Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta:

Nama : Khalda Nur Khairun Nisa
No Registrasi : 1305621027
Program Studi : Matematika

Dengan ini menyatakan bahwa skripsi yang saya buat dengan judul *"Analisis Keamanan Pesan Tersandi Menggunakan Kombinasi Hill Cipher dan Cipher Substitusi dengan Koset"* adalah:

1. Dibuat sendiri, mengadopsi hasil kuliah, buku-buku, dan referensi acuan yang tertera di dalam referensi pada skripsi saya.
2. Bukan merupakan hasil duplikasi skripsi yang telah dipublikasikan atau pernah dipakai untuk mendapatkan gelar sarjana di Universitas lain kecuali pada bagian-bagian sumber informasi dicantumkan berdasarkan tata cara referensi yang semestinya.

Pernyataan ini dibuat dengan sesungguhnya dan saya bersedia menanggung segala akibat yang timbul jika pernyataan saya tidak benar.

Jakarta, 1 Juli 2025



Khalda Nur Khairun Nisa



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS NEGERI JAKARTA
UPT PERPUSTAKAAN

Jalan Rawamangun Muka Jakarta 13220
Telepon/Faksimili: 021-4894221
Laman: lib.unj.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Negeri Jakarta, yang bertanda tangan di bawah ini, saya:

Nama : Khalda Nur Khairun Nisa
NIM : 1305621027
Fakultas/Prodi : FMIPA / Matematika
Alamat email : khaldankn@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada UPT Perpustakaan Universitas Negeri Jakarta, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah:

☒ Skripsi ☐ Tesis ☐ Disertasi ☐ Lain-lain (.....)

yang berjudul :

Analisis Keamanan Pesan Tersandi Menggunakan Kombinasi Hill Cipher
dan Cipher Substitusi dengan Forest

Dengan Hak Bebas Royalti Non-Eksklusif ini UPT Perpustakaan Universitas Negeri Jakarta berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya, dan menampilkan/mempublikasikannya di internet atau media lain secara *fulltext* untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan Universitas Negeri Jakarta, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta

Penulis

(Khalda Nur Khairun Nisa)
nama dan tanda tangan

KATA PENGANTAR

Alhamdulillah rabbil 'alamin. Puji syukur kehadiran Allah SWT yang telah memberikan rahmat serta nikmat-Nya sehingga penulis dapat menyelesaikan skripsi ini sebagai salah satu syarat dan tugas akhir memperoleh gelar Sarjana Matematika selama studi di Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam dengan judul "Analisis Keamanan Pesan Tersandi Menggunakan Kombinasi *Hill Cipher* dan *Cipher Substitusi* dengan Koset".

Penulis menyadari bahwa penulisan skripsi ini tidak akan selesai tanpa adanya bantuan dari beberapa pihak. Pada kesempatan ini penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak Ibnu Hadi, M.Si. selaku dosen pembimbing I yang telah dengan sabar membimbing, memberikan dukungan, serta memotivasi penulis selama proses penyusunan skripsi sehingga skripsi ini dapat diselesaikan dengan baik.
2. Ibu Dr. Lukita Ambarwati, S.Pd., M.Si. selaku dosen pembimbing II yang telah dengan sabar membimbing, memberikan dukungan, serta memotivasi penulis selama proses penyusunan skripsi sehingga skripsi ini dapat diselesaikan dengan baik.
3. Ibu Devi Eka Wardani Meganingtyas, S.Pd., M.Si. selaku dosen pembimbing akademik yang telah memberikan bimbingan dan arahan selama masa perkuliahan.
4. Bapak Dr. Yudi Mahatma, M.Si. selaku Koordinator Program Studi Matematika yang telah memberikan bimbingan, dukungan, serta kemudahan dalam berbagai proses administratif selama masa perkuliahan.
5. Bapak dan Ibu Dosen Program Studi Matematika yang telah memberikan ilmu dan bimbingan selama masa perkuliahan.

6. Kedua orang tua, serta kakak dan adik penulis yang telah memberikan dukungan, doa, motivasi, dan selalu menghibur serta memberikan semangat di saat-saat sulit.

7. Teman-teman Matematika angkatan 2021 yang telah kebersamai dan mewarnai perjalanan perkuliahan ini. Terima kasih atas kebersamaan yang hangat, semangat yang diberikan, bantuan di kala sulit, dan tawa yang menjadi pelipur penat.

8. Khalda Nur Khairun Nisa. Terima kasih kepada diri sendiri yang telah bertahan di tengah berbagai ujian yang datang. Terima kasih karena sudah mau terus berjuang dan tetap mempertahankan semangat untuk terus melangkah ke depan.

Penulis menyadari bahwa masih terdapat kekurangan dan kesalahan dalam penulisan skripsi ini disebabkan kurangnya ilmu dan wawasan. Oleh karena itu penulis mengharapkan kritik dan saran yang membangun sehingga dapat menjadi lebih baik lagi.

Semoga skripsi ini dapat memberikan manfaat bagi lingkungan akademik khususnya Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta, maupun pihak lain yang membutuhkan.

Jakarta, 1 Juli 2025

Intelligentia - Dignitas

Khalda Nur Khairun Nisa

ABSTRAK

KHALDA NUR KHAIRUN NISA. Analisis Keamanan Pesan Tersandi Menggunakan Kombinasi *Hill Cipher* dan Cipher Substitusi dengan Koset. Skripsi, Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta. Juli 2025.

Tingginya kasus kejahatan siber dan kurangnya tenaga profesional keamanan siber di Indonesia menjadikan kriptografi penting untuk dipahami. *Hill Cipher* adalah algoritma kriptografi klasik jenis cipher substitusi yang menggunakan matriks transformasi pada proses enkripsi dan dekripsinya. *Hill Cipher* memiliki kelemahan dalam analisis frekuensi bigram dan trigram karena blok plainteks yang sama menghasilkan blok cipherteks yang sama. Cipher substitusi dengan koset adalah kriptografi klasik yang pemetaan-nya *one to many* dengan mengaplikasikan konsep koset dalam algoritmanya untuk menyembunyikan hubungan statistik antara plainteks dengan cipherteks. Pada penelitian ini dilakukan kombinasi antara *Hill Cipher* dan cipher substitusi dengan koset. Tujuan dari penelitian ini adalah untuk menganalisis keamanan pesan tersandi menggunakan kombinasi *Hill Cipher* dan cipher substitusi dengan koset. Metode penelitian yang digunakan adalah studi literatur disertai implementasi dengan plainteks dan kunci tertentu. Hasil penelitian menunjukkan bahwa hasil kombinasi dua algoritma ini dapat mengatasi kelemahan *Hill Cipher* dalam analisis frekuensi bigram dan trigram, meningkatkan nilai *Shannon entropy* pada analisis frekuensi bigram dan trigram, serta meningkatkan nilai *min-entropy* pada analisis frekuensi trigram. Namun, pada analisis frekuensi bigram tidak menghasilkan nilai *min-entropy* yang lebih tinggi dari cipher substitusi dengan koset. Dari hasil percobaan didapatkan bahwa perbedaan urutan kombinasi algoritma menghasilkan pesan tersandi yang berbeda namun hasil uji statistik mengungkapkan bahwa perbedaan urutan kombinasi algoritma tidak berpengaruh secara signifikan terhadap tingkat keamanan pesan tersandi.

Kata kunci. Kriptografi, Analisis Keamanan, Analisis Frekuensi, Shannon Entropy, Min-Entropy

Intelligentia - Dignitas

ABSTRACT

KHALDA NUR KHAIRUN NISA. Security Analysis of Encrypted Messages Using a Combination of the Hill Cipher and Substitution Cipher with Cosets. Mini Thesis, Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Negeri Jakarta. July 2025.

The increasing number of cybercrime cases and the shortage of cybersecurity professionals in Indonesia highlight the importance of understanding cryptography. Hill Cipher is a classical cryptographic algorithm of the substitution cipher type that utilizes a transformation matrix in both its encryption and decryption processes. However, Hill Cipher has a weakness in bigram and trigram frequency analysis, as identical plaintext blocks produce identical ciphertext blocks. The coset-based substitution cipher is a classical cryptographic method that employs a one-to-many mapping by applying the concept of cosets in its algorithm to obscure the statistical patterns between plaintext and ciphertext. Therefore, this research proposes a combination of the Hill Cipher and the coset-based substitution cipher. The aim of this research is to analyze the security of encrypted messages using the combination of Hill Cipher and the coset-based substitution cipher. The research method involves a literature review and implementation using specific plaintext and keys. The results indicate that the proposed combination successfully mitigates the Hill Cipher's weaknesses in bigram and trigram frequency analysis, increases the Shannon entropy value in both bigram and trigram frequency analysis, and improves min-entropy value in trigram frequency analysis. However, in the bigram frequency analysis, the min-entropy value is not higher than that of the coset-based substitution cipher alone. Moreover, although different algorithmic orderings result in distinct ciphertexts, statistical analysis indicates that the ordering of the combination does not have a statistically significant impact on the security of the encrypted messages.

Keyword. *Cryptography, Security Analysis, Frequency Analysis, Shannon Entropy, Min-Entropy*

Intelligentia - Dignitas

DAFTAR ISI

LEMBAR PERSETUJUAN HASIL SIDANG SKRIPSI	i
LEMBAR PERNYATAAN	i
KATA PENGANTAR	i
ABSTRAK	iii
ABSTRACT	iv
DAFTAR ISI	v
DAFTAR TABEL	viii
DAFTAR GAMBAR	ix
DAFTAR LAMPIRAN	x
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	4
1.3 Batasan Masalah	5
1.4 Tujuan Penelitian	6
1.5 Manfaat Penelitian	6
BAB 2 KAJIAN PUSTAKA	7
2.1 Konsep Matematika yang Digunakan dalam Algoritma	7
2.1.1 Teori Bilangan	7
2.1.2 Teori Grup	13

2.1.3	Matriks	17
2.2	Kriptografi	21
2.2.1	Definisi Kriptografi	21
2.2.2	Terminologi dalam Kriptografi	22
2.2.3	Kriptografi Klasik	23
2.3	Kode ASCII	27
2.4	<i>Hill Cipher</i>	28
2.4.1	Pembentukan Kunci <i>Hill Cipher</i>	28
2.4.2	Enkripsi <i>Hill Cipher</i>	31
2.4.3	Dekripsi <i>Hill Cipher</i>	33
2.4.4	Contoh <i>Hill Cipher</i>	35
2.5	Cipher Substitusi dengan Koset	49
2.5.1	Enkripsi Cipher Substitusi dengan Koset	49
2.5.2	Dekripsi Cipher Substitusi dengan Koset	52
2.5.3	Contoh Cipher Substitusi dengan Koset	54
2.6	Analisis Keamanan pada Kriptografi	58
2.6.1	Analisis Frekuensi	58
2.6.2	Diagram Sebaran Frekuensi	59
2.6.3	<i>Shannon Entropy</i>	60
2.6.4	<i>Min-Entropy</i>	62
2.6.5	Analisis Keamanan <i>Hill Cipher</i>	63
2.6.6	Analisis Keamanan Cipher Substitusi dengan Koset	69
2.6.7	Uji Mann-Whitney U	76
BAB 3	METODOLOGI PENELITIAN	78
3.1	Metode Penelitian	78
3.2	Diagram Alir Penelitian	79
BAB 4	HASIL DAN PEMBAHASAN	80
4.1	Menentukan Plainteks	80
4.2	Menentukan Kunci	80
4.2.1	Pembentukan Kunci <i>Hill Cipher</i>	81

4.2.2	Menentukan Kunci Cipher Substitusi dengan Koset . . .	84
4.3	Analisis Keamanan <i>Hill Cipher</i>	85
4.3.1	Analisis Frekuensi Bigram	85
4.3.2	Analisis Frekuensi Trigram	87
4.4	Analisis Keamanan Cipher Substitusi dengan Koset	89
4.4.1	Analisis Frekuensi Bigram	91
4.4.2	Analisis Frekuensi Trigram	91
4.5	Analisis Keamanan Kombinasi Algoritma <i>Hill Cipher</i> Dilan- jutkan dengan Cipher Substitusi dengan Koset	92
4.5.1	Analisis Frekuensi Bigram	93
4.5.2	Analisis Frekuensi Trigram	95
4.6	Analisis Keamanan Kombinasi Algoritma Cipher Substitusi dengan Koset Dilanjutkan dengan <i>Hill Cipher</i>	98
4.6.1	Analisis Frekuensi Bigram	98
4.6.2	Analisis Frekuensi Trigram	100
4.7	Pengaruh Urutan Kombinasi terhadap Hasil Analisis Keamanan	103
4.7.1	Pengujian Statistik	103
4.7.2	Interpretasi	106
BAB 5	KESIMPULAN DAN SARAN	107
5.1	Kesimpulan	107
5.2	Saran	108
	DAFTAR PUSTAKA	110
	LAMPIRAN	113
	RIWAYAT HIDUP	183

DAFTAR TABEL

Tabel 4.1	Hasil Analisis Frekuensi Bigram	91
Tabel 4.2	Hasil Analisis Frekuensi Trigram	92
Tabel 4.3	Hasil Analisis Frekuensi Bigram	95
Tabel 4.4	Hasil Analisis Frekuensi Trigram	97
Tabel 4.5	Hasil Analisis Frekuensi Bigram	100
Tabel 4.6	Hasil Analisis Frekuensi Trigram	102
Tabel 4.7	Hasil Perhitungan Nilai Keamanan untuk Analisis Frekuensi Bigram	104
Tabel 4.8	Hasil Perhitungan Nilai Keamanan untuk Analisis Frekuensi Trigram	105
Tabel 5.1	Hasil Analisis Keamanan Pesan Tersandi	107

Intelligentia - Dignitas

DAFTAR GAMBAR

Gambar 2.1	Contoh Tabel Homofon	26
Gambar 2.2	Tabel ASCII (<i>Compact</i>)	27
Gambar 2.3	Diagram alur enkripsi <i>Hill Cipher</i>	32
Gambar 2.4	Diagram alur dekripsi <i>Hill Cipher</i>	34
Gambar 2.5	Diagram alur enkripsi cipher substitusi dengan koset .	51
Gambar 2.6	Diagram alur dekripsi cipher substitusi dengan koset	53
Gambar 2.7	Contoh diagram sebaran frekuensi huruf (unigram) .	60
Gambar 2.8	Contoh diagram sebaran frekuensi bigram	60
Gambar 2.9	Sebaran frekuensi huruf pada plainteks	64
Gambar 2.10	Sebaran frekuensi huruf pada cipherteks	64
Gambar 2.11	Sebaran frekuensi bigram pada plainteks	67
Gambar 2.12	Sebaran frekuensi bigram pada cipherteks	67
Gambar 2.13	Sebaran frekuensi huruf pada plainteks	70
Gambar 2.14	Sebaran frekuensi huruf pada cipherteks	70
Gambar 2.15	Sebaran frekuensi bigram pada plainteks	73
Gambar 2.16	Sebaran frekuensi bigram pada cipherteks	73
Gambar 3.1	Diagram Alir Penelitian	79

Intelligentia - Dignitas

DAFTAR LAMPIRAN

Lampiran 1. Enkripsi dan Dekripsi Hill Cipher dengan kunci berukuran 2x2	113
Lampiran 2. Enkripsi dan Dekripsi Hill Cipher dengan kunci berukuran 3x3	119
Lampiran 3. Enkripsi dan Dekripsi Cipher Substitusi dengan Koset ..	125
Lampiran 4. Cipherteks Cipher Substitusi dengan Koset Percobaan ke-2	130
Lampiran 5. Cipherteks Cipher Substitusi dengan Koset Percobaan ke-3	130
Lampiran 6. Cipherteks Cipher Substitusi dengan Koset Percobaan ke-4	131
Lampiran 7. Cipherteks Cipher Substitusi dengan Koset Percobaan ke-5	131
Lampiran 8. Enkripsi dan Dekripsi Hill-CSK dengan kunci K_{HC} berukuran 2x2	132
Lampiran 9. Cipherteks Hill-CSK dengan kunci K_{HC} berukuran 2x2 Percobaan ke-2	141
Lampiran 10. Cipherteks Hill-CSK dengan kunci K_{HC} berukuran 2x2 Percobaan ke-3	141
Lampiran 11. Cipherteks Hill-CSK dengan kunci K_{HC} berukuran 2x2 Percobaan ke-4	142
Lampiran 12. Cipherteks Hill-CSK dengan kunci K_{HC} berukuran 2x2 Percobaan ke-5	142
Lampiran 13. Enkripsi dan Dekripsi Hill-CSK dengan kunci K_{HC} berukuran 3x3	143
Lampiran 14. Cipherteks Hill-CSK dengan kunci K_{HC} berukuran 3x3 Percobaan ke-2	153
Lampiran 15. Cipherteks Hill-CSK dengan kunci K_{HC} berukuran 3x3	

Percobaan ke-3	153
Lampiran 16. Cipherteks Hill-CSK dengan kunci K_{HC} berukuran 3x3	
Percobaan ke-4	154
Lampiran 17. Cipherteks Hill-CSK dengan kunci K_{HC} berukuran 3x3	
Percobaan ke-5	154
Lampiran 18. Enkripsi dan Dekripsi CSK-Hill dengan kunci K_{HC}	
berukuran 2x2	155
Lampiran 19. Cipherteks CSK-Hill dengan kunci K_{HC} berukuran 2x2	
Percobaan ke-2	165
Lampiran 20. Cipherteks CSK-Hill dengan kunci K_{HC} berukuran 2x2	
Percobaan ke-3	165
Lampiran 21. Cipherteks CSK-Hill dengan kunci K_{HC} berukuran 2x2	
Percobaan ke-4	166
Lampiran 22. Cipherteks CSK-Hill dengan kunci K_{HC} berukuran 2x2	
Percobaan ke-5	166
Lampiran 23. Enkripsi dan Dekripsi CSK-Hill dengan kunci K_{HC}	
berukuran 3x3	167
Lampiran 24. Cipherteks CSK-Hill dengan kunci K_{HC} berukuran 3x3	
Percobaan ke-2	177
Lampiran 25. Cipherteks CSK-Hill dengan kunci K_{HC} berukuran 3x3	
Percobaan ke-3	177
Lampiran 26. Cipherteks CSK-Hill dengan kunci K_{HC} berukuran 3x3	
Percobaan ke-4	178
Lampiran 27. Cipherteks CSK-Hill dengan kunci K_{HC} berukuran 3x3	
Percobaan ke-5	178
Lampiran 28. Analisis Frekuensi	179