ANALISIS KEAMANAN PESAN TERSANDI MENGGUNAKAN 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	: Dr. Hadi Nasbey, S.Pd., M.Si. NIP. 197909162005011004		30/07/2025
Wakil Penanggung Jawab Dekan I	: Dr. Meiliasari, S.Pd., M.Sc. NIP. 197905042009122002		30/07/2025
Ketua	: Dr. Yudi Mahatma, M.Si. NIP.197610202008121001		21/07/2025
Sekretaris	: Dr. Eti Dwi Wiraningsih, S.Pd., M.Si. NIP.198102032006042001		22/07/2025
Penguji Ahli	: Med Irzal, M.Kom. NIP.197706152003121001		21/07/2025
Pembimbing I	: Ibnu Hadi, M.Si. NIP.198107182008011017		23/07/2025
Pembimbing II	: Dr. Lukita Ambarwati, S.Pd., M.Si. 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 Koset

Dengan Hak Bebas Royalti Non-Ekslusif 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

Alhamdulillahi rabbil 'alamin. Puji syukur kehadirat 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 membersamai 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

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 pemetaannya *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*

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*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN