PENGEMBANGAN METODE ENKRIPSI DAN DESKRIPSI *HYBRID* MENGGUNAKAN ALGORITMA *HILL CIPHER* DENGAN MATRIKS $m \times n$ DAN ALGORITMA ELGAMAL

SKRIPSI

untuk memenuhi persyaratan
dalam menyelesaikan program sarjana Strata-1 Matematika

Oleh:
Siti Rosyidah Fadinah
NIM. 2111011320017

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMBUNG MANGKURAT
BANJARBARU
2026

SKRIPSI

Pengembangan Metode Enkripsi dan Deskripsi menggunakan Algoritma *Hill cipher* dengan Matriks $m \times n$ dan Algoritma ElGamal

Oleh:
Siti Rosyidah Fadinah
2111011320017

telah dipertahankan di depan Dosen Penguji pada tanggal 21 Januari 2026
Susunan Dosen Penguji:

Pembimbing I

Thresye, S.Si M.Si
NIP 197205042000122002

Pembimbing II

Hermei Lissa, S.Pd., M.Si
NIP 199005222022032012

Dosen Penguji:
1. **Saman Abdurrahman, S.Si., M.Sc (**)
2. **Oni Soesanto, S.Si., M.Si (**)

Banjarbaru, 29 Januari 2026
Jurusan Matematika FMIPA ULM
Ketua,

Dr. Na'imah Hijriati, S.Si., M.Si
NIP 197911222008012013

PERNYATAAN

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memeproleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Pustaka.

Banjarbaru, 28 Januari 20226

Siti Rosyidah Fadinah
NIM. 2111011320017

ABSTRAK

PENGEMBANGAN METODE ENKRIPSI DAN DESKRIPSI *HYBRID* MENGGUNAKAN ALGORITMA *HILL CIPHER* DENGAN MATRIKS $m \times n$ DAN ALGORITMA ELGAMAL

(Oleh: Siti Rosyidah Fadinah; Pembimbing: Thresye, Hermei Lissa, 2025; 79 Halaman)

Kriptografi merupakan ilmu tentang sistem kerahasiaan, yang mencakup kriptografi (desain dan implementasi sistem sandi) dan kriptanalisis (menganalisis dan memecahkan sandi). Algoritma *Hill cipher* menggunakan perkalian matriks untuk proses enkripsi dan mencari *invers* matriks untuk melakukan deskripsi. Algoritma ElGamal menghasilkan kunci publik (p, g, y) digunakan untuk enkripsi (*ciphertext)* dan kunci privat (x) untuk deskripsi (*plaintext)*. Pada penelitian ini bertujuan mengembangkan metode Enkripsi menggunakan Algoritma *Hill cipher* dengan matriks persegi panjang $(m \times n)$, dan Algoritma ElGamal. Enkripsi adalah mengubah *plaintext* menjadi *ciphertext* yang tidak dapat dibaca, sebaliknya deskripsi mengubah *ciphertext* kembali menjadi *plaintext* yaitu bentuk aslinya. Proses penelitian ini dengan metode algoritma *hybrid* yaitu melakukan dua kali proses enkripsi dan deskripsi dimulai dengan algoritma *Hill cipher* dan dilanjutkan menggunakan algoritma ElGamal maka dari hasil penelitian ini menunjukkan bahwa penggunaan kunci matriks persegi panjang dapat menyamarkan pesan karena *ciphertext* yang dihasilkan lebih panjang dibandingkan *plaintext* yang diberikan. Matriks kunci yang dibentuk merupakan matriks yang memiliki Invers Moore-Penrose yang digunakan pada proses deskripsi, dan Algoritma ElGamal bergantung pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah algoritma ini menjadi sulit untuk dipecahkan. Gabungan kedua metode dalam pendekatan hybrid menghasilkan tingkat keamanan yang lebih tinggi, karena memadukan keunggulan Hill cipher dalam pengolahan blok teks dengan kekuatan ElGamal dalam menjaga kerahasiaan melalui sistem kunci publik.

Kata kunci: *Hybrid*, Enkripsi, Deskripsi, *Hill cipher*, ElGamal, Invers Moore-Penrose

ABSTRACT

DEVELOPMENT OF A HYBRID ENCRYPTION AND DECRYPTION METHOD USING THE HILL CIPHER ALGORITHM WITH MATRICES $m \times n$ AND THE ELGAMAL ALGORITHM

(By: Siti Rosyidah Fadinah; Supervisors: Thresye, Hermei Lissa, 2025; 79 Pages)

Cryptography is the science of secrecy systems, which includes cryptography (the design and implementation of ciphers) and cryptanalysis (analyzing and breaking ciphers). The hill cipher algorithm uses matrix multiplication for the encryption process and matrix inversion for decryption. The ElGamal algorithm generates a public key (p,g,y) for encryption (ciphertext) and a private key (x) for decryption (plaintext). This study aims to develop an encryption method using the Hill cipher algorithm with a rectangular matrix $m \times n$ and the ElGamal algorithm. Encryption is the proses of converting plaintext into unreadable ciphertext, while decryption convest ciphertext back into plaintext, its original form. The research process employs a hybrid algorithm method, performing two stage of encryption and descryption starting with the Hill cipher algorithm and countinuing with the algorithm. The result show that the use of a rectangular key matrix can obscure the message since the generated ciphertext is longer than the given plaintext. The key matrix constructed is one that has a Moore-Penrose invers, wich is used in the decryption process. Meanwhile, the ElGamal algorithm relies on the difficulty of solving the discrete logarithm problem in a large prime modulus, making it computationally hard to break. The combination of both methods in a hybrid approach results in a higher level of security, as it integrates the advantages of the Hill cipher in processing text blocks with the strength of the ElGamal algorithm in maintaining confidentiality through a public key system.

Keywords: Hybrid, Encryption, Descyption, Hill cipher, ElGamal, Moore–Penrose inverse

KATA PENGANTAR

Alhamdulillahirabbil'alamin, puji syukur ke hadirat Allah subhanahu wa ta'ala yang telah memberikan kemudahan bagi penulis, puji syukur penulis panjatkan kehadirat Allah subhanahu wa ta'ala atas segala berkat, rahmat, hidayah, karunia, dan izin-Nya, serta shalawat dan salam tercurahkan kepada junjungan besar Nabi Muhammad shalallahu 'alaihi wasallam beserta para keluarga, sahabat serta pengikut hingga akhir zaman sehingga penulis dapat menyelesaikan skripsi yang berjudul "Pengembangan Metode Enkripsi dan deskripsi *hybrid* menggunakan algoritma *Hill cipher* dengan matriks $m \times n$ dan algoritma Elgamal" dengan baik. Penyusunan skripsi ini bertujuan untuk memenuhi salah satu persyaratan dalam menyelesaikan program Strata-1 Matematika di Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat. Proses penyusunan skripsi ini tidak terlepas dari dukungan, doa, kerja sama, bimbingan, dan bantuan dari berbagai pihak. Selesainya penulisan skripsi ini penulis persembahkan kepada orang tua, keluarga tercinta, dan teman-teman yang penulis banggakan. Pada kesempatan ini juga, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Drs. Abdul Gafur, M.Si., M.Sc., Ph.D selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
2. Ibu Dr. Na'imah Hijriati, S.Si., M.Si selaku Koordinator Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
3. Ibu Thresye S.Si., M.Si., dan Ibu Hermei Lissa S.Pd., M.Si selaku dosen pembimbing yang telah mendampingi dan membimbing dalam penyusunan skripsi ini dari awal sampai akhir.
4. Bapak Saman Abdurrahman, S.Si., M.Sc selaku dosen penguji 1 dan Bapak Oni Soesanto, S.Si., M.Si selaku penguji 2 yang telah memberikan masukan untuk perbaikan dalam penyusunan skripsi ini.
5. Bapak Akhmad Yusuf S.Si., M.Kom selaku dosen penasehat akademik tahun 2021-2024 dan Ibu Hermei Lissa S.Pd., M.Si selaku dosen penasehat akademik tahun 2025-sekarang yang telah memberikan arahan dan bimbingan selama perkuliahan.
6. Bapak dan Ibu Dosen dan Staf Jurusan Matematika yang sudah memberikan ilmunya, memberikan arahan dan bantuan dalam hal kelengkapan adminitrasi dalam *rank*a penyusunan skripsi ini Bapak, Ibu, dan saudara-saudara saya serta keluarga dirumah, karena tanpa dukungan dan motivasi dari mereka saya mungkin tidak dapat menyelesaikan penelitian ini.
7. Kak zulaikah, Nahda, Diba, dan Maulidah yang telah banyak membantu dalam memahami, memberi motivasi, dukungan dan bantuan lainnya yang dibutuhkan dalam penelitian ini.

8. Seluruh teman saya (Ian, Putri, Elma, Helda, Puspa, Elfa, Dedew, Wafiq, NJ, Icha, Uswa, Dwi, Santi, WG, Putsyif, Suci, Asna, Ndut, Lita), dan rekan mahasiswa yang telah banyak memberikan bantuan, semangat, bimbingan, dan kerja sama dalam menyelesaikan penyusunan skripsi ini.
9. Dan banyak pihak yang tidak dapat penulis sebut satu persatu.

Penulis menyadari dalam penulisan dan penyusunan skripsi ini masih jauh dari kata sempurna, masih terdapat kekurangan baik dalam penulisan maupun dalam pembahasan materi. Oleh karena itu, kritik dan saran yang membangun akan senantiasa penulis harapkan demi kesempurnaan dimasa yang akan datang. Semoga skripsi ini dapat memberikan sumbangan yang bermanfaat bagi semua pihak.

Banjarbaru, 28 Januari 20226

Siti Rosyidah Fadinah
NIM. 2111011320017

DAFTAR ISI

DAFTAR TABEL

ARTI LAMBANG DAN SINGKATAN

$A^{\dagger}$: Invers Moore-Penrose dari matriks A

$a \bmod m$: sisa dari a dibagi oleh m

$a \equiv b \pmod m$: a kongruen b modulo m

$a|b$: a membegi b

$a \nmid b$: a tidak membagi b

C : enkripsi dari *plaintext* P

P : deskripsi dari *ciphertext* C

$rank\ (A)$: *rank* dari matriks A

■ : terbukti

I : matriks identitas

A^{*} : konjugat transpose dari matriks A

φ : phi euler

(a, b) : FPB dari a dan b

$ord_n r$: bilangan bulat r orde modulo n

A^{-1} : invers dari matriks A

A^{T} : transpose dari matriks A