ANALISIS TINGKAT KEAMANAN SANDI HILL CIPHER, RIVEST-SHAMIR-ADLEMAN (RSA), DAN ELGAMAL TERHADAP *BRUTE FORCE ATTACK*

SKRIPSI

Disusun untuk memenuhi salah satu syarat

memperoleh gelar Sarjana Matematika

Andi Tabina Maggusila Zain

1305622056

PROGRAM STUDI MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS NEGERI JAKARTA

2026

LEMBAR PERSETUJUAN HASIL SIDANG SKRIPSI

ANALISIS PERBANDINGAN TINGKAT KEAMANAN ALGORITMA HILL CIPHER, RSA (RIVEST–SHAMIR–ADLEMAN), DAN ELGAMAL TERHADAP *BRUTE FORCE ATTACK*

Nama : **Andi Tabina Maggusila Zain**

NIM : **1305622056**

		Nama	Tanda Tangan	Tanggal
Penanggung Jawab				
Dekan	:	Dr. Hadi Nasbey, S.Pd., M.Si. NIP. 197909162005011004		3 Juni 2026
Wakil Penanggung Jawab				
Wakil Dekan I	:	Dr. Meiliasari, S.Pd., M.Sc. NIP. 197905042009122002		2 Juni 2026
Ketua	:	Dr. Eti Dwi Wiraningsih, S.Pd., M.Si. NIP. 198102032006042001		18 Mei 2026
Penguji Ahli	:	Drs. Sudarwanto, M.Si., DEA. NIP. 196503251993031003		21 Mei 2026
Sekretaris	:	Dr. Yudi Mahatma, M.Si. NIP. 197610202008121001		18 Mei 2026
Pembimbing I	:	Ibnu Hadi, M.Si. NIP. 198107182008011017		21 Mei 2026
Pembimbing II	:	Devi Eka Wardani M., S.Pd., M.Si. NIP. 199005162019032014		22 Mei 2026

Dinyatakan lulus ujian skripsi pada tanggal: 28 April 2026

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	:	Andi Tabina Maggusila Zain
No Registrasi	:	1305622056
Program Studi	:	Matematika

Dengan ini menyatakan bahwa skripsi yang saya buat dengan judul ***"Analisis Tingkat Keamanan Sandi Hill Cipher, Rivest–Shamir–Adleman (RSA), dan ElGamal terhadap Brute Force Attack"*** 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, 21 April 2026

Andi Tabina Maggusila Z.

KEMENTERIAN PENDIDIKAN TINGGI, SAINS DAN TEKNOLOGI
UNIVERSITAS NEGERI JAKARTA
PERPUSTAKAAN DAN KEARSIPAN

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 : Andi Tabina Maggusila Zain
NIM : 1305622056
Fakultas/Prodi : FMIPA / Matematika
Alamat email : Aanditamz@gmail.com

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

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

yang berjudul :

ANALISIS TINGKAT KEAMANAN SANDI HILL CIPHER, RIVEST-SHAMIR-ADLEMAN (RSA), DAN ELGAMAL TERHADAP BRUTE FORCE ATTACK

Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan dan Kearsipan 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, 3 Juni 2026

Penulis

(Andi Tabina M.Z.)
nama dan tanda tangan

ABSTRAK

ANDI TABINA MAGGUSILA ZAIN. Analisis Tingkat Keamanan Sandi Hill Cipher, Rivest–Shamir–Adleman (RSA), dan ElGamal terhadap *Brute Force Attack*. Skripsi, Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta. April 2026.

Perkembangan kriptografi menuntut adanya peningkatan keamanan, khususnya pada algoritma klasik yang relatif mudah diserang menggunakan metode *brute force attack*. Salah satu algoritma klasik yang masih banyak dikaji adalah Hill Cipher. Penelitian ini bertujuan untuk meningkatkan keamanan Hill Cipher dengan mengombinasikannya dengan algoritma kriptografi modern, yaitu RSA dan ElGamal, serta menganalisis tingkat keamanannya terhadap *brute force attack*. Metode yang digunakan dalam penelitian ini adalah dengan membentuk kombinasi dua algoritma (Hill–RSA dan Hill–ElGamal) serta kombinasi tiga algoritma (Hill–RSA–ElGamal dan Hill–ElGamal–RSA). Proses yang dilakukan meliputi enkripsi kunci Hill Cipher menggunakan algoritma RSA dan ElGamal, serta perhitungan waktu yang dibutuhkan untuk melakukan *brute force attack* berdasarkan jumlah kombinasi kunci yang terbentuk. Selain itu, penelitian ini juga mengimplementasikan program enkripsi dan dekripsi kombinasi algoritma yang dapat digunakan untuk menghasilkan *ciphertext*.

Hasil penelitian menunjukkan bahwa kombinasi dua algoritma menghasilkan waktu *brute force* sebesar $3{,}48 \times 10^8$ untuk Hill–RSA dan $3{,}46 \times 10^8$ untuk Hill–ElGamal. Sementara itu, kombinasi tiga algoritma menghasilkan waktu yang jauh lebih besar, yaitu $8{,}28 \times 10^{11}$ untuk kedua variasi urutan. Hal ini menunjukkan bahwa peningkatan jumlah kombinasi algoritma memperbesar ruang kunci secara signifikan. Penelitian ini menunjukkan bahwa semakin besar ruang kunci yang dihasilkan, yang dipengaruhi oleh ukuran bilangan pada RSA dan ElGamal, maka semakin lama waktu yang dibutuhkan untuk melakukan *brute force attack*, sehingga tingkat keamanan sistem kriptografi meningkat.

Kata kunci. Hill Cipher, RSA, ElGamal, *brute force*, kriptografi

ABSTRACT

ANDI TABINA MAGGUSILA ZAIN. Security Analysis of Hill Cipher, Rivest-Shamir-Adleman (RSA), and ElGamal Against *Brute Force Attack*. Undergraduate Thesis, Mathematics Study Program, Faculty of Mathematics and Natural Sciences, Universitas Negeri Jakarta. April 2026.

The development of cryptography requires enhanced security, especially for classical algorithms that are relatively vulnerable to *brute force* attacks. One of the classical algorithms that is still widely studied is the Hill Cipher. This research aims to improve the security of the Hill Cipher by combining it with modern cryptographic algorithms, namely RSA and ElGamal, and to analyze its resistance against *brute force attacks*. The method used in this research involves forming combinations of two algorithms (Hill–RSA and Hill–ElGamal) and combinations of three algorithms (Hill–RSA–ElGamal and Hill–ElGamal–RSA). The process includes encrypting the Hill Cipher key using RSA and ElGamal, as well as calculating the time required to perform a *brute force attack* based on the number of possible key combinations. In addition, an encryption and decryption program is implemented to generate *ciphertext* using the combined algorithms.

The results show that the combination of two algorithms produces *brute force* times of 3.48×10^8 for Hill–RSA and 3.46×10^8 for Hill–ElGamal. Meanwhile, the combination of three algorithms produces a significantly larger time of 8.28×10^{11} for both variations. This indicates that increasing the number of algorithm combinations significantly expands the key space. This research shows that a larger key space, influenced by the size of the numbers used in RSA and ElGamal, results in a longer time required for a *brute force attack*, thereby increasing the security level of the cryptographic system.

Keywords. Hill Cipher, RSA, ElGamal, *brute force*, cryptography

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT yang telah memberikan rahmat dan nikmat-Nya, sehingga penulis dapat menyelesaikan skripsi ini sebagai salah satu syarat untuk memperoleh gelar Sarjana Matematika di Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam. Skripsi ini dilaksanakan sejak September 2025 dengan judul "Analisis Tingkat Keamanan Sandi Hill Cipher, Rivest-Shamir-Adleman (RSA), dan ElGamal terhadap *Brute Force Attack*".

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

1. Bapak Ibnu Hadi, M.Si. selaku dosen pembimbing I yang telah memberikan bimbingan, arahan, serta motivasi kepada penulis selama penyusunan skripsi ini, sehingga penulis dapat memahami dan menyelesaikan penelitian dengan lebih baik dan terarah.

2. Ibu Devi Eka Wardani Meganingtyas, S.Pd., M.Si. selaku dosen pembimbing II yang telah memberikan arahan, masukan, dan berbagai ide yang sangat membantu penulis dalam mengembangkan penelitian ini sehingga skripsi dapat tersusun dengan lebih baik dan terarah.

3. Bapak dan Ibu dosen yang telah memberikan ilmu, pengalaman, dan bimbingan selama masa perkuliahan, yang menjadi bekal berharga bagi penulis dalam menyelesaikan skripsi maupun untuk masa depan.

4. Kedua orang tua serta seluruh keluarga penulis yang senantiasa memberikan kasih sayang, doa, dan dukungan tanpa henti. Dari merekalah penulis belajar arti kesabaran, keikhlasan, dan rasa syukur, sehingga penulis dapat menjalani dan menyelesaikan skripsi ini dengan baik.

5. Deby Febrianty, Grace Maria, dan Leni Marni, yang telah menjadi sahabat penulis selama masa perkuliahan. Bersama mereka, penulis melalui berbagai

kegiatan, seperti pelaksanaan magang, mengikuti lomba wirausaha kampus, serta menjelajahi berbagai tempat baru yang memberikan banyak pengalaman dan kenangan. Selain itu, mereka juga menjadi teman seperjuangan dalam proses penyusunan skripsi, di mana banyak waktu dihabiskan bersama untuk berdiskusi, belajar, dan mengerjakan tugas hingga larut malam.

6. Qoshirotu Thorfi Gibran Yusuf, yang kehadirannya menjadi salah satu penyemangat bagi penulis untuk terus berkembang. Terima kasih karena telah menjadi rekan seperjalanan dalam proses penyusunan skripsi, saling membagikan semangat untuk tetap menyelesaikan pengerjaan skripsi meskipun di tengah waktu libur, sehingga penulis dapat menyelesaikan skripsi ini dengan lebih cepat dan baik. Bersamanya, penulis mengenal berbagai hal dan hobi baru yang memberikan pengalaman berbeda selama masa perkuliahan. Semangatnya dalam menambah wawasan dan pengalaman baru juga menjadi motivasi bagi penulis untuk terus belajar dan berkembang.

Penulis menyadari bahwa masih terdapat kekurangan dan kesalahan dalam penulisan skripsi ini disebabkan kurangnya ilmu dan komunikasi. 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 serta bagi penulis secara pribadi.

Jakarta, 21 April 2026

Andi Tabina Maggusila Z.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR