KRIPTOGRAFI HIBRIDA MENGGUNAKAN ALGORITMA SIMETRIS *AUTOKEY CIPHER–AFFINE CIPHER* DAN ALGORITMA ASIMETRIS RSA UNTUK KEAMANAN DATA TEKS BESERTA ANALISIS KEAMANANNYA

Skripsi

Disusun untuk memenuhi salah satu syarat
memperoleh gelar Sarjana Matematika

Nina Niawati

1305621006

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

2026

LEMBAR PERSETUJUAN HASIL SIDANG SKRIPSI

Kriptografi Hibrida Menggunakan Algoritma Simetris *Autokey Cipher–Affine Cipher* dan Algoritma Asimetris RSA untuk Keamanan Data Teks Beserta Analisis Keamanannya

Nama : Nina Niawati

No. Registrasi : 1305621006

	Nama	Tanda Tangan	Tanggal
Penanggung Jawab Dekan	: Dr. Hadi Nasbey, S.Pd., M.Si. NIP. 197909162005011004		21/08/2026
Wakil Penanggung Jawab Wakil Dekan I	: Dr. Meiliasari, S.Pd., M.Sc. NIP. 197905042009122002		21/08/2026
Ketua	: Ibnu Hadi, M.Si. NIP.198107182008011017		13/08/2026
Sekretaris	: Dr. Yudi Mahatma, M.Si. NIP.197610202008121001		13/08/2026
Penguji Ahli	: Drs. Sudarwanto, M.Si., DEA NIP.196503251993031003		12/08/2026
Pembimbing I	: Dr. Lukita Ambarwati, S.Pd., M.Si. NIP. 197210262001122001		12/08/2026
Pembimbing II	: Devi Eka Wardani M, S.Pd., M.Si. NIP.199005162019032014		13/08/2026

Dinyatakan lulus ujian skripsi tanggal 29 Juli 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	:	Nina Niawati
No Registrasi	:	1305621006
Program Studi	:	Matematika

Dengan ini menyatakan bahwa skripsi yang saya buat dengan judul **"Kriptografi Hibrida Menggunakan Algoritma Simetris *Autokey Cipher–Affine Cipher* dan Algoritma Asimetris RSA untuk Keamanan Data Teks Beserta Analisis Keamanannya"** 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, 17 Juli 2026

Nina Niawati

KATA PENGANTAR

Puji dan syukur kehadirat Allah SWT atas segala rahmat, nikmat, dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Kriptografi Hibrida Menggunakan Algoritma Simetris *Autokey Cipher–Affine Cipher* dan Algoritma Asimetris RSA untuk Keamanan Data Teks Beserta Analisis Keamanannya"**. Skripsi ini disusun sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Matematika pada Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta.

Penyelesaian skripsi ini tidak terlepas dari bantuan dan dukungan berbagai pihak yang telah memberikan bimbingan, masukan, serta motivasi dalam proses penelitian dan penyempurnaan skripsi ini. Oleh karena itu, dengan penuh rasa hormat dan kerendahan hati, penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Dr. Yudi Mahatma, M.Si. selaku Koordinator Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Jakarta yang telah memberikan arahan, dukungan, dan fasilitas selama penulis menjalani perkuliahan hingga menyelesaikan skripsi ini.

2. Ibu Dr. Lukita Ambarwati, S.Pd., M.Si. selaku dosen pembimbing I dan Ibu Devi Eka Wardani M, S.Pd., M.Si. selaku dosen pembimbing II yang dengan penuh kesabaran telah mendampingi penulis dalam proses penyusunan skripsi, memberikan arahan dan masukan, serta berbagi ilmu yang sangat membantu dalam menyelesaikan penelitian ini.

3. Segenap dosen Program Studi Matematika dan Rumpun Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Jakarta yang telah memberikan ilmu, pengetahuan, dan pengalaman selama penulis menempuh pendidikan, serta turut mendukung proses akademik penulis hingga penyelesaian skripsi ini.

4. Kedua orang tua tercinta, yang selalu menjadi tempat penulis memperoleh kasih sayang, ketenangan, dan keyakinan untuk terus melangkah dalam setiap proses kehidupan. Terima kasih telah mengajarkan penulis untuk menghargai setiap proses, bertanggung jawab atas pilihan, dan tidak mudah menyerah ketika menghadapi kesulitan. Selama menempuh pendidikan hingga menyelesaikan skripsi ini, doa dan kepercayaan yang diberikan menjadi kekuatan bagi penulis untuk tetap berusaha hingga mencapai tahap ini.

5. Finatri Handayani, sahabat yang telah hadir dalam perjalanan penulis sejak masa sekolah dasar hingga saat ini. Terima kasih telah menjadi tempat berbagi cerita dan bertukar pikiran, serta selalu hadir dengan nasihat, penguatan, dan dukungan dalam berbagai keadaan, baik ketika penulis menghadapi kesulitan maupun saat berbagi kebahagiaan. Meskipun kini kami menempuh pendidikan di perguruan tinggi yang berbeda, kehadiranmu tetap menjadi salah satu sumber kekuatan bagi penulis dalam menjalani proses penyusunan skripsi ini. Semoga persahabatan yang telah terjalin sejak masa kecil ini tetap terjaga, dan kita dapat terus melangkah, tumbuh, serta saling mendukung dalam setiap perjalanan yang akan datang.

6. Rompi Merah (Alwan, Bayu, Davis, Fina, Lintang, Nuha, dan Zulyan), teman-teman yang penulis kenal sejak sekolah dasar. Kedekatan yang berawal dari orang tua kami yang saling mengenal dan sering bersama berkembang menjadi persahabatan yang tetap terjalin hingga saat ini. Terima kasih telah menjadi tempat untuk tertawa, bermain, saling mendukung, dan melepas penat selama proses penyusunan skripsi, serta atas apresiasi dan bantuan yang diberikan. Penulis bersyukur dapat tumbuh bersama dan melihat kalian menjadi pribadi yang semakin dewasa dan membanggakan.

7. Keempat kucing kesayangan penulis, Milo, Moli, Mochi, dan Poni, yang telah menjadi teman setia dalam keseharian, termasuk

selama proses penyusunan skripsi ini. Terima kasih telah menemani dan menghibur penulis di tengah lelah dan penat, serta menghadirkan kebahagiaan melalui tingkah manja dan kebersamaan. Kehadiran kalian menjadi sumber energi bagi penulis untuk kembali bersemangat menjalani hari.

8. Seluruh teman-teman Program Studi Matematika serta teman-teman dari berbagai program studi yang telah menemani perjalanan perkuliahan dan penyusunan skripsi penulis. Terima kasih atas kebersamaan, dukungan, dan setiap momen yang telah menjadi bagian berharga dalam perjalanan ini.

9. Nina Niawati, sebagai seorang anak tunggal yang telah belajar tumbuh dan menghadapi berbagai hal dengan caranya sendiri. Terima kasih telah berani memulai sesuatu yang baru dan terus berusaha memahami berbagai hal yang sebelumnya belum pernah diketahui. Terima kasih telah tetap kuat ketika perjalanan terasa berat, mampu bangkit ketika keadaan membuat langkah terhenti, serta tetap menyelesaikan tanggung jawab yang telah dimulai. Segala hal yang telah dilalui menjadi bagian dari proses untuk belajar, tumbuh, dan mengenal diri sendiri lebih jauh, sekaligus menjadi bekal untuk menghadapi berbagai hal di masa mendatang.

Penulis menyadari bahwa skripsi ini masih memiliki berbagai kekurangan dan keterbatasan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun sebagai bahan perbaikan untuk penyempurnaan skripsi ini. Penulis berharap skripsi ini dapat memberikan manfaat bagi para pembaca serta pihak-pihak yang membutuhkan.

Jakarta, 22 Juli 2026

Penulis

Nina Niawati

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 : Nina Niawati
NIM : 1305621006
Fakultas/Prodi : FMIPA / Matematika
Alamat email : ninanw104@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 :
Kriptografi Hibrida Menggunakan Algoritma Simetris Autokey Cipher - Affine Cipher dan Algoritma Asimetris RSA untuk Keamanan Data Teks Beserta Analisis Keamanannya

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, 18 Agustus 2020

Penulis

(Nina Niawati)
nama dan tanda tangan

ABSTRAK

NINA NIAWATI. Kriptografi Hibrida Menggunakan Algoritma Simetris *Autokey Cipher–Affine Cipher* dan Algoritma Asimetris RSA untuk Keamanan Data Teks Beserta Analisis Keamanannya. Skripsi, Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta. Juli 2026.

Pesatnya digitalisasi meningkatkan risiko kejahatan siber seperti pencurian dan penyalahgunaan data, sehingga dibutuhkan pendekatan kriptografi yang optimal untuk melindungi kerahasiaan informasi. Algoritma simetris unggul dalam kecepatan enkripsi dan dekripsi namun lemah dalam distribusi kunci, sedangkan algoritma asimetris lebih aman dalam distribusi kunci tetapi prosesnya lebih lambat. Kedua kelemahan tersebut dapat saling melengkapi melalui penggabungan keunggulan algoritma simetris dan asimetris dalam satu sistem, sehingga penelitian ini bertujuan mengimplementasikan kriptografi hibrida yang menggabungkan algoritma simetris *Autokey Cipher* dan *Affine Cipher* dengan menerapkan dua urutan kombinasi, yaitu *Autokey–Affine* dan *Affine–Autokey* untuk pengamanan pesan, serta algoritma asimetris RSA untuk pengamanan kunci simetris. Metode penelitian yang digunakan adalah studi literatur, disertai implementasi dengan plainteks dan kunci tertentu. Tingkat keamanan sistem dianalisis menggunakan *Shannon Entropy* untuk menilai kualitas cipherteks dan *Brute Force Attack* untuk menilai ketahanan kunci. Hasil penelitian menunjukkan kedua kombinasi algoritma menghasilkan cipherteks dengan tingkat keacakan yang baik, dengan rata-rata persentase *Shannon Entropy* sebesar 95.50% pada kombinasi *Autokey–Affine* dan 95.38% pada kombinasi *Affine–Autokey*. Panjang kunci *Autokey Cipher* berpengaruh signifikan terhadap tingkat keacakan cipherteks, sedangkan variasi pasangan kunci *Affine Cipher* memberikan pengaruh yang relatif kecil. Analisis *Brute Force Attack* menunjukkan estimasi waktu penemuan kunci mencapai sekitar 8.4971×10^{1572} tahun. Kedua hasil analisis tersebut menunjukkan bahwa cipherteks yang dihasilkan memiliki tingkat keacakan yang baik, sementara estimasi waktu yang diperlukan untuk menemukan kunci yang benar melalui metode *Brute Force Attack* sangat lama sehingga memberikan tingkat ketahanan kunci yang tinggi. Dengan demikian, kombinasi enkripsi berlapis pada pesan dan pengamanan kunci melalui RSA saling melengkapi, sehingga sistem yang dihasilkan tidak hanya menjaga kerahasiaan isi pesan, tetapi juga memberikan perlindungan menyeluruh terhadap keamanan kuncinya.

Kata kunci. Kriptografi Hibrida, *Autokey Cipher*, *Affine Cipher*, RSA, *Shannon Entropy*, *Brute Force Attack*

ABSTRACT

NINA NIAWATI. Hybrid Cryptography Using the Symmetric Autokey Cipher–Affine Cipher Algorithms and the Asymmetric RSA Algorithm for Text Data Security and Security Analysis. Undergraduate Thesis, Mathematics Study Program, Faculty of Mathematics and Natural Sciences, Universitas Negeri Jakarta. July 2026.

The rapid advancement of digitalization has increased the risk of cybercrimes, such as data theft and misuse, thereby creating a need for optimal cryptographic approaches to protect information confidentiality. Symmetric algorithms offer advantages in terms of encryption and decryption speed but have limitations in key distribution, whereas asymmetric algorithms provide greater security in key distribution but involve slower processing.

These limitations can complement each other by combining the advantages of symmetric and asymmetric algorithms within a single system. Therefore, this study aims to implement a hybrid cryptographic system that combines the symmetric algorithms Autokey Cipher and Affine Cipher using two combination orders, namely Autokey–Affine and Affine–Autokey, to secure messages, along with the asymmetric RSA algorithm to protect the symmetric keys. The research methods consist of a literature review and implementation using specific plaintext and keys. The security level of the system is analyzed using Shannon Entropy to evaluate ciphertext quality and Brute Force Attack to assess resistance to key discovery. The results show that both algorithm combinations produce ciphertext with a good level of randomness, with average Shannon Entropy percentages of 95.50% for the Autokey–Affine combination and 95.38% for the Affine–Autokey combination. The length of the Autokey Cipher key has a significant effect on ciphertext randomness, whereas variations in Affine Cipher key pairs have a relatively small effect. The Brute Force Attack analysis estimates that the time required to discover the key reaches approximately 8.4971×10^{1572} years. These two analyses indicate that the resulting ciphertext has a good level of randomness, while the extremely long estimated time required to discover the correct key through a Brute Force Attack indicates a high level of resistance to key discovery. Thus, the combination of layered message encryption and RSA-based key protection complements each other, enabling the resulting system not only to maintain the confidentiality of message content but also to provide comprehensive protection for key security.

Keyword. Hybrid Cryptography, Autokey Cipher, Affine Cipher, RSA, Shannon Entropy, Brute Force Attack

DAFTAR ISI

Daftar Tabel

Daftar Gambar

DAFTAR LAMPIRAN