PENERAPAN KRIPTOGRAFI *HYBRID* PADA *AFFINE CIPHER* DAN ALGORITMA RSA MENGGUNAKAN TEOREMA SISA CINA

SKRIPSI

untuk memenuhi persyaratan
dalam menyelesaikan program sarjana Strata-1 Matematika

Oleh:
UMI NAHDATUS SA'ADAH
NIM. 2111011220023

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMBUNG MANGKURAT
BANJARBARU
2025

LEMBAR PENGESAHAN

SKRIPSI

PENERAPAN KRIPTOGRAFI *HYBRID* PADA *AFFINE CIPHER* DAN ALGORITMA RSA MENGGUNAKAN TEOREMA SISA CINA

Oleh:
Umi Nahdatus Sa'adah
2111011220023

telah dipertahankan di depan Dosen Penguji pada tanggal 5 Juni 2025
Susunan Dosen Penguji:

Pembimbing I

Thresye, S.Si., M.Si.
NIP 197205042000122002

Pembimbing II

Nurul Huda, S.Si., M.Si.
NIP 198104222006041003

Dosen Penguji:
1. Saman Abdurrahman, S.Si., M.Sc. ( )
2. Dr. Na'imah Hijriati, S.Si., M.Si. ( )

Banjarbaru, 24 Juni 2025
Himpunan 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 memperoleh 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, 24 Juni 2025

Umi Nahdatus Sa'adah
NIM. 2111011220023

ABSTRAK

PENERAPAN KRIPTOGRAFI *HYBRID* PADA *AFFINE CIPHER* DAN ALGORITMA RSA MENGGUNAKAN TEOREMA SISA CINA (Oleh: Umi Nahdatus Sa'adah, Pembimbing: Thresye, Nurul Huda, 2025, 72 halaman)

Kriptografi merupakan cara untuk menjaga informasi tetap aman dengan menyembunyikannya dalam kode rahasia. Pada kriptografi modern, algoritma kriptografi terbagi menjadi tiga macam yaitu algoritma simetris, algoritma asimetris, dan algoritma *hybrid*. Algoritma *hybrid* merupakan penggabungan dua kunci simetris dan asimetris. *Affine Cipher* merupakan kriptografi klasik yang menggunakan kunci simetris dan algoritma RSA merupakan algoritma asimetris yang populer. Penelitian ini bertujuan untuk menerapkan kriptografi *hybrid* pada *Affine Cipher* dan algoritma RSA dengan mengaplikasikan Teorema Sisa Cina. Penelitian ini diawali dengan mempelajari mengenai keterbagian, algoritma pembagian, bilangan prima, FPB, Algroitma Euclid, kongruensi, aritmatika modular, kongruensi linier, invers modular, sistem kongruensi simultan, Teorema Sisa Cina dan Teorema Euler. Kemudian membentuk kunci privat d dan kunci publik e. Penggabungan *Affine Cipher* dan algoritma RSA membuat sekuritas dari data menjadi dua tingkatan, yaitu *plaintext* dienkripsi dua kali menggunakan *Affine Cipher* lalu algoritma RSA. Begitupun sebaliknya, *ciphertext* dideskripsi dua kali menggunakan algoritma RSA dengan mengaplikasikan Teorema Sisa Cina lalu *Affine Cipher*.

Kata Kunci: Enkripsi, Deskripsi, *Affine Cipher*, Algoritma RSA, Teorema Sisa Cina.

ABSTRACT

THE IMPLEMENTATION OF HYBRID CRYPTOGRAPHY IN THE AFFINE CIPHER AND RSA ALGORITHM USING THE CHINESE REMAINDER THEOREM (By: Umi Nahdatus Sa'adah, Advisors: Thresye, Nurul Huda, 2025, 72 pages)

Cryptography is a way to keep information safe by hiding it in secret codes. In modern cryptography, cryptographic algorithms are divided into three types, namely symmetric algorithms, asymmetric algorithms and hybrid algorithms. A hybrid algorithm is a combination of two symmetric and asymmetric keys. Affine Cipher is classic cryptography that uses symmetric keys and the RSA algorithm is a popular asymmetric algorithm. This research aims to apply hybrid cryptography to the Affine Cipher and RSA algorithms by applying the Chinese Remainder Theorem. This research begins by studying divisibility, division algorithms, prime numbers, FPB, Euclid's algorithm, congruence, modular arithmetic, linear congruence, modular inverse, simultaneous congruence systems, Chinese Remainder Theorem and Euler's Theorem. Then form a private key d and a public key e. Combining Affine Cipher and the RSA algorithm creates data security at two levels. The plaintext is encrypted twice using Affine Cipher and then the RSA algorithm. Otherwise, the ciphertext is described twice using the RSA algorithm by applying the Chinese Remainder Theorem and then Affine Cipher.

Keywords: Encryption, Descryption, *Affine Cipher*, RSA Algorithm, Chinese Remainder Theorem.

PRAKATA

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 "Penerapan Kriptografi *Hybrid* Pada *Affine Cipher* dan Algoritma RSA Menggunakan Teorema Sisa Cina" 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. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat.
2. Koordinator Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat.
3. Ibu Thresye, S.Si., M.Si., dan Bapak Nurul Huda, S.Si., 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. dan Ibu Dr. Na'imah Hijriati, S.Si., M.Si. selaku dosen penguji yang telah memberikan masukan untuk perbaikan dalam penyusunan skripsi ini.
5. Bapak Dr. Pardi Affandi, S. Si., M. Sc. selaku dosen pembimbing akademik yang telah memberikan bimbingan, saran, motivasi dan semangat dalam masa perkuliahan.

6. Orang tua dan keluarga yang selalu memberikan dukungan, motivasi, pengertian dan doa yang tiada henti.
7. Seluruh sahabat, teman dan rekan khususnya kepada member @Ma(ng)gang💹🕒💼, @Emg agak laen 🏄 dan teman-teman angkatan 2021.
8. Sepupu dan keponakan yang telah menghibur penulis selama perkuliahan hingga penyusunan skripsi.
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, 24 Juni 2025

Umi Nahdatus Sa'adah
NIM. 2111011220023

DAFTAR ISI

DAFTAR TABEL

DAFTAR LAMPIRAN