KRIPTOSISTEM *HYBRID* PADA *HILL CIPHER* DAN MODIFIKASI KRIPTOSISTEM RSA (RSA *SQUARE)*

SKRIPSI

untuk memenuhi persyaratan dalam
menyelesaikan program sarjana Strata-1 Matematika

Oleh :
ALFINA RAUDHOH
2111011320002

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

KRIPTOSISTEM *HYBRID* PADA *HILL CIPHER* DAN MODIFIKASI KRIPTOSISTEM RSA (RSA *SQUARE)*

SKRIPSI

untuk memenuhi persyaratan dalam
menyelesaikan program sarjana Strata-1 Matematika

Oleh :
ALFINA RAUDHOH
2111011320002

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

LEMBAR PENGESAHAN

SKRIPSI

KRIPTOSISTEM HYBRID PADA HILL CHIPER DAN MODIFIKASI KRIPTOSISTEM RSA

Oleh:

Alfina Raudhoh

NIM. 2111011320002

telah dipertahankan di depan Dosen Penguji pada tanggal 22 Juli 2026

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. **Oni Soesanto, S.Si., M.Si. ( )**

Banjarbaru, 27 Juli 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 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, 27 Juli 2026

Alfina Raudhoh

NIM. 2111011320002

ABSTRAK

KRIPTOSISTEM *HYBRID* PADA *HILL CIPHER* DAN MODIFIKASI KRIPTOSISTEM RSA (RSA *SQUARE)* (Oleh: Alfina Raudhoh; Pembimbing: Thresye, Nurul Huda)

Kriptografi merupakan salah satu cabang matematika yang berperan penting dalam pengamanan informasi, khususnya pada era digital saat ini. *Hill Cipher* sebagai algoritma kriptografi simetris memiliki kecepatan enkripsi yang tinggi, namun lemah dalam aspek distribusi kunci dan keamanan. Sebaliknya, kriptosistem *RSA* sebagai algoritma kriptografi asimetris memiliki tingkat keamanan yang tinggi, tetapi proses enkripsi dan dekripsinya relatif lambat. Penelitian ini membahas penerapan kriptosistem *hybrid* yang mengombinasikan *Hill Cipher* dengan modifikasi kriptosistem RSA Square (RSASQ). Tujuan penelitian ini adalah menjelaskan proses pembentukan kunci serta proses enkripsi dan dekripsi pada kriptosistem *hybrid* tersebut. *Hill Cipher* digunakan sebagai algoritma kriptografi simetris untuk mengenkripsi pesan, sedangkan RSASQ digunakan untuk mengamankan kunci sesi *Hill Cipher* melalui mekanisme kunci publik dan kunci privat. Metode penelitian yang digunakan dalam penelitian ini bersifat teoritis dan deskriptif, yang meliputi tahapan pembentukan kunci simetris menggunakan algoritma *Hill cipher*, pembangkitan pasangan kunci asimetris RSA Square (RSASQ), serta penerapan proses enkripsi dan dekripsi melalui contoh numerik. Hasil penelitian menunjukkan bahwa kriptosistem hybrid yang digunakan dapat mengombinasikan mekanisme pertukaran kunci berbasis kriptografi asimetris dengan proses enkripsi data menggunakan kriptografi simetris. Melalui contoh numerik, sistem yang dirancang mampu menjalankan proses pembentukan kunci, enkripsi, dan dekripsi sesuai dengan prosedur algoritma yang telah ditentukan. Penelitian ini bersifat teoritis dan numerik, sehingga belum mencakup analisis keamanan komputasional maupun pengujian kinerja algoritma.

Kata Kunci: Kriptografi, Kriptosistem Hybrid, *Hill cipher*, RSA Square (RSASQ).

ABSTRACT

HYBRID CRYPTOSYSTEM BASED ON HILL CIPHER AND MODIFIED RSA CRYPTOSYSTEM (RSA SQUARE) *(By: Alfina Raudhoh; Advisors: Thresye, Nurul Huda)*

Cryptography is a branch of mathematics that plays a crucial role in securing information, particularly in the current digital era. The Hill cipher, as a symmetric cryptographic algorithm, offers high encryption speed but suffers from weaknesses in key distribution and security. In contrast, the RSA cryptosystem, which is an asymmetric cryptographic algorithm, provides a high level of security; however, its encryption and decryption processes are relatively slow. This study discusses the implementation of a hybrid cryptosystem that combines the Hill cipher with a modified RSA Square (RSASQ) cryptosystem. The purpose of this research is to explain the key generation process as well as the encryption and decryption procedures within the proposed hybrid cryptosystem. The Hill cipher is employed as a symmetric algorithm to encrypt the message, while RSASQ is used to secure the Hill cipher session key through a public–private key mechanism. The research method used in this study is theoretical and descriptive, which includes the stages of symmetric key formation using the Hill cipher algorithm, the generation of an asymmetric key pair RSA Square (RSASQ), and the implementation of the encryption and decryption processes through numerical examples. The research results demonstrate that the employed hybrid cryptosystem combines an asymmetric cryptography-based key exchange mechanism with a data encryption process utilizing symmetric cryptography. Through a numerical example, the designed system is shown to successfully execute key generation, encryption, and decryption processes in accordance with the established algorithmic procedures. As this study is theoretical and numerical in nature, it does not yet encompass computational security analysis or performance testing of the algorithms.

Keywords*: Cryptography, Hybrid Cryptosystem, Hill cipher, RSA Square (RSASQ).*

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 "Kriptosistem *Hybrid* pada *Hill Cipher* dan Modifikasi Kriptosistem RSA (RSA *Squre)*" 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 Prof. Sunardi, S.Si., M.Sc., Pc.D. selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
2. Ibu Dr. Na'imah Hijriati, S.Si., M.Si. selaku Ketua Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
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 Bapak Oni Soesanto, S.Si., M.Si. selaku dosen penguji yang telah memberikan masukan untuk perbaikan dalam penyusunan skripsi ini.

5. Ibu Thresye S.Si., M.Si. selaku dosen penasehat akademik yang telah memberikan arahan dan bimbingan selama perkuliahan.
6. Kedua orang tua tercinta dan seluruh keluarga yang selalu memberikan doa, kasih sayang, dukungan, motivasi, serta pengorbanan yang tiada henti sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
7. Keluarga kecil *Moodbooster*, yang telah menjadi bagian penting dalam perjalanan penulis selama masa perkuliahan. Terima kasih karena selalu hadir untuk saling menguatkan, mendengarkan, menghibur, serta memberikan semangat dalam setiap proses yang dilalui. Semoga pertemanan ini senantiasa terjaga, dan semoga setiap langkah yang kita tempuh ke depan dipenuhi kemudahan, keberkahan, serta kesuksesan.
8. Abiy, Asna, dan Rizka, yang telah menjadi teman seperjuangan sekaligus menghadirkan kehangatan layaknya rumah kedua bagi penulis selama menjalani masa perkuliahan. Terima kasih atas setiap dukungan, perhatian, bantuan, serta kebersamaan yang telah diberikan. Terima kasih telah menjadi tempat berbagi cerita, bertukar pikiran, dan saling menguatkan hingga penulis mampu menyelesaikan skripsi ini.
9. Teman-teman seperjuangan angkatan 2021, yang telah mewarnai perjalanan penulis selama masa perkuliahan dengan kebersamaan, dukungan, semangat, serta bantuan dalam berbagai proses hingga skripsi ini dapat diselesaikan.
10. Seluruh pihak yang telah membantu penulis dalam penyusunan skripsi ini, yang tidak dapat disebutkan satu per satu.
11. Terakhir, untuk diri sendiri, Alfina Raudhoh, anak perempuan terakhir dan harapan terakhir kedua orang tua. Terima kasih atas segala kerja keras, kesabaran, dan keteguhan dalam menghadapi setiap proses hingga skripsi ini dapat diselesaikan. Terima kasih karena selalu memilih untuk bertahan, terus berjalan, dan menyelesaikan apa yang telah dimulai. Terima kasih telah menjadi pribadi yang kuat dan tidak menyerah, meskipun tidak selalu yakin dengan diri sendiri. Semoga langkah kecil ini menjadi bukti bahwa saya mampu menyelesaikan apa yang telah saya perjuangkan. Semoga

setiap perjuangan, doa, dan pengorbanan yang telah dilakukan menjadi awal dari perjalanan yang lebih baik serta mampu membahagiakan dan membanggakan kedua orang tua, keluarga, dan diri sendiri.

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, 27 Juli 2026

Alfina Raudhoh

NIM. 2111011320002

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ARTI LAMBANG DAN SINGKATAN

$\mid$	: membagi
$\nmid$	: tidak membagi
$\equiv$	: kongruen
$\not\equiv$	: tidak kongruen
$=$	: sama dengan
$\neq$	: tidak sama dengan
$<$	: kurang dari
$>$	: lebih dari
$\leq$	: kurang dari sama dengan
$\geq$	: lebih dari sama dengan
ϕ	: fungsi Phi-Euler
mod	: modulo
(a,b)	: fpb dari a dan b
P	: plainteks (pesan asli)
C	: cipherteks (hasil enkripsi)
E	: fungsi enkripsi
D	: fungsi dekripsi
$\Longrightarrow$	: pembuktian dari kiri ke kanan
$\Longleftarrow$	: pembuktian dari kanan ke kiri
■	: terbukti