KRIPTOSISTEM *HYBRID* BERBASIS PADA MODIFIKASI *PLAYFAIR CIPHER* DAN MODIFIKASI KRIPTOSISTEM RSA

SKRIPSI

untuk memenuhi persyaratan

dalam menyelesaikan program sarjana Strata-1 Matematika

Oleh:

FARAH DIBA

NIM. 2111011220003

PROGRAM STUDI MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS LAMBUNG MANGKURAT

BANJARBARU

2025

HALAMAN PENGESAHAN

SKRIPSI

KRIPTOSISTEM HYBRID BERBASIS PADA MODIFIKASI PLAYFAIR *CIPHER* DAN MODIFIKASI KRIPTOSISTEM RSA

Oleh:

Farah Diba

NIM. 2111011220003

Telah di pertahankan di depan Dosen Penguji pada tanggal 27 Mei 2025

Susunan Dosen Penguji

Pembimbing I

Thresye, S.Si., M.Si.

NIP. 197205042000122002

Dosen Penguji:

1. Dr. Na'imah Hijriati, S.Si., M.Si. (...)
2. Oni Soesannto, S.Si., M.Si (...)

Pembimbing II

Akhmad Yusuf, S.Si., M.Kom.

NIP. 198004022005011001

Banjarbaru, 16 Juni 2025

Ketua Jurusan Matematika

FMIPA ULM

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, 23 Juni 2025

Farah Diba

NIM. 2111011220003

ABSTRAK

KRIPTOSISTEM *HYBRID* BERBASIS PADA MODIFIKASI *PLAYFAIR CIPHER* DAN MODIFIKASI KRIPTOSISTEM RSA (Oleh: Farah Diba; Pembimbing: Thresye, Akhmad Yusuf)

Keamanan informasi menjadi aspek yang sangat penting dalam transmisi data melalui jaringan, terutama dalam melindungi data sensitif dari ancaman peretasan. Salah satu cara dalam menjaga keamanannya ialah menggunakan kriptografi. Dalam penelitian ini, penulis bertujuan mengkaji dan menganalisa kriptosistem *hybrid* yang berbasis pada modifikasi *Playfair cipher* dengan kunci matriks 7×13 dan modifikasi kriptosistem RSA. Dalam penelitian ini, dilakukan evaluasi dengan pemrograman *Python* terhadap pengimplementasi kriptosistem *hybrid* dengan komponen simetrisnya modifikasi *Playfair cipher*, sedangkan komponen asimetrisnya terbagi dua, yaitu RSA klasik dan RSA yang dimodifikasi. Metode pada penelitian ini melibatkan pengumpulan dan studi konsep-konsep dasar terkait teori bilangan bulat, kongruensi, fungsi phi-euler, dan teori lainnya seperti algoritma *Playfair cipher* dan RSA. Berdasarkan pengujian terhadap pesan "Program Studi Matematika", bahwa proses RSA lebih cepat, namun RSA yang dimodifikasi menunjukkan peningkatan kompleksitas dan stabilitas performa. Meskipun membutuhkan waktu enkripsi sekitar 1,85 kali lebih lama dan dekripsi 3,2 kali lebih lama dibandingkan RSA klasik, modifikasi RSA meningkatkan keamanan dengan mengkuadratkan eksponen dalam pembentukan kunci. Selain itu, penggunaan matriks kunci 7×13 dalam *Playfair cipher* menunjukkan keunggulan dalam menangani karakter yang lebih kompleks dan memperkuat sistem terhadap serangan berbasis frekuensi. Dengan demikian, kriptosistem *hybrid* berbasis modifikasi *Playfair cipher* dan modifikasi RSA menunjukkan performa yang stabil dengan tingkat keamanan yang lebih tinggi dibandingkan versi klasik.

Kata Kunci: Teori Bilangan, Kriptosistem, *Playfair cipher,* RSA, Modifikasi, Kriptosistem *Hybrid*.

ABSTRACT

***HYBRID* CRIPTOSISTEM BASED ON *PLAYFAIR CIPHER* MODIFICATION AND RSA CRIPTOSISTEM MODIFICATION** (By: Farah Diba; Advisors: Thresye, Akhmad Yusuf)

Information security is a very important aspect in data transmission over networks, especially in protecting sensitive data from hacking threats. One way to maintain security is to use cryptography. In this study, the author aims to examine and analyze a hybrid cryptosystem based on a modified Playfair cipher with a 7×13 matrix key and a modified RSA cryptosystem. In this study, an evaluation was conducted using Python programming to implement the hybrid cryptosystem, with its symmetric component being the modified Playfair cipher, while its asymmetric component is divided into two parts: classical RSA and modified RSA. The methods used in this study involved the collection and study of basic concepts related to integer theory, congruence, Euler's phi function, and other theories such as the Playfair cipher and RSA algorithms. Based on testing of the message "Program Studi Matematika", the RSA process was faster, but the modified RSA showed an increase in complexity and performance stability. Although it requires approximately 1.85 times longer for encryption and 3.2 times longer for decryption compared to classical RSA, the modified RSA enhances security by squaring the exponent in key generation. Additionally, the use of a 7×13 key matrix in the Playfair cipher demonstrates advantages in handling more complex characters and strengthening the system against frequency-based attacks. Thus, the hybrid cryptosystem based on the modified Playfair cipher and modified RSA demonstrates stable performance with a higher security level compared to the classical versions.

Keywords: Number Theory, Cryptosystem, Playfair cipher, RSA, Modification, Hybrid Cryptosystem.

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* Berbasis Pada Modifikasi *Playfair cipher* Dan Modifikasi Kriptosistem RSA" 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 doa, dukungan, bimbingan, dan bantuan dari berbagai pihak. Selesainya penulisan skripsi ini, dipersembahkan untuk kedua orang tua, keluarga tercinta, dan teman-teman yang penulis banggakan. Pada kesempatan ini juga, penulis ucapkan 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 program studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
3. Ibu Thresye S.Si., M.Si. dan Akhmad Yusuf, S.Si., M.Kom. selaku dosen pembimbing yang telah mendampingi dan membimbing dalam penyusunan skripsi ini dari awal sampai akhir.
4. Ibu Dr. Na'imah Hijriati, 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 sabar dalam memberikan arahan dan bimbingan selama perkuliahan.

6. Abah dan Mama yang senantiasa mendukung, memberikan semangat, dan bersabar dalam proses pendidikan yang ditempuh selama ini.
7. Keluarga dan teman-teman dekat saya seperti Kaka Tami, Kak Salma, Kak Salwa, Dwi, Awinda, Ikhsan, Kak Lisa, Kak Yogi, dan teman-teman di IKASI Kota Banjarbaru yang memberikan semangat serta dukungan dalam proses penulisan ini.

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 senatiasa penulis harapkan demi kesempurnaan dimasa yang akan datang. Semoga skripsi ini dapat memberikan sumbangan yang bermanfaat bagi semua pihak.

Banjarbaru, 23 Juni 2025

Farah Diba

NIM. 2111011220003

DAFTAR ISI

Halaman

DAFTAR TABEL

Tabel **Halaman**

DAFTAR GAMBAR

Gambar **Halaman**

DAFTAR LAMPIRAN

ARTI LAMBANG DAN SINGKATAN

$a\|b$	:	a membagi habis b
$a \nmid b$	:	a tidak membagi habis b
$<$	:	Tanda "lebih kecil dari"
$>$	:	Tanda "lebih besar dari"
$\leq$	:	Tanda "lebih kecil atau sama dengan"
$\geq$	:	Tanda "lebih besar atau sama dengan"
$(a, b) = d$	:	Pembagi bersama terbesar (PBB) dari a dan b merupakan d
$a \ mod \ m$	:	Sisa dari a dibagi m
$a \equiv b \ (mod \ m)$	:	a kongruen dengan b modulo m
$a \not\equiv b$	:	a tidak kongruen b
$r_1, r_2, \dots, r_m$	:	Barisan r dengan elemen ke-m
$\phi(n)$	:	Fungsi Phi Euler terhadap n
P	:	Pesan yang ingin dikirimkan (*Plaintext*)
E	:	Proses enkripsi pesan (*plaintext*)
C	:	Hasil enkripsi (*Chipertext)*
D	:	Hasil dekripsi
■	:	Akhir dari suatu pembuktian
(d_2, n^2)	:	Kunci privat di RSA *Square* (RSASQ)
(e, n)	:	Kunci Publik di RSA Klasik dan RSA *Square* (RSASQ)
(d, n)	:	Kunci Privat di RSA Klasik