ALGORITMA *HYBRID* MENGGUNAKAN *MYSZKOWSKI CIPHER* DAN RSA UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

OLEH:
SUKMAWATI INDAH SAFITRI
NIM. 19610008

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2023

ALGORITMA *HYBRID* MENGGUNAKAN *MYSZKOWSKI CIPHER* DAN RSA UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Matematika (S.Mat)

Oleh
Sukmawati Indah Safitri
NIM. 19610008

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2023

ALGORITMA *HYBRID* MENGGUNAKAN *MYSZKOWSKI CIPHER* DAN RSA UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Sukmawati Indah Safitri
NIM. 19610008

Telah Disetujui untuk Diuji

Malang, 08 Juni 2023

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si	Mohammad Nafie Jauhari, M.Si
NIDT. 19900501 20160801 1 057	NIDT. 19870218 20160801 1 056

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.
NIP. 19741129 200012 2 005

ALGORITMA *HYBRID* MENGGUNAKAN *MYSZKOWSKI CIPHER* DAN RSA UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Sukmawati Indah Safitri
NIM. 19610008

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 15 Juni 2023

Ketua Penguji	:	Dr. Elly Susanti, M.Sc.	.....
Anggota Penguji 1	:	Hisyam Fahmi, M.Kom.	.....
Anggota Penguji 2	:	Muhammad Khudzaifah, M.Si.	.....
Anggota Penguji 3	:	Mohammad Nafie Jauhari, M.Si.	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Sukmawati Indah Safitri

NIM : 19610008

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA untuk Mengamankan Pesan Teks

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan dan pikiran saya, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila dikemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perilaku tersebut.

Malang, 15 Juni 2023

Yang membuat pernyataan,

Sukmawati Indah Safitri

NIM. 19610008

MOTO

"*Angin tidak berhembus untuk menggoyangkan pepohonan, melainkan untuk menguji kekuatan akarnya.*"

- Ali bin Abi Thalib

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Yang tersayang Bapak M. Zainal Aris dan yang tercinta Ibu Listiari yang senantiasa ikhlas mendoakan, menyemangati, serta perjuangannya yang tanpa henti untuk penulis.

Adik M. Arga Pramudya Kusuma serta saudara-saudari yang telah memberi dukungan kepada penulis.

Sahabat-sahabat saya Tre Hayu Ria Sageta, Rika Dina Amalia, Hakimatul Maulidiyah terimakasih banyak untuk kerjasamanya dari awal hingga akhir perkuliahan.

KATA PENGANTAR

Segala puji bagi Allah SWT atas rahmat, taufik serta hidayah-Nya, sehingga penulis mampu menyelesaikan penyusunan skripsi yang berjudul "Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA untuk Mengamankan Pesan Teks" sebagai salah satu syarat untuk memperoleh gelar sarjana dari Program Studi Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak. Untuk itu penulis ingin mengucapkan terima kasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya terutama kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si., selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc., selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Khudzaifah, M.Si. dan Mohammad Nafie Jauhari, M.Si. selaku dosen pembimbing, terimakasih atas bimbingan, kritik dan saran dan selalu meluangkan waktunya disela kesibukan. Semoga selalu dilimpahkan kesehatan dan keberkahan oleh-Nya.
5. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
6. Bapak M. Zainal Aris dan Ibu Listiari yang sangat hebat perjuangannya untuk memberikan pendidikan kepada putrinya hingga di titik ini. Saya persembahkan karya tulis sederhana ini untuk Bapak dan Ibu, terimakasih telah melahirkan, merawat, dan membesarkan saya dengan penuh cinta hingga saya tumbuh dewasa dan berada di posisi saat ini.
7. Terimakasih atas tangis dan tawa yang telah terlewati yang mampu mendewasakan saya, mampu menuntun saya untuk belajar mengikhlaskan dan menerima rasa kehilangan sebagai bentuk proses penempaan menghadapi dinamika kehidupan. Masa-masa itu akan menjadi pengalaman terbaik saya.

8. Seluruh teman-teman Soulmath’19 terimakasih selalu memberikan semangat, dukungan tanpa henti sehingga saya mampu menyelesaikan skripsi ini.

Semoga Allah SWT melimpahkan rahmat dan karunia-Nya kepada kita semua dan semoga skripsi ini bermanfaat bagi kita semua.

Malang, 15 Juni 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR LAMPIRAN

ABSTRAK

Safitri, Sukmawati. 2023. **Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA untuk Mengamankan Pesan Teks**. Skripsi Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Maulana Malik Ibrahim Malang, Pembimbing (1) : Muhammad Khudzaifah, M.Si, Pembimbing (2) : Mohammad Nafie Jauhari, M.Si.

Kata Kunci : *Hybrid*, *Myszkowski Cipher*, Algoritma, RSA.

Kriptografi klasik dan kriptografi modern memiliki sisi kelebihan dan kelemahan masing-masing dalam mengamankan pesan teks. Algoritma *hybrid* dapat menggabungkan dua algoritma kriptografi untuk menghasilkan tingkat keamanan pesan yang lebih tinggi jika dibandingkan dengan penggunaan satu jenis algoritma saja. Penelitian ini membahas tentang algoritma *hybrid* yang menggabungkan *Myszkowski Cipher* dan RSA yang merupakan kriptografi klasik dengan teknik transposisi serta kriptografi modern dengan teknik substitusi. Tujuan dilakukannya penelitian ini yaitu agar mendapatkan *ciphertext* yang lebih sulit dipecahkan oleh kriptanalisis. Proses algoritma *hybrid* dilakukan dengan mengenkripsi pesan teks dengan algoritma *Myszkowski Cipher* kemudian kata kunci yang digunakan dalam algoritma *Myszkowski Cipher* dienkripsi menggunakan algoritma RSA. Maka akan diperoleh *ciphertext* pesan dan *cipherkey* yang berbentuk numerik. Dalam proses dekripsinya dilakukan dengan mendekripsikan *cipherkey* dengan RSA terlebih dahulu untuk memperoleh bentuk alfabet, selanjutnya proses dekripsi *ciphertext* pesan menggunakan algoritma *Myszkowski Cipher* dapat dilakukan.

ABSTRACT

Safitri, Sukmawati. 2023. **Hybrid Algorithms Using Myszkowski Cipher and RSA to Secure Text Messages**. Thesis of Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Supervisor (1) : Muhammad Khudzaifah, M.Si, Supervisor (2) : Mohammad Nafie Jauhari, M.Si.

Keywords: Hybrid, Myzkowski Cipher, Algorithm, RSA.

Classical cryptography and modern cryptography have their own advantages and disadvantages in securing text messages. Hybrid algorithms can combine two cryptographic algorithms to produce a higher level of message security when compared to one type of algorithm. This study discusses a hybrid algorithm that combines Myszkowski Cipher and RSA which is classical cryptography with transposition techniques and modern cryptography with substitution techniques. The purpose of this research is to obtain ciphertext that is more difficult to crack by cryptanalysis. The hybrid algorithm process is done by encrypting text messages with the Myszkowski Cipher algorithm then the key used in the Myszkowski Cipher algorithm are encrypted using the RSA algorithm. Then two ciphertext will be obtained, namely text messages and numeric key. In the decryption process is done by decrypting the cipherkey with RSA first to obtain the alphabetical form, then the process of decrypting the ciphertext message using the Myszkowski Cipher algorithm can be done.

مستخلص البحث

سفطري ، سوكماواتي. ٣٢٠٢. **خوارزميات هجينة تستخدم تشفير *Myszkowski* و RSA لتأمين الرسائل النصية**. قسم الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكمية مالانج، المشرف (١): محمد خديفة، الماجستير، المشرف (٢): محمد نافع جوهري، الماجستير.

الكلمات المفتاحية: هجينة ، تشفير *Myszkowski* ، الخوارزمية ، RSA.

لتشفير الكلاسيكي والتشفير الحديث مزايا وعيوبهما في تأمين الرسائل النصية. يمكن أن تجمع الخوارزميات الهجينة بين خوارزميتين مشفرتين لإنتاج مستوى أعلى من أمان الرسائل عند مقارنتها باستخدام نوع واحد من الخوارزميات وحده. تناقش هذه الدراسة خوارزمية الهجينة تجمع بين تشفير *Myszkowski* و RSA وهو تشفير الكلاسيكي مع تقنيات تبديل وتشفير الحديث مع تقنيات الاستبدال. الغرض من هذا البحث هو الحصول على النص المشفر يصعب كسره عن طريق تحليل الشفرات. تتم عملية الخوارزمية الهجينة عن طريق تشفير الرسائل النصية باستخدام خوارزمية *Myszkowski* تشفير ثم يتم تشفير كلمات المرور المستخدمة في خوارزمية *Myszkowski* التشفير باستخدام الخوارزمية .RSA ثم سيتم الحصول على النصين المشفرين ، وهما الرسائل النصية والكلمات الرئيسية الرقمية. في عملية فك التشفير تتم عن طريق فك التشفير التشفير باستخدام RSA أولا للحصول على النموذج الأبجدي ، ثم يمكن إجراء عملية فك تشفير رسالة النص المشفر باستخدام خوارزمية *Myszkowski* تشفير .

BAB I

PENDAHULUAN

1.1 Latar Belakang

Manusia hidup sebagai makhluk sosial yang selalu menjadi bagian dari masyarakat tentu saling membutuhkan antar sesama. Di dalam kehidupan sehari-harinya manusia tidak bisa bertahan sendiri tanpa melakukan interaksi dengan orang lain secara langsung ataupun dengan cara komunikasi jarak jauh. Oleh karena itu, kita sebagai manusia hendaklah menjaga amanat berupa apapun yang dititipkan orang lain kepada kita. Salah satu amanat yang dititipkan oleh sesama manusia adalah pesan. Tak jarang manusia menitipkan suatu pesan melalui orang lain, hal ini dapat disebabkan keterbatasan jarak untuk menyampaikan pesan tersebut secara langsung ataupun keterbatasan yang lainnya. Terkadang pesan itu bersifat pribadi dan hanya diperbolehkan untuk dibaca pihak penerima yang diinginkan pengirim, maka sebagai pihak perantara harus bisa menjaga keamanan pesan yang telah dititipkan tersebut.

Dalam menjaga keamanan dari pesan yang dikirim, maka diperlukan sebuah sistem yang bisa mengamankan isi pesan (*plaintext*). Menjaga keamanan pesan dengan menggunakan suatu kunci dan yang memiliki izin untuk mendapatkan kunci tersebut hanyalah pengirim dan penerima pesan saja dapat menjadi suatu alternatif dalam pengamanan pesan. Alqur'an surah An – Nisa' ayat 58 menjelaskan: (Kemenag, 2019)

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat."

Tafsir Ibnu Katsir menyatakan bahwa ayat ini menjelaskan tentang amanah bagi manusia sebagai hamba-Nya, amanat yang dititipkan oleh Allah kepada manusia itu seperti shalat, zakat, puasa, bertaubat, nazar dan lain-lain, yang semuanya diberikan tanpa pengawasan hamba-Nya yang lain. Demikian pula amanat berupa hak sebagian hamba dengan hamba lainnya, seperti titipan-titipan dan lain-lain, semuanya merupakan amanat yang dilaksanakan tanpa pemeriksaan saksi. Bagi manusia yang tidak melakukannya di dunia ini akan dimintai pertanggungjawaban atas perbuatannya pada hari kebangkitan kelak (Katsir, 2015).

Terdapat beberapa cara untuk mengamankan pesan dan salah satunya adalah dengan menerapkan ilmu kriptografi. Ilmu kriptografi adalah suatu teknik dalam matematika yang mempelajari tentang proses keamanan pengiriman dan penerimaan informasi data, misalnya validitas data, kesatuan data, dan autentikasi data (Tulloh dkk., 2016). Menurut Meylisa Siska, ilmu kriptografi merupakan sebuah ilmu pengetahuan yang di dalamnya membahas tentang kemanan sebuah pesan yang ditunjukan pengirim kepada penerima pesan agar sampai dengan selamat dan dapat terjaga keamanannya. Ilmu kriptografi adalah sebuah ilmu matematis yang bisa disebut sebagai ilmu kriptologi. Ilmu kriptologi ini memiliki tujuan untuk menjaga keamanan informasi yang ada di dalam sebuah data, sehingga informasi data yang dikirimkan itu tidak akan bisa diketahui oleh orang yang tidak berwenang. Orang yang merancang algoritma enkripsi dan algoritma dekripsi disebut dengan kriptografer (Bangun, 2019).

Myszkowski Cipher merupakan salah satu jenis dari algoritma cipher transposisi kriptografi klasik. Algoritma transposisi ini memerlukan kata kunci dengan karakter yang berulang (Pohan, 2007). *Myszkowski Cipher* memiliki keunikan dan dapat dimodifikasi dengan mudah, algoritma cipher transposisi ini cukup menarik karena terdapat perbedaan dalam pembacaan dan penulisan *ciphertext* ketika memiliki nomor kunci yang sama (Khairina, 2019). Algoritma transposisi *Myszkowski Cipher* ini merupakan variasi dari *Columnar Transposition* yang diciptakan oleh tokoh yang bernama Émile Victor Théodore Myszkowski pada tahun 1902.

Berikut adalah beberapa penelitian terdahulu yang terkait diantaranya yaitu penelitian Khairina, pada penelitian ini peneliti memodifikasi algoritma *Myszkowski Transposition Cipher* dengan *Chess Board Pattern*. Enkripsi dan dekripsi dengan *Chess Board Pattern* dilakukan dengan mengikuti pola papan catur berwarna hitam putih. Kombinasi algoritma *Myszkowski* dengan *Chess Board Pattern* menghasilkan variasi pola enkripsi dan dekripsi yang beragam, sehingga proses enkripsi dan dekripsi menjadi lebih rumit (Khairina, 2019). Kemudian penelitian oleh Agustina, pada penelitian ini dilakukan suatu analisis dalam perspektif keamanan file yang bertujuan untuk mengamankan file menggunakan metode RSA. Proses penerapannya yaitu suatu data yang dikirim terlebih dahulu dienkripsi oleh pengirim dan menghasilkan data terenkripsi selanjutnya akan dikirim kepada penerima untuk dilakukan proses dekripsi yang menghasilkan suatu data yang sebenarnya. Dari penelitian ini dapat disimpulkan bahwa tingkat keamanan dengan menggunakan metode RSA termasuk dalam kategori metode yang aman dipakai untuk proses pengamanan dokumen (Agustina dkk., 2017).

Selanjutnya penelitian oleh Jamaludin, penggunaan *Hybrid Cryptosystem* dalam penelitian ini merupakan kombinasi dari algoritma *Hill Cipher* sebagai bagian algoritma simetri, dan dikombinasikan dengan algoritma RSA sebagai bagian algoritma asimetri untuk pengamanan pesan teks. Hasil penelitian dari kedua kombinasi algoritma *Hill Cipher* dan RSA bisa diterapkan untuk peningkatan pengamanan pada pesan teks dimana *plaintext* yang dikirim dienkripsi oleh algoritma *Hill Cipher* serta pengamanan kunci oleh algoritma RSA. (Jamaludin, 2018). Selain itu terdapat penelitian oleh Tri Rahajoeningrum yang menghasilkan suatu pengujian yang menunjukkan bahwa algoritma RSA berhasil diimplementasikan untuk pengamanan data transkrip akademik mahasiswa. Berdasarkan pengujian diperoleh waktu komputasi algoritma RSA adalah sebesar 15625 mikrodetik. Sedangkan kompleksitas memori yang dibutuhkan algoritma RSA sebesar 3908 *bytes* (Rahajoeningroem & Aria, 2011).

Kelemahan yang dimiliki oleh algoritma *Myszkowski Cipher* sebagai kriptografi klasik yaitu jika kita mengenkripsi pesan dengan menerapkan hanya satu algoritma saja akan mudah dipecahkan oleh kriptanalisis jika tidak digabung dengan algoritma lain, karena masih tergolong algoritma kriptografi dengan kunci simetris. Namun, penerapan algoritma kriptografi kunci simetris masih sering dilakukan karena bisa menjalankan proses enkripsi dan dekripsi pesan dalam waktu yang terbilang cukup efektif, akan tetapi perlindungan kunci pada algoritma kunci simetris ini masih kurang aman, sehingga untuk mengamankan isi pesan yang dikirim kunci yang digunakan harus sering diganti untuk mencegah penyerangan pada kriptografi oleh kriptanalisis. Sementara itu, kriptografi asimetris adalah kebalikannya, keamanan dari kunci yang digunakan pada algoritma asimetris

sangatlah terjamin, akan tetapi proses ketika melakukan enkripsi dan dekripsi pesan akan lebih lambat karena masih memerlukan waktu yang lebih banyak dalam prosesnya.

Hybrid merupakan gabungan antara krirptografi yang memakai kunci simetris dan kriptografi yang memakai kunci asimetris. Dalam penggunaan algoritma *hybrid*, teknik enkripsi yang digunakan adalah enkripsi simetri dimana kunci dekripsi sama dengan kunci enkripsi. Untuk kunci publik kriptografi, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi (Jamaludin, 2018). Sistem enkripsi *hybrid* ini banyak digunakan selain dapat meningkatkan keamanan pesan teks dan kunci yang dikirimkan, algoritma *hybrid* juga akan melibatkan lebih banyak perhitungan jika dibandingkan dengan menggunakan saatu algoritma saja. Penggunaan sistem enkripsi algoritma *hybrid* yang digunakan pada penelitian ini adalah suatu kombinasi dari kriptografi algoritma *Myszkowski Cipher* yang termasuk bagian dari algoritma kriptografi kunci simetris dan algoritma RSA (*Rivest, Shamir, Adleman*) yang termasuk bagian dari algoritma kriptografi kunci asimetris agar dapat meningkatkan perlindungan dari pesan teks dan akan menghasilkan *ciphertext* yang lebih sulit dipecahkan.

Algoritma RSA merupakan algoritma asimetris yang teruji sebagai sistem kriptografi yang aman karena kesulitan dalam proses memfaktorkan bilangan yang sangat besar (Jamaludin, 2018). Sehingga penulis memutuskan untuk mengambil judul penelitian Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA untuk Mengamankan Pesan Teks.

1.2 Rumusan Masalah

Berdasarkan penjelasan dari latar belakang di atas, diperoleh rumusan masalah penelitian sebagai berikut:

1. Bagaimana hasil proses enkripsi algoritma *hybrid Myszkowski Cipher* dan RSA?
2. Bagaimana hasil proses dekripsi algoritma *hybrid Myszkowski Cipher* dan RSA?

1.3 Tujuan Penelitian

Berdasarkan pada beberapa rumusan masalah penelitian di atas, tujuan dari dilakukannya penelitian ini adalah:

1. Mengetahui hasil proses enkripsi algoritma *hybrid Myszkowski Cipher* dan RSA.
2. Mengetahui hasil proses dekripsi algoritma *hybrid Myszkowski Cipher* dan RSA.

1.4 Manfaat Penelitian

Manfaat yang dapat kita peroleh dari penelitian ini diantaranya yaitu:

1. Bagi mahasiswa, diharapkan penelitian ini bisa menjadi sebuah rujukan serta pengembangan pembelajaran kriptografi mengenai *Myszkowski Cipher* dan RSA.
2. Bagi pembaca, penelitian ini mampu memberikan informasi untuk mengetahui proses penyandian pesan dengan kriptografi secara *hybrid* dengan menggunakan algoritma *Myszkowski Cipher* dan RSA.
3. Bagi UIN Malang, penelitian ini diharapkan bisa menjadi sebuah sumbangan pemikiran keilmuan pada program studi matematika khususnya di

konsorsium aljabar kriptografi tentang teknik enkripsi dan dekripsi secara *hybrid*.

4. Bagi peneliti, dapat meningkatkan keamanan pesan secara *hybrid* menggunakan algoritma *Myszkowski Cipher* dan RSA.

1.5 Batasan Masalah

Dalam upaya pencegahan munculnya permasalahan yang sering terjadi dalam penelitian maka disusun beberapa batasan masalah yaitu:

1. Pada penelitian ini penulis memilih kata kunci yang memiliki karakter yang sama.
2. Pembangkitan kunci privat dan perhitungan modulo dalam algoritma RSA dilakukan dengan *software Microsoft Excel* dan *Python*.

1.6 Definisi Istilah

1. Enkripsi : Proses pengubahan bentuk pesan asli yang akan dikirim kepada penerima pesan menjadi suatu pesan rahasia yang tidak bisa terbaca oleh sembarang orang.
2. Dekripsi : Negasi dari proses enkripsi dengan mengembalikan pesan rahasia tersebut menjadi pesan yang asli seperti sebelum dikirimkan.
3. Modifikasi : Pengubahan dari bentuk semula menjadi bentuk yang baru.
4. Algoritma : Rangkaian proses yang digunakan untuk menyelesaikan atau menjalankan suatu proses masalah tertentu.
5. *Plaintext* : Teks asli yang merupakan input pada suatu proses enkripsi.
6. *Ciphertext* : Teks tersamar yang dihasilkan dari sebuah proses enkripsi.
7. *Cipherkey* : Kata kunci tersamar yang dihasilkan dari proses enkripsi.

8. Kriptanalisis : Ilmu untuk memecahkan kode yang telah diamankan dengan ilmu kriptografi.

1.7 Sistematika Penulisan

Sistematika pada penulisan ini digunakan untuk memudahkan dari segi pemahaman jalan pikiran secara keseluruhan dalam tugas akhir di sini dibagi menjadi lima bab, yakni:

Bab I Pendahuluan

Pada bab ini terdiri atas latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, definisi istilah, dan sistematika penulisan tugas akhir.

Bab II Kajian Teori

Pada bab ini diuraikan tentang konsep-konsep yang berisi teori-teori sebagai kerangka berfikir untuk menyelesaikan masalah dalam penelitian tugas akhir ini. Teori-teori tersebut diantaranya yaitu aritmatika modulo, keterbagian, bilangan prima, definisi kriptografi, algoritma *hybrid*, teknik transposisi, teorema sisa cina, teorema kecil fermat, algoritma *Myzkowski Cipher*, dan algoritma RSA.

Bab III Metode Penelitian

Bagian ini akan membahas tentang jenis penelitian, pra penelitian, dan tahapan penelitian.

Bab IV Hasil dan Pembahasan

Bagian hasil dan pembahasan ini akan menjelaskan dan menguraikan secara keseluruhan langkah-langkah yang disebutkan dalam metode penelitian dan menjawab rumusan masalah

Bab V Penutup

Pada bab ini berisi tentang kesimpulan dari hasil pembahasan sebelumnya dan saran- saran dalam penelitian selanjutnya.

BAB II

KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Aritmatika Modulo

Properti pembagian bilangan bulat menyebabkan konsep seperti angka bilangan prima dan aritmatika modulo. Aritmatika modulo memiliki peran penting dalam operasi bilangan bulat, terutama dalam bidang kriptografi. Aritmatika modulo menggunakan operator "mod". Operator "mod" akan menunjukkan sisa dari hasil pembagian (Ginting, 2010). Aritmatika modulo sering digunakan dalam ilmu kriptografi, hal ini bertujuan supaya setiap alfabet yang terenkripsi memiliki pasangan alfabet dalam lingkup huruf A-Z yang berjumlah 26 karakter.

Definisi 2.1:

Misalkan a, b dan $m > 1$ merupakan sebarang bilangan bulat. Maka a disebut kongruen b modulo m, atau dapat dirumuskan dengan

$$a \equiv b \ (mod\ m),$$

jika $m|(a - b)$; maka m **membagi** $a - b$ (Ling & Xing, 2004).

Teorema 2.1:

Untuk sembarang bilangan bulat a dan b maka $a \equiv b \ (modulo\ n)$ jika dan hanya jika a dan b memiliki sisa positif yang sama ketika dibagi oleh n (Ling & Xing, 2004).

Bukti:

Misalkan $a \equiv b(mod\ n)$, sehingga $a = b + kn$ untuk k suatu bilangan bulat, pembagian b oleh n, diperoleh sisa r dengan $b = qn + r$ dan $0 \leq r < n$. Selanjutnya diperoleh $a = b + kn = (qn + r) + kn = (q + k)n + r$. Ini menunjukkan bahwa a dan b memiliki sisa yang sama bila dibagi oleh n. Sebaliknya, misalkan a dan b memiliki sisa yang sama jika dibagi oleh n, yaitu $a = q_1n + r$ dan $b = q_2n + r$ dengan $0 \leq r < n$. Dengan demikian $a - b = (q_1n + r) - (q_2n + r) = (q_1 - q_2)n$ atau $n|a - b$ atau $a \equiv b\ (mod\ n)$.

Contoh 2.1:

1. $90 \equiv 30\ (mod\ 60)$ berarti 90 dibagi 60 adalah 1, sisa 30.
2. $15 \equiv 3\ (mod\ 12)$ berarti 15 dibagi 12 adalah 1, sisa 3.
3. $a \equiv 0\ (mod\ m)$ berarti $m|a$.
4. $a \equiv 0\ (mod\ 2)$ berarti a adalah genap.
5. $a \equiv 1\ (mod\ 2)$ berarti a adalah ganjil.

2.1.2 Keterbagian

Keterbagian bilangan bulat memiliki peranan penting sebagai dasar teori bilangan. Dasar teori bilangan yang berkaitan dengan pembagian akan dikembangkan menjadi operasi bilangan dengan tingkatan lebih tinggi. Berikut akan dibahas beberapa penjelasan singkat mengenai keterbagian.

Definisi 2.2:

Misal q adalah bilangan bulat, q dikatakan habis dibagi p yang merupakan suatu bilangan bulat tak nol jika ada suatu bilangan bulat x sehingga $q = px$.

Notasi dari keterbagian bilangan bulat dapat dituliskan sebagai berikut:

1. $p \mid q$ dibaca p membagi q, p faktor dari q, q habis dibagi p, atau q kelipatan dari p.
2. $p \nmid q$ dibaca p tidak membagi q, p bukan faktor dari q, q tidak habis dibagi p, atau q bukan kelipatan dari p (Suwanti & Fayeldi, 2019).

Teorema 2.2:

Misalkan $a, b, c \in \mathbb{Z}$ maka:

1. Jika $a|b$ maka $a|xb$ untuk setiap $x \in \mathbb{Z}, a \neq 0$
2. Jika $a|b$ dan $b|c$, maka $a|c$, $a \neq 0, b \neq 0$
3. Jika $a|b$ dan $a|c$, maka $a|b + c$, $a \neq 0, b \neq 0, c \neq 0$

Bukti:

1. Jika $a|b$ maka $a|xb$ untuk setiap $x \in \mathbb{Z}, a \neq 0$

$$a|b \rightarrow b = ka \rightarrow xb = (kx)a \rightarrow a|xb. \blacksquare$$

2. Jika $a|b$ dan $b|c$, maka $a|c$, $a \neq 0, b \neq 0$

$$a|b \; b = ka$$

$$b|c \; c = xb$$

Maka,

$$c = x(ka)$$

$$c = (kx)a \rightarrow a|c. \blacksquare$$

3. Jika $a|b$ dan $a|c$, maka $a|b + c$, $a \neq 0, b \neq 0, c \neq 0$

$$a|b \rightarrow b = ka$$

$$a|c \rightarrow c = xa$$

Maka,

$$b + c = ka + xa$$

$$b + c = (k + x)a \rightarrow a|b + c. \blacksquare$$

Contoh 2.2:

Akan ditunjukkan salah satu nilai n positif yang memenuhi $n|16$. Notasi $n|16$ dapat diartikan bahwa n habis membagi 16 atau 16 habis dibagi n dan n merupakan suatu faktor atau kelipatan dari 16. Adapun bilangan yang merupakan faktor dari 16 terdiri dari himpunan bilangan $\{1, 2, 4, 8, 16\}$ sehingga nilai n adalah salah satu dari anggota himpunan bilangan tersebut.

2.1.3 Bilangan Prima

Ada suatu bilangan bulat positif yang memiliki peran penting pada ilmu matematika yang disebut dengan bilangan prima. Bilangan prima merupakan bilangan bulat positif yang lebih besar dari 1 serta hanya akan habis dibagi 1 dan dirinya sendiri (Ginting, 2010). Sedangkan bilangan bulat positif yang bukan prima dinamakan dengan bilangan komposit yaitu suatu bilangan yang mempunyai lebih dari dua faktor prima (Puspita dkk., 2015). Bilangan prima akan diperlukan dalam proses pembangkitan kunci pada algoritma RSA.

Definisi 2.3:

Bilangan bulat positif p dengan $(p > 1)$ disebut suatu bilangan prima, jika pembaginya hanya 1 dan p.

Contoh 2.3:

Contoh dari bilangan prima yaitu $2, 3, 5, 7, 11, 13$, dst. Bilangan prima dimanfaatkan pada proses pembangkitan algoritma RSA karena bilangan prima dapat menjaga keamanan pesan yang terenkripsi, semakin besar bilangan prima

maka akan semakin tinggi tingkat kerumitan bagi kriptanalisis untuk mengartikan sebuah *ciphertext*.

Teorema 2.3:

Diberikan p suatu bilangan prima dengan $a, b \in \mathbb{Z}$ sedemikian sehingga $p|a + b$ dan $p|a$, maka $p|b$.

Bukti:

Akan dibuktikan bahwa $p|b$. $p|a + b$ berarti terdapat $n_1 \in \mathbb{Z}$ sedemikian sehingga $a + b = n_1.p$. Selanjutnya, $p|a$ berarti terdapat $n_2 \in \mathbb{Z}$ sehingga $a = n_2.p$. Kemudian substitusikan $a = n_2.p$ ke dalam persamaan $a + b = n_1.p$, maka diperoleh:

$$a + b = n_1.p$$

$$(n_2.p) + b = n_1.p$$

$$b = n_1.p - n_2.p$$

$$= (n_1 - n_2)p$$

$$= n.p, n \in \mathbb{Z}$$

$b = n.p$ sehingga dapat diartikan bahwa $p|b$.■

Definisi 2.4:

Dua bilangan bulat a dan b disebut relatif prima jika bilangan tersebut memenuhi $FPB(a, b) = 1$

Contoh 2.4:

1. 3 dan 5 merupakan bilangan yang relatif prima karena $FPB(3, 5) = 1$
2. 31 dan 120 merupakan bilangan yang relatif prima karena $FPB(31, 120) = 1$

Semua bilangan bulat positif yang kurang dari bilangan prima p akan relatif prima dengan p, misalkan bilangan 1, 2, 3, dan 4 akan relatif prima terhadap bilangan prima 5.

2.1.4 Kriptografi

Kriptografi berasal dari Bahasa Yunani yang terdiri dari dua kata yaitu *kripto* dan *graphia*. Secara etimologi *kripto* diartikan dengan rahasia dan *graphia* diartikan sebagai tulisan (Fachrurozi, 2006). Sehingga dapat diartikan kriptografi merupakan sebuah ilmu pengetahuan yang mengandung seni dan bertujuan untuk menjaga keamanan dari sebuah pesan.

Berdasarkan waktunya, ilmu kriptografi dibedakan menjadi 2 jenis yaitu ilmu kriptografi klasik dan ilmu kriptografi modern. Kriptografi klasik merupakan metode enkripsi dengan kunci simetris dan menghasilkan *ciphertext* dengan cara substitusi (pertukaran huruf) atau transposisi (perubahan letak huruf). Sedangkan kriptografi modern juga menggunakan konsep yang sama dengan kriptografi klasik (substitusi dan transposisi), akan tetapi terdapat berbedaan proses pada algoritma kriptografi modern yaitu memiliki tingkat kesulitan yang kompleks karena harus diproses melalui sebuah sistem atau *software* dalam komputer (Anggriani, 2019).

2.1.5 Algoritma *Hybrid*

Hybrid cryptosystem atau algoritma *hybrid*, secara umum memiliki konsep keamanan terhadap komunikasi *client* dan *server* dalam suatu jaringan internet dengan menggunakan kriptografi simetris. Peranan kriptografi asimetris, hanya ditujukan dalam *key exchange* (pertukaran kunci) dalam arti untuk menyepakati dan saling bertukar kunci rahasia yang akan dipakai saat berkomunikasi. Jadi pertukaran kunci rahasia dilakukan dalam keadaan terenkripsi dengan kriptografi asimetris

namun saat komunikasi menggunakan kriptografi simetris. Pada saat ini kriptografi algoritma *hybrid* digunakan secara luas dikarenakan menggabungkan keuntungan yang terdapat kepada kedua *cryptosystem* tersebut (Basri, 2015).

Tyagi mengatakan bahwa *Hybrid Cryptosystem* merupakan gabungan dari *asymmetric cryptosystem* dan *symmetric cryptosystem* dengan memanfaatkan kelebihan masing-masing algortima (Pangaribuan, 2018). Dalam penggunaan algoritma *hybrid*, teknik enkripsi yang digunakan adalah enkripsi simetri dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi (Jamaludin, 2018).

2.1.6 Teknik Transposisi

Teknik transposisi yaitu teknik yang menggunakan permutasi karakter (Wahyuni et al., 2021). Permutasi karakter ini merupakan perpindahan posisi tiap karakter atau bit *plaintext* dengan pola-pola yang telah ditentukan. Plaintext mengalami perubahan posisi karakter sehingga *plaintext* akan menjadi sulit dipecahkan.

Salah satu algoritma kriptografi klasik yang cukup populer adalah *transposition cipher*. Cipher transposisi ini memiliki berbagai macam bentuk dan algoritma, diantara contoh dari cipher transposisi ini adalah *Rail Fence Cipher*, *Route Cipher*, *Columnar Cipher* dan *Myszkowski Cipher* (Ekwardo, 2018).

2.1.7 Teorema Sisa Cina

Teorema Sisa Cina atau biasa disebut dengan *Chinese Remainder Theorem* (CRT) adalah suatu algoritma untuk menyelesaikan sebuah persoalan dengan menggunakan prinsip kongruensi modulo atau sisa pembagian (Tao, 2019).

Teorema ini digeneralisasi di dalam aljabar abstrak yang dipublikasikan dalam abad ke-3 hingga abad ke-5 oleh seorang matematikawan dari Cina yang bernama Sun Tzu. Teorema Sisa Cina memiliki relevansi pada proses enkripsi dan dekripsi dalam kriptografi algoritma RSA untuk mengubah *plaintext* yang semula berbentuk alfabet menjadi numerik.

Teorema 2.4:

Misalkan p dan q adalah dua bilangan yang relatif prima. Jika $x = a\ (mod\ p)$ dan $x = a\ (mod\ q)$, maka $x = a\ (mod\ pq)$.

Bukti:

Misalkan $b = x\ (mod\ pq)$. Kita akan membuktikan bahwa $b = a$ dengan catatan $b < pq$. Karena $x = a\ (mod\ p)$, kita tahu bahwa $b = a\ (mod\ p)$. Sama halnya dengan $b = a\ (mod\ q)$. Maka dapat kita peroleh $b = pt_1 + a\ = qt_2 + a$ untuk bilangan bulat t_1, t_2. Ini berarti bahwa $pt_1 = qt_2$, dan terdapat perkalian p dan q, dimana p dan q adalah relatif prima dan tidak sama dengan nol sehingga hasil perkalian dari p dan q adala pq. Diberikan $b < pq$ maka dapat disimpulkan bahwa $pt_1 = qt_2 = 0$.■

Contoh 2.5:

Karena $37 = 2\ (mod\ 5)$ dan $37 = 2\ (mod\ 7)$ maka diperoleh $37 = 2\ (mod\ (7)(5))$ yaitu $37 = 2\ (mod\ 35)$.

2.1.8 Teorema Kecil Fermat

Teorema Kecil Fermat (*Fermat's Little Theorem*) adalah teori dasar untuk menguji keprimaan suatu bilangan yang ditemukan oleh matematikawan bernama Pierre De Fermat dari Prancis pada tahun 1640 (Tao, 2019).Teorema ini disebut teorema kecil untuk membedakannya dengan Teorema Terakhir Fermat (*Fermat's*

Last Theorem). Teorema Kecil Fermat digunakan pada pembuktian formula dekripsi pada algoritma RSA.

Teorema 2.5:

Untuk sebuah bilangan prima p dan sebarang bilangan bulat a maka p selalu membagi $(a^p - a)$, atau dapat dituliskan dengan:

$$p|a^p - a \longrightarrow (a^p - a) \equiv 0(mod\ p) \rightarrow a^p \equiv a\ mod\ p\ \rightarrow a^{p-1} \equiv 1\ mod\ p.$$

Bukti:

Misalkan diberikan kumpulan dari $p - 1$ yang merupakan kelipatan pertama dari a dengan himpunan V, sehingga:

$$V\ =\ \{a, 2a, 3a, \dots, p - 1(a)\}$$

Maka, setiap anggota V pasti kongruen modulo p terhadap salah satu $1, 2, 3, \dots, p - 1$. Kalikan semua kongruensi ini sehingga diperoleh:

$$a, 2a, 3a, \dots, (p-1)a \equiv 1, 2, 3, \dots, (p-1)(mod\ p)$$

$$a^{p-1}(p-1)! \equiv (p-1)!\,(mod\ p)$$

$$a^{p-1} \quad \equiv 1(mod\ p). \blacksquare$$

Contoh 2.6:

$$2^{5-1} \equiv 1\ mod\ 5$$

$$2^4\ \equiv 1\ mod\ 5$$

$$16\ \equiv 1\ mod\ 5$$

2.1.9 Algoritma *Myzskowski Cipher*

Algoritma *Myszkowski Cipher* merupakan cipher transposisi yang diciptakan oleh Émile Victor Théodore Myszkowski pada tahun 1902, pada proses enkripsinya algortima *Myszkowski Cipher* memerlukan kata kunci yang memiliki huruf berulang di dalamnya. Hal ini akan berpengaruh pada penomoran kata kunci karena

kemunculan dari huruf selanjutnya pada kata kunci diperlakukan seolah-olah urutan abjad, misalnya kata kunci TOMAT menghasilkan penomoran numerik "43214" karena huruf pertama dalam abjad adalah A sehingga menjadi urutan 1, kemudian huruf kedua pada abjad yang terdapat dalam kata kunci tersebut adalah huruf M sehingga menjadi urutan nomor 2 dan seterusnya sehingga T mendapatkan urutan terakhir yaitu nomor 4. Pada kata kunci yang memiliki huruf yang sama akan diberi penomoran yang sama sehingga algoritma *Myszkowski* berbeda dengan algoritma transposisi yang lainnya.

Contoh proses enkripsi menggunakan algoritma *Myszkowski Cipher* pada *plaintext* "KRIPTOGRAFI MODERN" dengan kata kunci "TOMAT" yaitu sebagai berikut:

Tabel 2.1 Proses Enkripsi *Myzskowski Cipher*

T	O	M	A	T
4	*3*	*2*	*1*	*4*
K	R	I	P	T
O	G	R	A	F
I	M	O	D	E
R	N	X	X	X

Plaintext ditulis secara horizontal pada kolom yang sesuai dengan banyaknya kata kunci, karena kalimat pada *plaintext* belum memenuhi kolom yang tersedia maka ditambahkan huruf X pada akhir kalimat untuk mempermudah proses enkripsi pesan. Setelah kalimat *plaintext* memenuhi baris dan kolom yang telah disediakan maka pembacaan *ciphertext* dilakukan dengan arah vertikal dari atas kemudian urut ke bawah berdasarkan dengan urutan nomor terkecil ke terbesar dalam penomoran huruf pada kata kunci, sedangkan pada huruf kata kunci yang

memiliki penomoran yang sama *ciphertext* dibaca secara horizontal ke kanan kemudian urut kebawah. Oleh karena itu diperoleh *ciphertext* sebagai berikut:

Tabel 2.2 Proses Penulisan *Ciphertext Myzskowski Cipher*

No.	**Huruf**	***Ciphertext***
1	A	PADX
2	M	IROX
3	O	RGMN
4	T	KTOFIERX
		PADXIROXRGMNKTOFIERX

Sehingga diperoleh *ciphertext* "PADXIROXRGMNKTOFIERX" yang berjumlah sebanyak 20 karakter. Proses dekripsi untuk pesan teks yang telah terenkripsi dapat dilakukan dengan membagi jumlah karakter huruf pada pesan teks yang dienkripsi dengan jumlah karakter huruf yang dipakai dalam kata kunci dan hasilnya digunakan dalam penentuan banyak baris yang akan disusun dengan *ciphertext* dalam contoh kasus di penelitian ini yaitu:

$$\frac{\sum karakter\ ciphertext}{\sum karakter\ kata\ kunci} = \frac{20}{5} = 4$$

Sehingga banyak baris yang harus disediakan yaitu sebanyak 4 baris ke bawah, sedangkan jumlah kolom mengikuti jumlah karakter kata kunci yang digunakan yaitu sebanyak 5 kolom, kemudian urutkan *ciphertext* "PADXIROXRGMNKTOFIERX" berdasarkan kunci terkecil ke kunci yang terbesar dengan menggunakan kata kunci "TOMAT" dan *ciphertext* ditulis secara vertikal pada Tabel 2.3.

Tabel 2.3 Dekripsi Kunci Pertama

T	**O**	**M**	**A**	**T**
4	*3*	*2*	*1*	*4*
			P	
			A	
			D	
			X	

Tabel 2.4 Dekripsi Kunci Kedua

T	**O**	**M**	**A**	**T**
4	*3*	*2*	*1*	*4*
		I	P	
		R	A	
		O	D	
		X	X	

Tabel 2.5 Dekripsi Kunci Ketiga

T	**O**	**M**	**A**	**T**
4	*3*	*2*	*1*	*4*
	R	I	P	
	G	R	A	
	M	O	D	
	N	X	X	

Tabel 2.6 Dekripsi Kunci Keempat

T	**O**	**M**	**A**	**T**
4	*3*	*2*	*1*	*4*
K	R	I	P	**T**
O	G	R	A	**F**
I	M	O	D	**E**
R	N	X	X	**X**

Kemudian pembacaan *plaintext* dilakukan secara horizontal dari kolom pertama ke kolom terakhir dan menghilangkan huruf X di akhir kalimat, sehingga diperoleh *plaintext* "KRIPTOGRAFI MODERN".

2.1.10 Algoritma RSA

RSA adalah sebuah algoritma kriptografi asimetris. RSA merupakan algoritma pertama yang cocok untuk *digital signature* seperti halnya enkripsi, dan salah satu yang paling maju dalam bidang kriptografi dengan kunci asimetris. RSA memanfaatkan kunci yang berbeda ketika melakukan enkripsi dan dekripsi. Kunci yang diperlukan ketika mengenkripsi pesan dinamakan dengan kunci publik, sedangkan kunci yang dimanfaatkan ketika mendekripsi pesan adalah kunci privat. Pengirim memiliki kunci publik sehingga bisa melakukan enkripsi sedangkan penerima dalam melakukan dekripsi pesan akan menggunakan kunci privat yang telah dikirimkan oleh pengirim. Kunci publik bisa dimiliki oleh siapa saja, akan tetapi kunci privat hanya bisa dimiliki penerima pesan saja sehingga pihak ketiga tidak berhak mengetahuinya (Rahajoeningroem & Aria, 2011).

Proses pertama yang harus dilakukan dalam mengenkripsi sebuah pesan teks pada algoritma RSA yaitu pembangitan kunci, proses pembangkitan kunci publik dan kunci privat dalam algoritma RSA melalui beberapa proses sebagai berikut:

1. Pilih dua buah bilangan prima yang besar supaya lebih susah dipecahkan dan tulis sebagai p dan q. Kemudian nilai dari p dan q harus dirahasiakan.
2. Tentukan nilai dari

$$N = p\ x\ q \qquad (i)$$

   Hasil dari nilai n tidak perlu dirahasiakan.

3. Tentukan nilai dari

$$\phi(N) = (p - 1)(q - 1) \qquad (ii)$$

4. Ambil sebarang bilangan bulat positif untuk dijadikan kunci publik yang akan dituliskan sebagai e, bilangan yang dipilih haruslah yang relatif prima terhadap $\phi(N)$ dan nilai $1 < e < \phi(N)$. Sehingga e relatif prima terhadap $\phi(N)$, yang berarti bahwa faktor pembagi terbesar keduanya adalah 1 atau dapat dituliskan dengan

$$gcd(e, \phi(N)) = 1 \qquad (iii)$$

Untuk menentukan nilai tersebut dapat menggunakan metode faktorisasi prima atau pohon faktor.

5. Tentukan kunci privat yang disimbolkan dengan d yang memenuhi persyaratan sebagai berikut

$$(e.d)\ mod\ \phi(N) = 1 \qquad (iv)$$

6. Untuk menentukan nilai d yang sesuai dengan persamaan tersebut dapat digunakan suatu *software Microsoft Excel* dengan formula:

"=$(kolom\ data\ (e.d))mod(nilai\ dari\ \phi(N))$".

Sehingga diperoleh pasangan kunci berikut:

1. Kunci Publik adalah pasangan dari (e, N) (v)
2. Kunci Privat adalah pasangan dari (d, N) (vi)
3. Nilai N tidak bersifat rahasia, namun nilai N digunakan saat proses enkripsi/dekripsi pesan oleh pengirim maupun penerima pesan.

Rumus yang digunakan dalam enkripsi pesan RSA yaitu:

$$C = M^e\ mod\ N \qquad (vii)$$

Sedangkan rumus dekripsi pada algoritma RSA yaitu:

$$P = C^d \bmod N \qquad (viii)$$

Teorema 2.6:

Proses dekripsi algoritma RSA dinyatakan dengan $P = C^d \bmod N$. (Tao, 2019)

Bukti:

Cukup dengan membuktikan $P = C^d \ (mod\ p)$ dan $P = C^d \ (mod\ q)$, karena keduanya menghasilkan $P = C^d \bmod N$ berdasarkan Teorema Sisa Cina. Pertama, kita buktikan $P = C^d \ (mod\ p)$. Dari $C = M^e \bmod N$, kita tahu bahwa $C = M^e \ (mod\ p)$, dan karenanya $C^d = M^{ed} \ (mod\ p)$.

Karena $ed = 1 \ (mod\ (p-1)(q-1))$ kita peroleh $ed = t(p-1)(q-1) + 1$ untuk sebarang bilangan bulat t. Oleh karena itu:

$$\begin{aligned} M^{ed} &= M \,.\, M^{t(p-1)(q-1)} \ (mod\ p) \\ &= M \,.\, \left(M^{(p-1)}\right)^{t(q-1)} \ (mod\ p) \\ &= M \,.\, (1)^{t(q-1)} (mod\ p) \text{ “Teorema Kecil Fermat”} \\ &= M \ (mod\ p) \end{aligned}$$

Dengan sifat simetri, maka $M^{ed} = M \ (mod\ q)$ juga terbukti. ■ Sehingga dapat disimpulkan bahwa formula dekripsi RSA dituliskan dengan:

$$P = C^d \bmod N = (M^e)^d \bmod N = M^{ed} \bmod N.$$

Contoh proses enkripsi atau pengamanan pesan teks yang akan dikirim dengan menerapkan algoritma RSA yaitu sebagai berikut:

1. Penentuan *plaintext* yang akan dikirimkan

   Misalkan *plaintext* yang akan dikirimkan yaitu “KRIPTOGRAFI MODERN” selanjutnya akan ditentukan kunci pada algoritma asimetris RSA.

2. Proses pembangkitan kunci pada algoritma RSA

   Untuk menentukan kunci publik ambil sebarang bilangan prima p dan q, misalkan $p = 51$ dan $q = 5$. Kemudian menggunakan persamaan (i) ditentukan nilai dari:

   $$N = p\ x\ q$$

   $$N = 51\ x\ 5$$

   $$N = 255$$

   Setelah diperoleh nilai N, selanjutnya akan ditentukan nilai dari $\phi(N)$ menggunakan persamaan (ii) sebagai berikut:

   $$\phi(N) = (p - 1)(q - 1)$$

   $$\phi(N) = (51 - 1)(5 - 1)$$

   $$\phi(N) = (50)(4)$$

   $$\phi(N) = 200$$

   Kemudian, pilih sebarang bilangan prima e yang relatif prima dengan $\phi(N)$ atau dapat dituliskan seperti persamaan (iii) yang memenuhi syarat $1 < e < \phi(N)$. Misalkan diambil nilai $e = 7$ dimana

   $$gcd(7, 200) = 1$$

   Sehingga dapat ditentukan kunci privat d dengan menggunakan persamaan (iv) yaitu:

$$(e.d) mod\ \phi(N) \ = 1$$

$$(7.d)\ mod\ 200 \ = 1$$

Dengan menggunakan *software Microsoft Excel* diperoleh nilai d yang memenuhi persamaan tersebut adalah sebagai berikut:

Tabel 2.7 Penentuan Nilai Kunci Privat *d*

$\boldsymbol{e}$	$\boldsymbol{d}$	$(\boldsymbol{e.d})$	$(\boldsymbol{e.d})\ \boldsymbol{mod}\ \mathbf{200}$
7	1	7	7
7	2	14	14
7	3	21	21
⋮	⋮	⋮	⋮
7	342	2394	194
7	343	2401	**1**

Maka nilai d yang memenuhi persamaan (iv) yaitu $d = 343$.

Sehingga berdasarkan persamaan (v) telah diperoleh kunci publik

$$(e, N) \ = \ (7, 255)$$

dan berdaasarkan persamaan (vi) diperoleh kunci privat

$$(d, N) \ = \ (343, 255)$$

3. Proses enkripsi pesan teks algoritma RSA

   Menggunakan persamaan $(viii)$ maka pesan dienkripsi sebagai berikut:

   Plaintext : KRIPTOGRAFI MODERN

   Kunci Publik : $(7, 255)$

$$C = M^e\ mod\ N$$

$$C = M^7\ mod\ 255$$

Tabel 2.8 Proses Enkripsi Algoritma RSA dengan ASCII

Plaintext	$\boldsymbol{M}$	$\boldsymbol{M^7\ mod\ 255}$	**Hasil *Ciphertext***
K	75	$75^7\ mod\ 255$	165

R	82	$82^7 \ mod \ 255$	193
I	73	$73^7 \ mod \ 255$	112
P	80	$80^7 \ mod \ 255$	245
T	84	$84^7 \ mod \ 255$	84
O	79	$79^7 \ mod \ 255$	139
G	71	$71^7 \ mod \ 255$	11
R	82	$82^7 \ mod \ 255$	193
A	65	$65^7 \ mod \ 255$	125
F	70	$70^7 \ mod \ 255$	145
I	73	$73^7 \ mod \ 255$	112
M	77	$77^7 \ mod \ 255$	53
O	79	$79^7 \ mod \ 255$	139
D	68	$68^7 \ mod \ 255$	17
E	69	$69^7 \ mod \ 255$	69
R	82	$82^7 \ mod \ 255$	193
N	78	$78^7 \ mod \ 255$	192

Dengan menggunakan *python* dan rumus untuk menentukan *ciphertext* yang berupa numerik pada algoritma RSA maka diperoleh hasil *ciphertext* [165 193 112 245 84 139 11 193 125 145 112 53 139 17 69 193 192]. Proses pengembalian *ciphertext* ke *plaintext* (dekripsi) dari algoritma RSA bisa dilakukan dengan memanfaatkan kunci privat yang telah didapatkan, dalam contoh kasus di penelitian ini yaitu

$$(d, N) \ = \ (343, 255)$$

Sehingga proses dekripsi pesan teks menggunakan persamaan $(viii)$ dapat dilakukan sebagai berikut:

$$P \ = \ C^d \ mod \ N$$

$$P = C^{343} \, mod \, 255$$

Dengan menggunakan *software python* untuk menentukan hasil, maka diperoleh:

Tabel 2.9 Proses Dekripsi Algoritma RSA dengan ASCII

Ciphertext	$C^{343} \, mod \, 255$	**Hasil**	***Plaintext***
165	$165^{343} \, mod \, 255$	75	K
193	$193^{343} \, mod \, 255$	82	R
112	$112^{343} \, mod \, 255$	73	I
245	$245^{343} \, mod \, 255$	80	P
84	$84^{343} \, mod \, 255$	84	T
139	$139^{343} \, mod \, 255$	79	O
11	$11^{343} \, mod \, 255$	71	G
193	$193^{343} \, mod \, 255$	82	R
125	$125^{343} \, mod \, 255$	65	A
145	$145^{343} \, mod \, 255$	70	F
112	$112^{343} \, mod \, 255$	73	I
53	$53^{343} \, mod \, 255$	77	M
139	$139^{343} \, mod \, 255$	79	O
17	$17^{343} \, mod \, 255$	68	D
69	$69^{343} \, mod \, 255$	69	E
193	$193^{343} \, mod \, 255$	82	R
192	$192^{343} \, mod \, 255$	78	N

Sehingga *ciphertext* berhasil kembali pada pesan semula yang diinput pada proses enkripsi algoritma RSA yaitu *plaintext:*

P = “KRIPTOGRAFI MODERN”.

2.2 Kajian Integrasi Topik dengan Alqur’an/Hadits

Firman Allah pada Alqur’an surah Al–Baqarah ayat 1 yang berbunyi: (Kemenag, 2019)

"Alif Lām Mīm."

Para ahli tafsir memiliki pendapat yang berbeda mengenai potongan huruf yang terdapat pada beberapa surat dalam Alqur'an. Diantaranya ada yang berpendapat bahwa itu adalah huruf-huruf yang hanya Allah yang tau maknanya, sehingga mengembalikan ilmu mengenai hal itu kepada Allah dan tidak menafsirkannya. Pendapat ini dinukil Al-Qurthubi dalam tafsirnya dari Abu Bakar, Umar, Utsman, 'Ali, dan Ibnu Mas'ud R.A. Sebagian ulama' meringkas masalah tersebut dengan menyatakan: "Tidak diragukan lagi bahwa huruf-huruf ini tidak diturunkan oleh Allah dengan sia-sia dan tanpa makna" dan para ulama sendiri belum memiliki kesepakatan mengenai huruf-huruf tersebut. Barangsiapa yang menemukan pendapat yang didasarkan pada dalil yang kuat, maka hendaklah ia mengikutinya, jika tidak maka hendaklah ia menyerahkan maknanya kepada Allah hingga diperoleh kejelasan mengenai hal itu (Katsir, 2015).

Alqur'an surah Al–Baqarah ayat 1 secara tak langsung juga mengajarkan kepada manusia tentang mengamankan sebuah pesan, karena pada ayat tersebut hanya orang tertentu saja yang dapat mengartikan dan menerjemahkan makna yang terkandung di dalamnya. Begitupun dalam kriptografi, pesan yang dienkripsi tidak dirahasiakan dan dapat dibaca oleh semua orang namun hanya pihak yang mendapatkan kunci dekripsinya saja yang dapat mengartikan isi pesan tersebut.

2.3 Kajian Topik dengan Teori Pendukung

Dalam penelitian ini terdapat beberapa teori pendukung untuk membantu dalam menyelesaikan permasalahan yang ada pada penelitian ini. Teori yang digunakan dalam pembangkitan kunci pada algoritma RSA diantaranya yaitu

aritmatika modulo, keterbagian dan bilangan prima. Pada algoritma *Myszkowski Cipher* memerlukan teori tentang teknik transposisi karena *Myszkowski Cipher* tidak memerlukan perhitungan khusus dalam melakukan enkripsi dan dekripsinya.

Setelah itu terdapat teori mengenai algoritma *hybrid* yang akan digunakan dalam topik utama pembahasan penelitian ini yaitu algoritma yang akan menggabungkan *Myszkowski Cipher* dan RSA. Terdapat pula beberapa teorema sebagai pembuktian rumus algoritma RSA serta contoh proses enkripsi dan dekripsi pada masing-masing algoritma sebagai gambaran awal permasalahan yang akan diselesaikan dalam penelitian. Dalam penelitian ini akan dijelaskan simulasi enkripsi dan dekripsi pesan dengan algoritma *hybrid* menggunakan *Myzkowski Cipher* dan RSA melalui proses berikut ini:

1. Menentukan *plaintext* dan kunci untuk dienkripsi menggunakan algoritma *Myszkowski Cipher.*
2. Setelah mendapatkan *ciphertext* hasil enkripsi dari algoritma *Myszkowski Cipher*, kemudian mengenkripsi kata kunci dengan algoritma RSA dengan menggunakan persamaan (vii).
3. Dalam mengenkripsi kata kunci pada algoritma *Myszkowski Cipher* menggunakan algoritma RSA kita perlu membangkitkan kunci publik (v) dan kunci privat (vi) terlebih dahulu sesuai dengan (Definisi 2.3) mengenai bilangan prima dan (Definisi 2.4) tentang relatif prima suatu bilangan.
4. Kemudian mengenkripsi kata kunci pada algoritma *Myszkowski Cipher* dengan memanfaatkan kunci publik (v) yang sudah ditetapkan pada algoritma RSA dengan persamaan (vii) yang akan menghasilkan *cipherkey* berbentuk angka.

5. Selanjutnya pengirim akan membagikan kunci privat (vi) kepada penerima pesan untuk proses dekripsi kata kunci yang terenkripsi.
6. Setelah kunci privat didapatkan, kata kunci dapat didekripsi dengan persamaan $(viii)$ algoritma RSA untuk mendapatkan kata kunci berbentuk huruf yang digunakan dalam algoritma *Myszkowski Cipher*.
7. Kemudian melakukan dekripsi pada pesan teks yang terenkripsi menggunakan kata kunci dalam algoritma *Myszkowski Cipher* yang telah didekripsi dari algoritma RSA sehingga diperoleh *plaintext* dari pesan yang dikirimkan.
8. Mendapatkan *plaintext* dari pesan teks yang dikirimkan.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Jenis penelitian ini adalah penelitian kualitatif karena berfokus pada pemahaman yang mendalam, pengembangan algoritma *hybrid* menggunakan *Myzkowski Cipher* dan algoritma RSA dimana peneliti sebagai instrumen penelitian serta menggunakan studi kepustakaan untuk menambah pemahaman teori yang akan dikembangkan. Definisi dari studi kepustakaan yaitu segala upaya oleh peneliti ketika mengumpulkan informasi yang berkaitan dengan topik dan permasalahan yang akan dibahas dalam penelitian. Informasi tersebut bisa didapatkan penulis dari buku akademik, laporan suatu penelitian, artikel ilmiah, tesis, disertasi, ensiklopedia dan sumber tertulis lainnya baik cetak ataupun elektronik (Purwono, 2008). Pada penelitian ini penulis mengumpulkan dan mengkaji materi yang relevan dengan algoritma *hybrid* dengan algoritma RSA dan *Myszkowski Cipher* dari jurnal, tugas akhir dan artikel ilmiah.

3.2 Pra Penelitian

Peneliti melakukan pengkajian kepustakaan untuk memperoleh sketsa awal mengenai penelitian mengenai algoritma *hybrid Myszkowski Cipher* dan RSA. Kemudian peneliti menyatukan materi dari beberapa referensi dan teori dari beberapa referensi itu akan digunakan dalam bab pembahasan dari hasil penelitian. Tahap selanjutnya adalah menentukan judul yang sesuai dengan penelitian yaitu algoritma *hybrid Myszkowski Cipher* dan RSA untuk mengamankan pesan teks.

3.3 Tahapan Penelitian

Terdapat beberapa langkah dalam tahapan penelitian yang dilakukan diantaranya yaitu:

1. Penentuan algoritma yang sesuai untuk diterapkan pada proses enkripsi dan dekripsi pesan secara *hybrid*. Berdasarkan latar belakang dari penelitian ini maka akan digunakan suatu kombinasi *hybrid Myszkowski Cipher* dan algoritma RSA (*Rivest, Shamir, Adleman*) untuk pengamanan pesan teks.
2. Mengkombinasikan kedua algoritma secara *hybrid* dengan mengenkripsi kata kunci yang digunakan pada *Myszkowski Cipher* dengan algoritma RSA menggunakan proses pembangkitan kunci dengan memanfaatkan bilangan prima sesuai (Definisi 2.3) sehingga kata kunci yang semula berbentuk alfabet setelah dienkripsi dengan RSA menjadi berbentuk angka melalui proses dekrispsi menggunakan (Teorema 2.6).
3. Melakukan simulasi algoritma *hybrid* dengan menggunakan *Myszkowski Cipher* dan algoritma RSA.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Proses Enkripsi Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA

Algoritma *Myszkowski Cipher* merupakan salah satu jenis algoritma tranposisi cipher yang memiliki keunikan tersendiri. Pada proses enkripsi, *plaintext* ditulis secara horizontal dari kiri ke kanan, kemudian *ciphertext* dibaca secara vertikal sesuai dengan urutan kunci (Khairina, 2019). Untuk melakukan enkripsi dengan algoritma *Myszkowski Cipher* harus ditentukan kata kunci terlebih dahulu, kata kunci yang digunakan sebaiknya memiliki huruf yang berulang seperti "MATEMATIKA" yang terdapat perulangan huruf M, A, dan T yang akan memperkuat hasil enkripsi karena untuk huruf yang sama akan diberi penomoran yang sama dan penulisan *ciphertext* dilakukan secara horizontal dari kiri ke kanan pada nomor yang sama.

Algoritma RSA membutuhkan dua kunci yang berbeda pada proses enkripsi dan dekripsi nya sehingga proses enkripsi dan dekripsi hanya dapat dilakukan oleh pihak yang memiliki kunci yang sesuai. Secara garis besar algoritma RSA menggunakan tiga tahapan untuk mengamankan pesan teks yaitu pembangkitan kunci, proses enkripsi pesan teks dan yang terakhir yaitu proses dekripsi pesan teks. Pembangkitan kunci merupakan suatu tahapan untuk menghasilkan dua buah kunci yang berbeda yaitu kunci privat yang digunakan untuk mendekripsi pesan dan kunci publik yang digunakan untuk mengenkripsi pesan teks yang dikirimkan oleh pihak pengirim pesan kepada pihak penerima pesan tersebut (Safarina, 2017).

Berikut akan dijelaskan tentang enkripsi algoritma *Hybrid*.

Algoritma *Hybrid Myzskowski Cipher* dan RSA untuk Enkripsi

1. Memberikan penomoran pada kata kunci yang digunakan oleh algoritma *Myszkowski Cipher*.
2. Membuat kolom dengan ukuran sesuai banyak karakter kata kunci.
3. Menentukan jumlah baris yang harus dibuat yaitu dengan persamaan

$$\frac{\sum karakter\ ciphertext}{\sum karakter\ kata\ kunci} = \sum baris$$

4. Menuliskan *plaintext* pesan teks secara horizontal dari kiri ke kanan.
5. *Ciphertext* dibaca secara vertikal berdasarkan urutan kata kunci terkecil, untuk kata kunci yang memiliki penomoran sama maka *ciphertext* dibaca secara horizontal kemudian vertikal.
6. Selanjutnya kata kunci pada algoritma *Myzskowski Cipher* yang semula berbentuk alfabet akan dienkripsi dengan RSA supaya menjadi bentuk numerik, langkah pertama yaitu menentukan nilai p dan q dengan bilangan prima yang berbeda.
7. Setelah nilai p dan q ditentukan, akan didapatkan nilai N yang merupakan hasil kali dari p dan q sesuai dengan persamaan (i).
8. Kemudian menentukan nilai dari $\phi(N)$ dengan menggunakan persamaan (ii).
9. Selanjutnya adalah memilih sebarang bilangan untuk kunci publik atau nilai e yang relatif prima terhadap $\phi(N)$ dan nilai $1 < e < \phi(N)$. Karena e relatif prima terhadap $\phi(N)$, maka faktor pembagi terbesar keduanya adalah 1 atau dapat dituliskan dengan $gcd(e, \phi(N)) = 1$ pada persamaan (iii).

10. Setelah nilai e diperoleh, maka akan ditentukan kunci privat yang disimbolkan dengan d yang memenuhi syarat sesuai dengan persamaan ke (iv) yaitu $(e.d)\ mod\ \phi(N)\ =\ 1$. Maka diperoleh pasangan kunci publik dan kunci privat yang dapat dituliskan dengan (e, N) untuk kunci publik dan (d, N) untuk kunci privat berdasarkan pada persamaan (v) dan (vi).
11. Setelah semua langkah terpenuhi, dapat dilakukan enkripsi pada kata kunci yang digunakan pada algoritma *Myzskowski Cipher* dengan persamaan $(vii)\ C = M^e\ mod\ N$.

4.1.1 Simulasi Enkripsi Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA

Pada proses enkripsi pesan teks dalam penelitian ini akan digunakan data sebagai berikut:

Plaintext : TAHUN INI SIDANG SKRIPSI DAN LULUS

Kunci : MATEMATIKA

Untuk melakukan enkripsi algoritma *Hybrid* menggunakan *Myszkowski Cipher* dan RSA perlu dilakukan dua tahapan. Tahapan yang pertama yaitu mengenkripsi pesan menggunakan algoritma *Myszkowski Cipher*, kemudian kunci yang digunakan dalam mengenkripsi pesan pada algoritma *Myzskowski Cipher* dienkripsi menggunakan algoritma RSA. Proses tersebut dilakukan supaya kata kunci yang semula berbentuk alfabet pada algoritma *Myszkowski Cipher* berubah menjadi bentuk numerik dengan enkripsi algoritma RSA. Berikut ini akan dijelaskan proses enkripsi pesan teks pada algoritma *Hybrid* menggunakan *Myszkowski Cipher* dan RSA.

4.1.2 Proses Enkripsi Pesan Teks

Proses enkripsi dapat dilakukan dengan cara menulis pesan teks secara horizontal dalam kolom dan baris yang telah disesuaikan dengan banyaknya karakter kunci seperti pada tabel berikut:

Tabel 4.10 Proses Enkripsi *Myszkowski Cipher*

M	**A**	**T**	**E**	**M**	**A**	**T**	**I**	**K**	**A**
5	**1**	**6**	**2**	**5**	**1**	**6**	**3**	**4**	**1**
T	A	H	U	N	I	N	I	S	I
D	A	N	G	S	K	R	I	P	S
I	D	A	N	L	U	L	U	S	X

Pada akhir kalimat dilakukan penambahan huruf X sebagai pelengkap pada kolom tabel enkripsi yang kosong sehingga dapat memudahkan dalam pembacaan *ciphertext* saat dilakukan proses enkripsi tahap pertama pesan teks pada algoritma *Myszkowski Cipher* ini. Pembacaan *ciphertext* dari tabel tersebut dilakukan secara vertikal dari atas ke bawah berdasarkan dari urutan penomoran karakter pada kata kunci yang paling kecil, sedangkan untuk karakter yang memiliki penomoran yang sama pembacaan *ciphertext* dilakukan secara horizontal dari kiri ke kanan kemudian sampai pada kolom yang paling bawah. Sehingga berdasarkan tabel tersebut diperoleh hasil *ciphertext* yaitu AIIAKSDUX UGN IIU SPS TNDSIL HNNRAL.

4.1.3 Proses Enkripsi Kunci

Pada proses enkripsi tahap kedua menggunakan algoritma RSA akan dilakukan enkripsi pada kata kunci yang telah digunakan pada algoritma *Myszkowski Cipher* sebelumnya, sehingga kata kunci MATEMATIKA yang semula berbentuk alfabet akan dienkripsi dengan algoritma RSA yang

menghasilkan *cipherkey* dalam bentuk numerik. Pada proses enkripsinya, algoritma RSA dilakukan melalui beberapa proses yaitu sebagai berikut:

1. Menentukan nilai p dan q

   Dalam penelitian ini akan mengambil dua bilangan prima yang berbeda sebagai nilai p dan q yang dituliskan sebagai:

   $$p = 47$$

   $$q = 23$$

2. Menentukan nilai N

   Nilai N akan diperoleh dari hasil kali nilai p dan q sesuai pada persamaan (i) yaitu:

   $$N = p.q$$

   $$N = 47.23$$

   $$N = 1081$$

   Sehingga diperoleh nilai N yang akan digunakan untuk pasangan dari kunci publik dan kunci privat.

3. Menentukan $\phi(N)$

   $$\phi(N) = (p-1)(q-1)$$

   $$\phi(N) = 46.22$$

   $$\phi(N) = 1012$$

4. Menentukan kunci publik e

   $$1 < e < \phi(N)$$

   Ambil $e = 17$ maka,

   $$GCD(e, \phi(N)) = 1$$

   $$GCD(17{,}1012) = 1$$

Lakukan pengecekan bahwa $GCD(17{,}1012) = 1$ dengan metode Euclid:

$$1012 \; mod \; 17 = 9$$

$$17 \; mod \; 9 = 8$$

$$9 \; mod \; 8 = 1$$

$$8 \; mod \; 1 = 0$$

sehingga $e = 17$ memenuhi syarat tersebut.

5. Menentukan kunci privat d

$$e.d \; mod \; \phi(N) = 1$$

Tabel 4.11 Penentuan Kunci Privat *d*

$\boldsymbol{e.d}$	$\boldsymbol{e.d \; mod \; \phi(N)}$
17.1 = 17	17 mod 1012 = 17
17.2 = 34	34 mod 1012 = 34
17.3 = 51	51 mod 1012 = 51
⋮	⋮
17.893 = 15181	15181 mod 1012 = 1

kunci publik $(e, N) = (17, 1081)$ dan kunci privat $(d, N) = (893, 1081)$.

Enkripsi kunci *Myszcowski Cipher* dengan algoritma RSA:

$$C = M^e \; mod \; N$$

$$C = M^{17} \; mod \; 1081$$

$$P \; = \; MATEMATIKA$$

Perhitungan *ciphertext* RSA berdasarkan ASCII menggunakan *Python*:

$$C = 77^{17}\ mod\ 1081 = 151$$

$$C = 65^{17}\ mod\ 1081 = 849$$

$$C = 84^{17}\ mod\ 1081 = 700$$

$$C = 69^{17}\ mod\ 1081 = 483$$

$$C = 77^{17}\ mod\ 1081 = 151$$

$$C = 65^{17}\ mod\ 1081 = 849$$

$$C = 84^{17}\ mod\ 1081 = 700$$

$$C = 73^{17}\ mod\ 1081 = 646$$

$$C = 75^{17}\ mod\ 1081 = 679$$

$$C = 65^{17}\ mod\ 1081 = 849$$

Sehingga diperoleh *Ciphertext* (*C*) = [151 849 700 483 151 849 700 646 679 849].

4.2 Proses Dekripsi Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA

Langkah awal untuk melakukan dekripsi pada algoritma RSA yaitu dengan menentukan bilangan prima p dan q yang merupakan faktor dari nilai N yang telah diterima. Setelah itu, menentukan nilai $\phi(N)$ sesuai dengan persamaan (ii), kemudian mencari nilai e yang relatif prima dengan $\phi(N)$, kemudian hitung nilai d sebagai kunci privat untuk mengamankan pesan sehingga $de = 1\ (mod\ \phi(N))$ dengan menggunakan persamaan (ix) yaitu:

$$d = \frac{1 + (k.\phi(N)}{e}$$

dengan mencoba nilai $k = 1,2,3,$ ... hingga diperoleh nilai d yang bulat. Setelah itu dapat dilakukan dekripsi sesuai dengan persamaan $(viii)$ yaitu $P = C^d \ mod \ N$.

Proses dekripsi *Myszkowski Cipher* dapat dilakukan dengan menuliskan *ciphertext* secara vertikal dari atas ke bawah secara berurutan sesuai dengan penomoran kunci. Pada penomoran kunci yang sama, *ciphertext* ditulis secara horizontal. Hal ini yang menjadikan kelebihan algoritma *Myszkowski Cipher* dari algoritma cipher transposisi lainnya karena pembacaan *ciphertext* dapat dilakukan secara dua arah. Namun algoritma ini juga memiliki kelemahan karena tidak ada perubahan karakter dari pesan aslinya (Kusumaningtyas, 2018).

Algoritma *Hybrid Myzskowski Cipher* dan RSA untuk Dekripsi

1. Melakukan pembagkitan kunci privat dari nilai N yang telah diterima untuk memperoleh nilai d sebagai kunci privat algoritma RSA.
2. Setelah didapatkan nilai d, maka dapat dilakukan proses perhitungan sesuai dengan persamaan $(viii)$ yaitu $P = C^d \ mod \ N$ menggunakan *software Python*.
3. Kata kunci algoritma *Myzkowski Cipher* yang telah kembali ke bentuk alfabet dapat digunakan untuk mendekripsi pesan teks yang sebelumnya terenkripsi dengan algoritma *Myzkowski Cipher*.
4. Menentukan jumlah baris menggunakan persamaan:

$$\frac{\sum karakter \ ciphertext}{\sum karakter \ kata \ kunci} = \sum baris$$

5. Kemudian *ciphertext* pesan teks dituliskan secara vertikal berdasarkan urutan pada penomoran kata kunci, setelah itu *plaintext* dari pesan teks tersebut dibaca secara horizontal agar dapat kembali ke pesan awal.

4.2.1 Simulasi Dekripsi Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA

Pada proses dekripsi dalam penelitian ini akan digunakan hasil enkripsi sebelumnya yaitu sebagai berikut:

Ciphertext : AIIAKSDUX UGN IIU SPS TNDSIL HNNRAL

Cipherkey : [151 849 700 483 151 849 700 646 679 849]

Nilai $N = 1081$ dan $d = 893$ yang diperoleh berdasarkan persamaan (ix) untuk algoritma RSA. Berikut akan dijelaskan mengenai proses dan langkah-langkah mendekripsikan pesan teks dan kata kunci dengan algoritma *Hybrid* menggunakan *Myzskowski Cipher* dan RSA.

4.2.2 Proses Dekripsi Kunci

Dalam melakukan dekripsi pada kunci dengan algoritma RSA dapat dilakukan dengan menggunakan persamaan $(viii)$ sebagai berikut:

$$P = C^d \ mod \ N$$

$$P = C^{893} \ mod \ 1081$$

Ciphertext (C) = [151 849 700 483 151 849 700 646 679 849]

$$P = 151^{893} \ mod \ 1081 = 77$$

$$P = 849^{893} \ mod \ 1081 = 65$$

$$P = 700^{893} \ mod \ 1081 = 84$$

$$P = 483^{893} \ mod \ 1081 = 69$$

$$P = 151^{893} \ mod \ 1081 = 77$$

$$P = 849^{893} \ mod \ 1081 = 65$$

$$P = 700^{893} \ mod \ 1081 = 84$$

$$P = 646^{893} \ mod \ 1081 = 73$$

$$P = 679^{893}\ mod\ 1081 = 75$$

$$P = 849^{893}\ mod\ 1081 = 65$$

Sehingga diperoleh hasil dekripsi kunci sebagai berikut:

77	**65**	**84**	**69**	**77**	**65**	**84**	**73**	**75**	**65**
M	A	T	E	M	A	T	I	K	A

4.2.3 Proses Dekripsi Pesan

Dalam melakukan dekripsi menggunakan algoritma *Myszkowski Cipher*, perlu dilakukan perhitungan banyak baris pada tabel yang harus disediakan untuk penulisan *ciphertext*, sebagai berikut:

$$\frac{\sum karakter\ ciphertext}{\sum karakter\ kata\ kunci} = \frac{29}{10} = 2.9$$

Maka, jumlah baris yang harus disediakan adalah 3 baris karena dalam menentukan banyak baris akan selalu dibulatkan ke bilangan yang lebih tinggi dan jumlah kolom mengikuti banyaknya jumlah karakter kata kunci yaitu sebanyak 10 kolom. Setelah itu, *ciphertext* dituliskan ke dalam baris secara vertikal berdasarkan nomor urut pada karakter yang telah ditentukan.

Tabel 4.12 Proses Dekripsi Kunci Ke-1 *Myszkowski Cipher*

M	**A**	**T**	**E**	**M**	**A**	**T**	**I**	**K**	**A**
5	1	6	2	5	1	6	3	4	1
	A				**I**				**I**
	A				**K**				**S**
	D				**U**				**X**

Tabel 4.13 Proses Dekripsi Kunci Ke-2 *Myszkowski Cipher*

M	**A**	**T**	**E**	**M**	**A**	**T**	**I**	**K**	**A**
5	1	6	2	5	1	6	3	4	1
	A		**U**		I				I
	A		**G**		K				S
	D		**N**		U				X

Tabel 4.14 Proses Dekripsi Kunci Ke-3 *Myszkowski Cipher*

M	**A**	**T**	**E**	**M**	**A**	**T**	**I**	**K**	**A**
5	1	6	2	5	1	6	3	4	1
	A		U		I		**I**		I
	A		G		K		**I**		S
	D		N		U		**U**		X

Tabel 4.15 Proses Dekripsi Kunci Ke-4 *Myszkowski Cipher*

M	**A**	**T**	**E**	**M**	**A**	**T**	**I**	**K**	**A**
5	1	6	2	5	1	6	3	4	1
	A		U		I		I	**S**	I
	A		G		K		I	**P**	S
	D		N		U		U	**S**	X

Tabel 4.16 Proses Dekripsi Kunci Ke-5 *Myszkowski Cipher*

M	**A**	**T**	**E**	**M**	**A**	**T**	**I**	**K**	**A**
5	1	6	2	5	1	6	3	4	1
T	A		U	**N**	I		I	S	I
D	A		G	**S**	K		I	P	S
I	D		N	**L**	U		U	S	X

Tabel 4.17 Proses Dekripsi Kunci Ke-6 *Myszkowski Cipher*

M	**A**	**T**	**E**	**M**	**A**	**T**	**I**	**K**	**A**
5	1	6	2	5	1	6	3	4	1
T	A	**H**	U	N	I	**N**	I	S	I
D	A	**N**	G	S	K	**R**	I	P	S
I	D	**A**	N	L	U	**L**	U	S	X

Pembacaan *plaintext* dilakukan secara horizontal dari kiri ke kanan, sehingga pesan berhasil dipecahkan dan didapatkan hasil *plaintext* dengan menghilangkan huruf X di akhir kalimat maka *plaintext* kembali seperti semula yaitu *P* = TAHUN INI SIDANG SKRIPSI DAN LULUS.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan di atas maka diperoleh kesimpulan sebagai berikut:

1. Hasil proses enkripsi algoritma *hybrid* menggunakan *Myszkowski Cipher* dan RSA yaitu *ciphertext* yang terenkripsi secara transposisi dan yang kedua adalah *cipherkey* berbentuk numerik yang digunakan untuk mendekripsi pesan teks.
2. Hasil proses dekripsi algoritma *hybrid Myszkowski Cipher* dan algoritma RSA yaitu *plaintext* pesan teks dan *plaintext* kata kunci yang digunakan pada algoritma *Myzskowski Cipher*. Dengan menggunakan algoritma *hybrid* ini keamanan pesan teks lebih terjaga karena pengirim hanya mengirimkan *ciphertext* pesan, *cipherkey* berbentuk angka dan nilai N.

5.2 Saran untuk Penelitian Lanjutan

Pada penelitian ini membahas tentang pengamanan pesan teks dengan menggunakan algoritma *hybrid* menggunakan *Myszkowski Cipher* dan algoritma RSA dengan pemilihan bilangan prima yang kecil. Untuk penelitian berikutnya disarankan menggunakan pemilihan bilangan prima pada algoritma RSA yang lebih besar, serta dapat digunakan pemrograman untuk mempermudah perhitungan ketika melakukan proses enkripsi dan dekripsi.

DAFTAR PUSTAKA

Agustina, A. N., Aryanti, & Nasron. (2017). *Pengamanan Dokumen Menggunakan Kombinasi Metode RSA (Rivest Shamir Adleman) Dan Vigenere Cipher*. Prosiding Seminar Nasional Multi Disiplin Ilmu & Call For Papers Unisbank, 14–19.

Bangun, M. S. (2019). *Implementasi Algoritma Route Cipher Dalam Pengamanan File Pdf*. Building of Informatics, Technology and Science (BITS), 1(1), 1–6.

Basri. (2015). *Pendekatan Kriptografi Hybrid pada Keamanan Dokumen Elektronik dan HypertextTransfer Protocol Secure (HTTPS) (Analisis Potensi Implementasi Pada Sistem Keamanan)*. Jurnal Ilmu Komputer, 1(2), 32–37.

Ekwardo, O. (2018). *Modifikasi Columnar transposition Menggunakan Sebuah Fungsi Transposisi*. Teknik Informatika ITB, 1–4.

Ginting, D. B. (2010). *Peranan Aritmetika Modulo dan Bilangan Prima pada Algoritma Kriptografi RSA (Rivest-Shamir-Adleman)*. Media Informatika, 9(2), 48–57.

Jamaludin, J. (2018). *Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem*. Sinkron: Jurnal Dan Penelitian Teknik Informatika, 2(April 2018). https://jurnal.polgan.ac.id/index.php/sinkron/article/view/139

Katsir, I. (2015). *Tafsir Ibnu Katsir Juz 1-30*.

Kemenag. (2019). *Al-Qur'an dan Terjemahannya*. In Al-Qur'an dan Terjemahannya. http://journal.um-surabaya.ac.id/index.php/JKM/article/view/2203

Khairina, N. (2019). *Modifikasi Myszkowski Transposition Cipher dengan Chess Board Pattern*. Prosiding Seminar Nasional Teknologi Informatika, 2(1), 28–34.

Kusumaningtyas, J. A. (2018). *Analisa Algoritma Ciphers Transposition : Study Literature*. Multimatrix, I(1), 1–12. http://jurnal.unw.ac.id:1254/index.php/mm/article/view/152/106

Ling, S., & Xing, C. (2004). *Coding Theory A First Course*. Cambridge University Press. https://www.ptonline.com/articles/how-to-get-better-mfi-results

Pangaribuan, L. J. (2018). *Kriptografi Hybrida Agloritma Hill Cipher Dan Rivest Shamir Adleman (RSA) Sebagai Pengembangan Kriptografi Kunci Simetris (Studi Kasus : Nilai Mahasiswa Amik Mbp)*. Jurnal Teknologi Informasi Dan Komunikasi, 7(1), 11–26.

Pohan, R. Y. (2007). *Studi dan Perbadingan Berbagai Macam Algoritma Cipher Transposisi*. Informatika.Stei.Itb.Ac.Id, 1–5. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2007-2008/Makalah1/MakalahIF5054-2007-A-021.pdf

Purwono. (2008). Studi Kepustakaan. *Universitas Gajah Mada*, 66–72.

Puspita, S., Noviani, E., & Prihandono, B. (2015). Metode Solovay-Strassen Untuk Pengujian Bilangan Prima. *Buletin Ilmiah Mat. Stat. Dan Terapannya (Bimaster)*, *04*(1), 85–94.

Rahajoeningroem, T., & Aria, M. (2011). Studi dan Implementasi Algoritma RSA untuk Pengamanan Data Transkrip Akademik Mahasiswa. *Majalah Ilmiah Unikom*, *8*(1), 77–90. http://jurnal.unikom.ac.id/_s/data/jurnal/v08-n01/volume-81-artikel-9.pdf/pdf/volume-81-artikel-9.pdf

Safarina, N. (2017). Penerapan Algoritma RSA dan DES pada Pengamanan File Teks. *Pelita Informatika Budi Darma*, *XVI*(1), 55–60.

Suwanti, V., & Fayeldi, T. (2019). *Teori Bilangan Berbasis Penemuan Terbimbing*. repository.unikama.ac.id.

Tao, Y. (2019). *Correctness Proof of RSA* [Chinese University of Hong Kong Correctness]. http://www.cse.cuhk.edu.hk/~taoyf/course/bmeg3120/notes/rsa-proof.pdf

Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. *Jurnal Matematika UNISBA*, *2*(1), 118–125. https://ejournal.unisba.ac.id/index.php/matematika/article/view/4067

Wahyuni, F., Khudzaifah, M., & Jauhari, M. N. (2021). Penyandian Super Enkripsi Menggunakan Columnar Transposition dan Modifikasi Hill Cipher dengan Invers Kiri Matriks Persegi Panjang. *Jurnal Riset Mahasiswa Matematika*, *1*(2), 105–117. https://doi.org/10.18860/jrmm.v1i2.14224

LAMPIRAN

Lampiran 1 ASCII Code

ASCII	SIMBOL	
0	NULL	(Null character)
1	SOH	(Start of Header)
2	STX	(Start of Text)
3	ETX	(End of Text)
4	EOT	(End of Transmission)
5	ENQ	(Enquiry)
6	ACK	(Acknowledgement)
7	BEL	(Bell)
8	BS	(Backspace)
9	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowledgement)
22	SYN	(Synchronous idle)
23	ETB	(End of transmission block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
32		(Space)
33	!	(Exclamation mark)
34	"	(Quotation mark ; quotes)
35	#	(Number sign)
36	$	(Dollar sign)
37	%	(Percent sign)
38	&	(Ampersand)
39	'	(Apostrophe)
40	(	(round brackets or parentheses)

41	)	(round brackets or parentheses)
42	*	(Asterisk)
43	+	(Plus sign)
44	,	(Comma)
45	-	(Hyphen)
46	.	(Dot , full stop)
47	/	(Slash)
48	0	(number zero)
49	1	(number one)
50	2	(number two)
51	3	(number three)
52	4	(number four)
53	5	(number five)
54	6	(number six)
55	7	(number seven)
56	8	(number eight)
57	9	(number nine)
58	:	(Colon)
59	;	(Semicolon)
60	<	(Less-than sign)
61	=	(Equals sign)
62	>	(Greater-than sign ; Inequality)
63	?	(Question mark)
64	@	(At sign)
65	A	(Capital A)
66	B	(Capital B)
67	C	(Capital C)
68	D	(Capital D)
69	E	(Capital E)
70	F	(Capital F)
71	G	(Capital G)
72	H	(Capital H)
73	I	(Capital I)
74	J	(Capital J)
75	K	(Capital K)
76	L	(Capital L)
77	M	(Capital M)
78	N	(Capital N)
79	O	(Capital O)
80	P	(Capital P)
81	Q	(Capital Q)
82	R	(Capital R)
83	S	(Capital S)
84	T	(Capital T)
85	U	(Capital U)
86	V	(Capital V)

87	W	(Capital W)
88	X	(Capital X)
89	Y	(Capital Y)
90	Z	(Capital Z)
91	[	(square brackets or box brackets)
92	\	(Backslash)
93	]	(square brackets or box brackets)
94	^	(Caret or circumflex accent)
95	_	(underscore , understrike , underbar or low line)
96	`	(Grave accent)
97	a	(Lowercase a)
98	b	(Lowercase b)
99	c	(Lowercase c)
100	d	(Lowercase d)
101	e	(Lowercase e)
102	f	(Lowercase f)
103	g	(Lowercase g)
104	h	(Lowercase h)
105	i	(Lowercase i)
106	j	(Lowercase j)
107	k	(Lowercase k)
108	l	(Lowercase l)
109	m	(Lowercase m)
110	n	(Lowercase n)
111	o	(Lowercase o)
112	p	(Lowercase p)
113	q	(Lowercase q)
114	r	(Lowercase r)
115	s	(Lowercase s)
116	t	(Lowercase t)
117	u	(Lowercase u)
118	v	(Lowercase v)
119	w	(Lowercase w)
120	x	(Lowercase x)
121	y	(Lowercase y)
122	z	(Lowercase z)
123	{	(curly brackets or braces)
124	|	(vertical-bar, vbar, vertical line or vertical slash)
125	}	(curly brackets or braces)
126	~	(Tilde ; swung dash)
127	DEL	(Delete)
128	Ç	(Majuscule C-cedilla)
129	ü	(letter "u" with umlaut or diaeresis ; "u-umlaut")
130	é	(letter "e" with acute accent or "e-acute")
131	â	(letter "a" with circumflex accent or "a-circumflex")
132	ä	(letter "a" with umlaut or diaeresis ; "a-umlaut")

133	à	(letter "a" with grave accent)
134	å	(letter "a" with a ring)
135	ç	(Minuscule c-cedilla)
136	ê	(letter "e" with circumflex accent or "e-circumflex")
137	ë	(letter "e" with umlaut or diaeresis ; "e-umlaut")
138	è	(letter "e" with grave accent)
139	ï	(letter "i" with umlaut or diaeresis ; "i-umlaut")
140	î	(letter "i" with circumflex accent or "i-circumflex")
141	ì	(letter "i" with grave accent)
142	Ä	(letter "A" with umlaut or diaeresis ; "A-umlaut")
143	Å	(Capital letter "A" with a ring)
144	É	(Capital letter "E" with acute accent or "E-acute")
145	æ	(Latin diphthong "ae" in lowercase)
146	Æ	(Latin diphthong "AE" in uppercase)
147	ô	(letter "o" with circumflex accent or "o-circumflex")
148	ö	(letter "o" with umlaut or diaeresis ; "o-umlaut")
149	ò	(letter "o" with grave accent)
150	û	(letter "u" with circumflex accent or "u-circumflex")
151	ù	(letter "u" with grave accent)
152	ÿ	(Lowercase letter "y" with diaeresis)
153	Ö	(letter "O" with umlaut or diaeresis ; "O-umlaut")
154	Ü	(letter "U" with umlaut or diaeresis ; "U-umlaut")
155	ø	(slashed zero or empty set)
156	£	(Pound sign ; symbol for the pound sterling)
157	Ø	(slashed zero or empty set)
158	×	(multiplication sign)
159	*ƒ*	(function sign ; f with hook sign ; florin sign)
160	á	(letter "a" with acute accent or "a-acute")
161	í	(letter "i" with acute accent or "i-acute")
162	ó	(letter "o" with acute accent or "o-acute")
163	ú	(letter "u" with acute accent or "u-acute")
164	ñ	(letter "n" with tilde ; enye)
165	Ñ	(letter "N" with tilde ; enye)
166	ª	(feminine ordinal indicator)
167	º	(masculine ordinal indicator)
168	¿	(Inverted question marks)
169	®	(Registered trademark symbol)
170	¬	(Logical negation symbol)
171	½	(One half)
172	¼	(Quarter or one fourth)
173	¡	(Inverted exclamation marks)
174	«	(Angle quotes or guillemets)
175	»	(Guillemets or angle quotes)
176	▒	
177	▒	
178	▓	

179	│	(Box drawing character)
180	┤	(Box drawing character)
181	Á	(Capital letter "A" with acute accent or "A-acute")
182	Â	(letter "A" with circumflex accent or "A-circumflex")
183	À	(letter "A" with grave accent)
184	©	(Copyright symbol)
185	╣	(Box drawing character)
186	║	(Box drawing character)
187	╗	(Box drawing character)
188	╝	(Box drawing character)
189	¢	(Cent symbol)
190	¥	(YEN and YUAN sign)
191	┐	(Box drawing character)
192	└	(Box drawing character)
193	┴	(Box drawing character)
194	┬	(Box drawing character)
195	├	(Box drawing character)
196	─	(Box drawing character)
197	┼	(Box drawing character)
198	ã	(Lowercase letter "a" with tilde or "a-tilde")
199	Ã	(Capital letter "A" with tilde or "A-tilde")
200	╚	(Box drawing character)
201	╔	(Box drawing character)
202	╩	(Box drawing character)
203	╦	(Box drawing character)
204	╠	(Box drawing character)
205	═	(Box drawing character)
206	╬	(Box drawing character)
207	¤	(generic currency sign)
208	ð	(Lowercase letter "eth")
209	Ð	(Capital letter "Eth")
210	Ê	(letter "E" with circumflex accent or "E-circumflex")
211	Ë	(letter "E" with umlaut or diaeresis ; "E-umlaut")
212	È	(letter "E" with grave accent)
213	ı	(lowercase dot less i)
214	Í	(Capital letter "I" with acute accent or "I-acute")
215	Î	(letter "I" with circumflex accent or "I-circumflex")
216	Ï	(letter "I" with umlaut or diaeresis ; "I-umlaut")
217	┘	(Box drawing character)
218	┌	(Box drawing character)
219		(Block)
220		(Bottom half block)
221	¦	(vertical broken bar)
222	Ì	(letter "I" with grave accent)
223		(Top half block)
224	Ó	(Capital letter "O" with acute accent or "O-acute")

225	ß	(letter "Eszett" ; "scharfes S" or "sharp S")
226	Ô	(letter "O" with circumflex accent or "O-circumflex")
227	Ò	(letter "O" with grave accent)
228	õ	(letter "o" with tilde or "o-tilde")
229	Õ	(letter "O" with tilde or "O-tilde")
230	µ	(Lowercase letter "Mu" ; micro sign or micron)
231	þ	(Lowercase letter "Thorn")
232	Þ	(Capital letter "thorn")
233	Ú	(Capital letter "U" with acute accent or "U-acute")
234	Û	(letter "U" with circumflex accent or "U-circumflex")
235	Ù	(letter "U" with grave accent)
236	ý	(Lowercase letter "y" with acute accent)
237	Ý	(Capital letter "Y" with acute accent)
238	¯	(macron symbol)
239	´	(Acute accent)
240	-	(Hyphen)
241	±	(Plus-minus sign)
242	_	(underline or underscore)
243	¾	(three quarters)
244	¶	(paragraph sign or pilcrow)
245	§	(Section sign)
246	÷	(The division sign ; Obelus)
247	¸	(cedilla)
248	°	(degree symbol)
249	¨	(Diaeresis)
250	·	(Interpunct or space dot)
251	¹	(superscript one)
252	³	(cube or superscript three)
253	²	(Square or superscript two)
254	■	(black square)
255	nbsp	(non-breaking space or no-break space)

RIWAYAT HIDUP

Sukmawati Indah Safitri, lahir di Malang pada tanggal 15 Januari 2001. Memiliki nama panggilan Sukma. Bertempat tinggal di Jalan Kebonagung RT.06 RW.01 No.24 A, Kelurahan Tamanharjo, Kecamatan Singosari, Kabupaten Malang, Jawa Timur. Merupakan anak pertama dari Bapak M. Zainal Aris dan Ibu Listiari serta memiliki seorang adik yang bernama M. Arga Pramudya Kusuma.

Jenjang pendidikannya dimulai sejak bersekolah di TK Muslimat XV di Desa Tamanharjo dan lulus pada tahun 2007. Kemudian melanjutkan pendidikan dasar di SD Negeri Tamanharjo 2 yang lulus pada tahun 2013. Setelah itu menempuh pendidikan di SMP Negeri 3 Singosari yang lulus pada tahun 2016. Pendidikan selanjutnya ditempuh di SMA Negeri 1 Singosari bidang minat IPA dan lulus pada tahun 2019. Kemudian melanjutkan ke jenjang perguruan tinggi di Universitas Islam Negeri Maulana Malik Ibrahim Malang dengan menekuni Program Studi Matematika Fakultas Sains dan Teknologi.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

BUKTI KONSULTASI SKRIPSI

Nama	:	Sukmawati Indah Safitri
NIM	:	19610008
Fakultas / Program Studi	:	Sains dan Teknologi / Matematika
Judul Skripsi	:	Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA untuk Mengamankan Pesan Teks
Pembimbing I	:	Muhammad Khudzaifah, M.Si.
Pembimbing II	:	Mohammad Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1.	04 Oktober 2022	Konsultasi Bab I	1.
2.	21 November 2022	Konsultasi Bab II,III	2.
3.	12 Desember 2022	Konsultasi Keagamaan	3.
4.	10 Januari 2023	ACC Bab I, II, III	4.
5.	08 Maret 2023	Konsultasi Bab IV	5.
6.	13 Maret 2023	Konsultasi Bab IV	6.
7.	25 Maret 2023	Konsultasi Keagamaan	7.
8.	28 Maret 2023	ACC Revisi Seminar Proposal	8.
9.	29 Maret 2023	Konsultasi Bab IV	9.
10.	03 April 2023	Konsultasi Bab IV dan V	10.
11.	04 April 2023	Konsultasi Keagamaan	11.
12.	05 April 2023	Konsultasi Bab V	12.
13.	04 Mei 2023	Konsultasi Revisi Bab I-V	13.
14.	11 Mei 2023	ACC Revisi Seminar Hasil	14.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

15.	04 Juni 2023	ACC Revisi Bab I-V	15.
16.	08 Juni 2023	ACC Keagamaan	16.
17.	15 Juni 2023	ACC Keseluruhan	17.

Malang, 15 Juni 2023
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005