ALGORITMA *CIPHER BLOCK CHAINING* DAN ALGORITMA *RABIN* SEBAGAI *HYBRID CRYPTOSYSTEM* PADA PENGAMANAN PESAN TEKS

SKRIPSI

OLEH
IRBAH NAFIAH
NIM. 18610052

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

ALGORITMA *CIPHER BLOCK CHAINING* DAN ALGORITMA *RABIN* SEBAGAI *HYBRID CRYPTOSYSTEM* PADA PENGAMANAN 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
Irbah Nafiah
NIM.18610052

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

ALGORITMA *CIPHER BLOCK CHAINING* DAN ALGORITMA *RABIN* SEBAGAI *HYBRID CRYPTOSYSTEM* PADA PENGAMANAN PESAN TEKS

SKRIPSI

Oleh
Irbah Nafiah
NIM. 18610052

Telah Disetujui Untuk Diuji
Malang, 11 April 2023

Dosen Pembimbing I	Dosen Pembimbing II
Prof. Dr. H. Turmudi, M.Si, Ph.D	Mohammad Nafie Jauhari, M.Si
NIP. 19571005 198203 1 006	NIDT. 19870218 20160801 1 056

Mengetahui,
Ketua Program Studi Matematika

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

ALGORITMA *CIPHER BLOCK CHAINING* DAN ALGORITMA *RABIN* SEBAGAI *HYBRID CRYPTOSYSTEM* PADA PENGAMANAN PESAN TEKS

SKRIPSI

Oleh
Irbah Nafiah
NIM. 18610052

Telah Dipertahankan di Depan Penguji Seminar Hasil Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Satjana Matematika (S.Mat)

Tanggal 8 Mei 2023

Ketua Penguji	: Juhari, M. Si	.....
Anggota Penguji I	: Muhammad Khudzaifah, M. Si	.....
Anggota Penguji II	: Prof. Dr. H. Turmudi, M.Si., Ph.D	.....
Anggota Penguji III	: 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 : Irbah Nafiah

NIM : 18610052

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Algoritma *Cipher Block Chaining* dan Algoritma *Rabin* sebagai *Hybrid Cryptosystem* pada Pengamanan Pesan Teks

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

Malang, 8 Mei 2023

Yang membuat pernyataan

Irbah Nafiah

NIM. 18610052

MOTTO

“Jalani, nikmati, dan syukuri”

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk :

Kedua orang tua penulis Bapak Suparman dan Ibu Kasmonah yang selalu mendoakan dan mendukung seiring proses mengerjakan skripsi ini. Kedua kakak penulis, Lailatul Fitriani dan Mukhammad Ghufron Novianto yang senantiasa memberi semangat dan motivasi.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah SWT yang telah melimpahkan taufik dan hidayah-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi ini sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang Matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Dalam proses penyusunan skripsi ini, penulis menyadari sepenuhnya bahwa penyelesaian skripsi ini tidak terlepas dari motivasi, dukungan, serta bimbingan dari berbagai pihak. Oleh sebab itu, penulis ingin menyampaikan terima kasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya penulis sampaikan kepada :

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Elly Susanti, M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Prof. Dr. H. Turmudi, M.Si., Ph.D, selaku dosen pembimbing I yang telah dengan sabar membimbing serta memberikan arahan kepada penulis dalam menyelesaikan naskah skripsi ini.
5. Mohammad Nafie Jauhari, M.Si, selaku dosen pembimbing II yang telah membimbing kepada penulis dalam pengerjaan skripsi ini.
6. Juhari, M. Si, selaku Ketua Penguji dalam Ujian Skripsi yang telah memberikan masukan dan saran kepada penulis.
7. Muhammad Khudzaifah, M.Si, selaku Anggota Penguji I dalam Ujian Skripsi yang telah memberikan masukan dan arahan kepada penulis.
8. Orang tua tercinta Suparman dan Kasmonah yang senantiasa memberi restu, doa, motivasi, dukungan, serta nasehat kepada penulis.
9. Lailatul Fitriani dan Mukhammad Ghufron Novianto selaku kakak dari penulis yang senantiasa memberikan dukungan, semangat, dan motivasi kepada penulis.

10. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
11. Teman-teman mahasiswa Program Studi Matematika angkatan 2018.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 08 Mei 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

ABSTRAK

Nafiah, Irbah. 2023. **Algoritma *Cipher Block Chaining* dan Algoritma *Rabin* sebagai *Hybrid Cryptosystem* Pada Pengamanan Pesan Teks.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Prof. Dr, H. Turmudi, M.Si., Ph. D, (II) Mohammad Nafie Jauhari, M.Si.

Kata Kunci: Kriptografi, *Cipher Block Chaining*, *Rabin*, *Hybrid Cryptosystem.*

Pengiriman suatu pesan yang bersifat rahasia memerlukan proses pengiriman pesan yang aman untuk menjaga isi pesan. Oleh karena itu, diperlukan suatu metode untuk mengamankan isi dari pesan rahasia yang disebut sebagai kriptografi. Kriptografi terdiri dari dua bagian berdasarkan kunci yang digunakannya, yaitu kriptografi simetris dan kriptografi asimetris. Penelitian ini menggunakan algoritma simetris *Cipher Block Chaining* dan algoritma asimetris *Rabin* sebagai *hybrid cryptosystem* yang bertujuan untuk mengamankan pesan teks. Tahapan penelitian ini dilakukan dengan proses enkripsi terhadap *plaintext* menggunakan algoritma *Cipher Block Chaining.* Kemudian, proses enkripsi dilakukan terhadap kunci simetris dan *initial vector* dari algoritma Cipher Block Chaining menggunakan algoritma *Rabin*. Pada proses dekripsi pesan, algoritma *Rabin* digunakan untuk mendekripsikan *cipherkey*, sedangkan algoritma *Cipher Block Chaining* digunakan untuk mendekripsikan *ciphertext*. Hasil dari penelitian ini menunjukkan bahwa penggabungan algoritma *Cipher Block Chaining* dan algoritma *Rabin* memiliki tingkat keamanan pesan yang tinggi, karena kriptosistem ini menghasilkan kunci simetri dan *Initial Vector* yang bersifat rahasia. Hasil dari proses enkripsi dan dekripsi terhadap *plainkey* dan *plaintext* tidak berubah.
.

ABSTRACT

Nafiah, Irbah. 2023. **Cipher Block Chaining Algorithm and Rabin Algorithm as a Hybrid Cryptosystem in Security of Text Messages.** Thesis of Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Supervisors: (I) Prof. Dr, H. Turmudi, M.Si., Ph. D, (II) Mohammad Nafie Jauhari, M.Si.

Keywords: Cryptography, Cipher Block Chaining, Rabin, Hybrid Cryptosystem.

Sending a message that is confidential requires a secure message delivery process to protect the contents of the message. Therefore, we need a method to secure the contents of a secret message which is known as cryptography. Cryptography consists of two parts based on the key it uses, namely symmetric cryptography and asymmetric cryptography. This study uses the symmetric Cipher Block Chaining algorithm and the Rabin asymmetric algorithm as a hybrid cryptosystem to secure text messages are considered. The stages of this research were carried out by encrypting plaintext using the Cipher Block Chaining algorithm. Then, the encryption process is carried out on the symmetric key and initial vector of the Cipher Block Chaining algorithm using the Rabin algorithm. In the message decryption process, the Rabin algorithm is used to decrypt the cipherkey, while the Cipher Block Chaining algorithm is used to decrypt the ciphertext. The results of this study indicate that the combination of the Cipher Block Chaining algorithm and the Rabin algorithm has a high level of message security because this cryptosystem produces a symmetric key and Initial Vector which are confidential. The results of the encryption and decryption processes for plainkey and plaintext do not change.

مستخلص البحث

إربة، نافعة. ٢٠٢٣. خوارزمية *Cipher Block Chaining* وخوارزمية *Rabin* كنظام تشفير هجين على أمان الرسائل النصية. البحث الجا معي. ، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية، مالانغ.

المشرف :

(١)البروفيسور، الدكتور، ترمودي، الماجستير، الحاج ، (٢)مُحَمَّد نافع جوهري، الماجستير.

الكلمات المفتاحية: التشفير، *Cipher Block Chaining*، *Rabin*، نظام التشفير الهجين.

يحتاج إرسال رسائل سرية إلى عملية تسليم رسائل آمنة لحماية محتويات الرسالة. لذلك نحتاج إلى طريقة لتأمين محتويات رسالة سرية وتعرف باسم التشفير. يتكون التشفير من جزأين يعتمدين على المفتاح الذي يستخدمه ، وهما التشفير المتماثل والتشفير غير المتماثل. تستخدم هذه الدراسة خوارزمية *Cipher Block Chaining* المتماثل وخوارزمية *Rabin* غير المتماثلة كنظام تشفير هجين يهدف إلى تأمين الرسائل النصية. تم تنفيذ مرحلة هذا البحث عن طريق تشفير النص الصريح باستخدام خوارزمية *Cipher Block Chaining*. ثم يتم تنفيذ عملية التشفير على المفتاح المتماثل والمتجه الأولي لخوارزمية *Cipher Block Chaining* باستخدام خوارزمية *Rabin*. في عملية فك تشفير الرسائل ، يتم استخدام خوارزمية *Rabin* لفك تشفير مفتاح التشفير ، بينما يتم استخدام خوارزمية *Cipher Block Chaining* لفك تشفير النص المشفر. تشير نتائج هذه الدراسة العلمية إلى أن الجمع بين الخوارزمية *Cipher Block Chaining* والخوارزمية *Rabin* أكثر أمانًا ، لأن نظام التشفير هذا ينتج مفتاحًا متماثلًا سريًا وناقلًا أوليًا. لا تتغير نتائج عمليات التشفير وفك التشفير للمفتاح العادي والنص العادي.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pesan merupakan perintah, nasihat, permintaan yang disampaikan secara langsung maupun tidak langsung. Pesan tak langsung disampaikan melalui perantara berupa data teks, gambar, maupun audio visual. Dalam penyampaian pesan tersebut, terdapat pesan yang bersifat rahasia dan ada yang tidak. Pesan rahasia bertujuan hanya orang yang berhak menerimalah yang mengetahui isi pesan tersebut. Hal ini menjadikan pesan yang bersifat rahasia memerlukan suatu metode untuk menjaga keamanan dan kerahasiaan isi dari pesan tersebut.

Suatu pesan rahasia yang dikirim melalui perantara semestinya dapat tersampaikan kepada pihak yang berhak menerima. Maka dari itu, keamanan isi dari pesan rahasia menjadi prioritas utama dalam menyampaikan pesan tersebut. Sebagaimana telah dijelaskan firman Allah swt. dalam al-Qur'an surah An-Nisa' ayat 58 yang artinya (LPMQ, 2019):

> "*Sesungguhnya Allah menyuruhmu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum diantara manusia hendaknya kamu menetapkan dengan adil. Sungguh, Allah sebaik-baik yang memberi pengajaran kepadamu. Sungguh, Allah Maha Mendengar, Maha Melihat*".

Pada proses pengiriman pesan rahasia, jalur pengiriman yang akan dilalui harus dipastikan memiliki keamanan yang terjamin agar terhindar dari pencurian dan manipulasi isi pesan. Pesan rahasia yang diamankan menggunakan teknik enkripsi dan dekripsi dengan memanfaatkan fungsi matematika inilah yang disebut sebagai algoritma kriptografi (Kurniawan, 2008). Dalam algoritma

kriptografi, terdapat dua proses dasar yang dilakukan yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana pesan asli (*plaintext*) yang akan dikonversikan menjadi teks tersandi/rahasia (*ciphertext*) dengan memanfaatkan suatu kunci, sehingga plainteks akan sulit dibaca oleh pihak ketiga yang tidak berwenang. Sedangkan, dekripsi merupakan teknik untuk mengonversi *ciphertext* menjadi *plaintext*. Seiring pesatnya kemajuan teknologi, algoritma kriptografi terus dikembangkan untuk meningkatkan keamanan dan kerahasiaan suatu pesan. Berdasarkan kunci yang digunakan, algoritma kriptografi terdiri dari dua jenis yaitu algoritma simetris dan asimetris. Algoritma simetris adalah algoritma kriptografi yang mempunyai kunci yang sama untuk melakukan proses enkripsi dan dekripsinya, sedangkan algoritma asimetris adalah algoritma kriptografi menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Pada algoritma asimetris, kunci enkripsinya bersifat umum (kunci publik) dan kunci dekripsi bersifat rahasia (kunci privat) (Munir, 2006).

Algoritma *Cipher Block Chaining* (CBC) merupakan salah satu algoritma simetris yang menerapkan operasi *block cipher*, di mana hasil enkripsi dari blok pesan sebelumnya akan digunakan sebagai *Initial Vector* dalam proses enkripsi blok pesan selanjutnya sebelum dienkripsi dengan kuncinya. Hal ini menjadikan hasil enkripsi setiap blok pesan bergantung pada *plaintext*-nya dan seluruh blok *plaintext* sebelumnya, sehingga apabila terdapat potongan *plaintext* yang diketahui oleh penyerang, namun tidak akan banyak membantu untuk memecahkannya. Untuk proses dekripsi pada algoritma CBC, blok *ciphertext* sebelumnya akan digunakan sebagai umpan maju (*feedforward*) pada akhir dekripsi (Rosmala, 2012).

Algoritma *Rabin* merupakan algoritma asimetris yang menggunakan metode pemfaktoran bilangan untuk mengamankan pesan. Pada algoritma *Rabin*, kunci publik akan digunakan pada proses enkripsi dan kunci privat digunakan pada proses dekripsi. Tingkat keamanan yang dihasilkan pada algoritma *Rabin* bergantung pada kesulitan memfaktorkan bilangan yang sangat besar, sehingga semakin besar kunci privat maka semakin baik keamanan pesan yang dirahasiakan.

Suhandinata (2019) menyatakan bahwa kecepatan proses enkripsi dan dekripsi kriptografi hibrid antara algoritma *Blowfish* dan algoritma RSA relatif cepat namun tidak secepat algoritma pembentuknya. Kemudian, Ollinka (2021) menyimpulkan bahwa *Hybrid Cryptosystem* menggunakan algoritma *Gronsfeld Cipher* dan algoritma *Rabin* untuk mengamankan dokumen PDF memerlukan waktu yang lebih lama pada proses dekripsi dibanding proses enkripsinya. Pangaribuan (2018) menyatakan bahwa proses dekripsi *hybrid cryptosystem* menggunakan algoritma *Hill Cipher* pada matriks 3×3 dan algoritma RSA membutuhkan waktu yang lebih lama dibanding dengan proses dekripsi menggunakan algoritma *Hill Cipher*. Dengan demikian, perlu adanya pengembangan dan modifikasi algoritma untuk menghasilkan *cipher* yang relatif kuat dengan waktu proses enkripsi dan dekripsi yang relatif singkat.

Hybrid cryptosystem merupakan metode dalam ilmu kriptografi dengan menggabungkan algoritma simetris dan algoritma asimetris. Kelemahan yang dimiliki algoritma simetris adalah keamanan pada kunci yang digunakan, tetapi proses enkripsi dan dekripsi pesan lebih cepat dibanding algoritma asimetri. Pada algoritma asimetris, keamanan kunci yang digunakan lebih tinggi, namun proses

enkripsi dan dekripsi pesan membutuhkan waktu yang lebih lama dibanding dengan algoritma simetri. Dengan demikian, *hybrid cryptosystem* bertujuan untuk memberikan melindungi kunci simetris serta meningkatkan kecepatan kriptografi kunci asimetris.

Berdasarkan permasalahan di atas, peneliti akan memadukan konsep algoritma CBC dan algoritma *Rabin* sebagai *hybrid cryptosystem* untuk meningkatkan keamanan pesan teks dan dapat mengatasi kelemahan beberapa penelitian sebelumnya, sehingga didapatkan *ciphertext* yang sulit dipecahkan dan diketahui oleh pihak lain yang tidak berkepentingan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dibuat, rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana proses enkripsi menggunakan algoritma CBC dan algoritma *Rabin* sebagai *Hybrid Cryptosystem* dalam pengamanan pesan?
2. Bagaimana proses dekripsi menggunakan algoritma CBC dan algoritma *Rabin* sebagai *Hybrid Cryptosystem* dalam pengamanan pesan?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Mendeskripsikan proses enkripsi menggunakan algoritma CBC dan algoritma *Rabin* sebagai *Hybrid Cryptosystem* pada pengamanan pesan.

2. Mendeskripsikan proses dekripsi menggunakan algoritma CBC dan algoritma *Rabin* sebagai *Hybrid Cryptosystem* pada pengamanan pesan pada pengamanan pesan.

1.4 Manfaat Penelitian

Penelitian ini memiliki manfaat untuk berbagai pihak yang dapat dijabarkan sebagai berikut:

1. Bagi penulis

   Penelitian ini dapat memperkaya ilmu pengetahuan mengenai kriptografi hibrid pada algoritma CBC dan algoritma *Rabin*.

2. Bagi pembaca

   Penelitian ini dapat menambah wawasan tentang proses enkripsi dan dekripsi tentang kriptografi hibrid pada algoritma CBC dan algoritma *Rabin* dalam pengamanan pesan teks.

3. Bagi lembaga

   Penelitian yang telah dibuat dapat memperkaya bahan literasi dan informasi yang mencakup mata kuliah terutama pada kriptografi.

1.5 Batasan Masalah

Pembahasan dalam penelitian ini dibatasi dengan menggunakan karakter khusus berjumlah 53 karakter yang terdiri dari alfabet kecil a-z, alfabet kapital A-Z, dan spasi dalam ASCII (*American Code for Information Interchange*) untuk proses enkripsi dan dekripsi.

1.6 Definisi Istilah

Penelitian ini menggunakan beberapa istilah tetentu, sehingga agar pembaca dapat memahaminya akan dijelaskan sebagai berikut:

1. *Symmetric key* adalah kunci yang digunakan sebagai parameter dalam proses enkripsi dan dekripsi pada algoritma simetris.
2. *Cipher key* adalah kunci yang diperoleh dari proses enkripsi terhadap *Symmetric key* dalam algoritma *hybrid cryptosystem.*
3. Bit adalah satuan terkecil pada sistem angka biner.
4. *Hybrid Cryptosystem* adalah gabungan dari kriptosistem yang menggunakan satu kunci (algoritma kriptografi simetris) dan kriptosistem yang menggunakan kunci publik dan kunci privat (algoritma kriptografi asimetris).
5. *Cipher Block Chaining* (CBC) adalah salah satu algoritma kriptografi yang mengoperasikan block cipher menggunakan *Initial Vector* dengan ukuran tertentu dan memiliki ukuran yang sama dengan satu blok *plaintext*-nya.
6. *Initial Vector* adalah suatu blok yang berperan sebagai pengganti *block ciphertext* sebelumnya pada pengoperasian awal algoritma CBC untuk menghasilkan blok *cipher* pertama.
7. Algoritma *Rabin* adalah salah satu algoritma kriptografi asimetris yang menggunakan kunci publik untuk proses enkripsi dan kunci privat untuk proses dekripsinya.

BAB II
KAJIAN PUSTAKA

2.1 Teori Pendukung

2.1.1 Keterbagian

Keterbagian (*divisibility*) merupakan dasar dari pengembangan konsep teori bilangan. Jika suatu bilangan bulat dibagi oleh suatu bilangan bulat yang lain, maka akan menghasilkan bilangan bulat lain atau bukan termasuk bilangan bulat.

Definisi 2.1

Misalkan $a, b \in \mathbb{Z}$, dengan $a \neq 0$, maka a disebut membagi b dan ditulis sebagai $a|b$ jika $b = ak$, untuk suatu $k \in \mathbb{Z}$ (Irawan *et al*., 2014).

Berdasarkan definisi ini, suatu bilangan bulat a dengan $a \neq 0$ dinyatakan membagi bilangan bulat b apabila terdapat suatu bilangan k sedemikian hingga $b = ak$. Notasi $a|b$ dapat dibaca dengan "a membagi b", "b faktor dari a", "b habis dibagi a", atau "b kelipatan dari a", sedangkan notasi $a \nmid b$ menyatakan bahwa a tidak membagi b. Apabila $a|b$ dan $0 < a < b$, maka a disebut sebagai pembagi sejati dari b.

Contoh:

1. $4|20$, karena terdapat $5 \in \mathbb{Z}$ sehingga $20 = 4.5$
2. $7 \nmid 13$, karena tidak ada $k \in \mathbb{Z}$ sedemikian hingga $13 = 7k$.
3. $6|18$, karena terdapat $3 \in \mathbb{Z}$ sehingga $18 = 6.3$

Kemudian, untuk sebarang bilangan bulat a, b, x berlaku:

Teorema 2.1

Jika $a|b$, maka $a|bx$ untuk setiap bilangan bulat $x; a \neq 0$.

Bukti

Diketahui $a, b,$ dan x adalah bilangan bulat. Karena $a|b$, maka terdapat $k \in \mathbb{Z}$ sedemikian hingga $b = ak$ (berdasarkan definisi 2.1). Perhatikan bahwa jika b dikalikan dengan x, maka $bx = (ak)x$ untuk setiap $x \in \mathbb{Z}$. Selanjutnya, menggunakan asosiatif perkalian maka $bx = a(kx)$ dengan $kx \in \mathbb{Z}$. Hal ini berarti, $a|bx$ (terbukti).

Contoh:

$4|8$ maka $4|8.2$ atau $4|8.3$ atau $4|8.4$ dan seterusnya.

Teorema 2.2

Jika $a|b$ dan $b|x$, maka $a|x$; $a \neq 0, b \neq 0$.

Bukti

Perhatikan bahwa

$a|b \longrightarrow b = ak$ untuk $k \in \mathbb{Z}$ (persamaan 1)

$b|x \longrightarrow x = bt$ untuk $t \in \mathbb{Z}$ (persamaan 2)

Selanjutnya, mensubstitusikan b pada persamaan 2, sehingga diperoleh $x = (ak)t$. Kemudian, menggunakan asosiatif perkalian diperoleh $x = a(kt)$ untuk suatu $kt \in \mathbb{Z}$. Jadi, $a|x$ (terbukti).

Contoh:

$7|14$ dan $14|28$, maka $7|28$.

$9|36$ dan $36|72$, maka $9|72$.

Teorema 2.3

Jika $a|b$ dan $a|x$, maka $a|b \pm x$; $a \neq 0$.

Bukti

$a|b \rightarrow b = ak_1$; untuk suatu $k_1 \in \mathbb{Z}$ (i(berdasarkan definisi 2.1))

$a|x \rightarrow x = ak_2$; untuk suatu $k_2 \in \mathbb{Z}$ (ii(berdasarkan definisi 2.1))

Selanjutya, keduanya dijumlahkan sehingga diperoleh

$b + x = a(k_1 + k_2)$ dengan $(k_1 + k_2) \in \mathbb{Z}$

dan sesuai definisi berlaku $a|b + x$.

Hal ini berlaku juga dengan mengurangkan (i) (ii), maka diperoleh

$b - x = a(k_1 - k_2)$ dengan $(k_1 - k_2) \in \mathbb{Z}$

dan sesuai definisi berlaku $a|b - x$.

Jadi, $a|b \pm x$ (terbukti).

Definisi 2.2 *Greatest Common Divisor* (Faktor Persekutuan Terbesar)

Suatu bilangan bulat positif a merupakan pembagi persekutuan dari b dan c yang tidak nol jika $a|b$ dan $a|c$. Kemudian, bilangan bulat a adalah pembagi persekutuan terbesar atau FPB dari bilangan bulat b dan c yang tidak nol jika a adalah bilangan bulat positif terbesar sedemikian hingga $a|b$ dan $a|c$ (Irawan *et al*., 2014).

Bilangan bulat a juga disebut sebagai FPB dari bilangan bulat b dan c yang tidak nol jika memenuhi syarat sebagai berikut:

1. $a > 0$,
2. $a|b$ dan $a|c$, dan
3. Jika $d|b$ dan $d|c$ maka $d|a$.

Notasi FPB dari b dan c dapat dituliskan dengan $a = FPB(b, c)$ dan karena $a > 0$, maka $a = (b, c) \geq 1$ sehingga $FPB(b, c) = FPB(b, -c) = FPB(-b, c) = FPB(-b, -c)$. Misalnya pembagi persekutuan terbesar dari 18 dan 14 adalah 2 ditulis dengan $FPB(18,14) = 2$, sehingga $(18,14) = (18, -14) = (-18,14) = (-18, -14) = 2$.

Teorema 2.4

Jika d adalah pembagi persekutuan terbesar dari $a \neq 0$ dan $b \neq 0$, maka terdapat bilangan bulat x dan y sedemikian sehingga $d = (a, b) = xa + yb$ (Irawan et al., 2014).

Bukti

Misalkan $M = \{(xa + yb) | x, y \in \mathbb{Z}\}$. Maka, anggota dari M adalah bilangan bulat positif, nol, dan negatif.

Ambil $S = \{xa + yb | xa + yb > 0\}$ maka $S \subset \mathbb{N}$, dengan $\mathbb{N}$ merupakan himpunan bilangan asli. Karena $S \subset \mathbb{N}$ dan $\mathbb{N}$ terurut dengan baik, maka S mempunyai elemen terkecil, misalnya d dan $d > 0$. Akibatnya, $d = x_0.a + y_0.b$ untuk $x_0, y_0 \in \mathbb{Z}$.

Selanjutnya akan ditunjukkan bahwa d adalah pembagi persekutuan dari a dan b.

1. Ambil sembarang $x_1 = xa + yb$ di S, maka

   $x_1 = kd + r; 0 \leq r < d$

   $xa + yb = k(x_0 a + y_0 b) + r$

   $r = (x - kx_0)a + (y - y_0 k)b \in S$

   Karena $0 \leq r$ dan $r < d$ sedangkan d elemen terkecil dari S maka $r = 0$

   Sehingga $(x - kx_0)a + (y - y_0 k)b = 0$

   $\leftrightarrow (xa + yb) - (kx_0 a + ky_0 b) = 0$

   $\leftrightarrow (xa + yb) - k(x_0 a + y_0 b) = 0$

   $\leftrightarrow (xa + yb) - kd = 0$

   $\leftrightarrow (xa + yb) = kd$

   $x_1 = kd$ untuk suatu $x_1 = xa + yb \in S$

   Sehingga $d | x_1$ untuk setiap $x_1 \in S$.

Perhatikan bahwa $a = 1.a + 0.b \in S$ dan $b = 0.a + 1.b \in S$, sehingga diperoleh $d|a$ dan $d|b$ untuk setiap $a, b \in S$.

2. Akan dibuktikan bahwa d adalah pembagi terbesar.

   Misalkan terdapat $m \in \mathbb{Z}$ sehingga $m|a$ dan $m|b$, maka menurut Teorema 2.3 diperoleh $m|(x_0.a + y_0.b)$ atau $m|h$.

   Dengan demikian dapat disimpulkan bahwa

   $d = FPB(a, b) = x_0a + y_0b$ untuk suatu $x_0, y_0 \in \mathbb{Z}$.

Contoh

$FPB(6,22) = 2$, maka $2 = 6x + 22y$ dengan $x, y \in \mathbb{Z}$. Nilai x dan y yang memenuhi persamaan adalah sebagai berikut:

$x = 4$ dan $y = -1$

$x = 7$ dan $y = -2$

$x = 18$ dan $y = -5$ dan seterusnya.

Teorema 2.5 Algoritma *Euclid*

Misal diberikan dua bilangan bulat a dan b dengan$a \geq b > 0$. Dengan membuat pengulangan dari algoritma pembagian akan diperoleh persamaan sebagai berikut:

$b = a.q_1 + r_1$ dengan $0 \leq r_1 < c$

$a = r_1.q_2 + r_2$ dengan $0 \leq r_2 < r_1$

$r_1 = r_2.q_3 + r_3$ dengan $0 \leq r_3 < r_2$

$\vdots$

$r_{n-2} = r_{n-1}.q_n + r_n$ dengan $0 \leq r_n < r_{n-1}$

$r_{n-1} = r_n.q_{n+1} + 0$ dst.

Misal pembagi persekutuan terbesar dari a dan b adalah $r_n = (a, b)$ yang merupakan sisa terakhir yang tidak nol dalam proses rekursif pembagian ini.

Nilai x dan y yang bulat persamaan $(a, b) = ax + by$ dapat diperoleh dengan eliminasi $r_{n-1}, \dots, r_2, r_1$ dari persamaan di atas.

Bukti

Untuk membuktikan $r_n = (a, b)$ harus ditunjukkan bahwa $r_n|a$ dan $r_n|b$ dan jika $k|a$ dan $k|b$ maka $k|r_n$. Oleh sebab itu, pada proses rekursif pembagian ini diperoleh bahwa $r_{k+1} = 0$ maka $r_n|r_{n-1}$.

Sedangkan untuk $r_{n-2} = r_{n-1}q_n + r_n$ dan $r_n|r_{n-1}$ dan $r_n|r_n$, maka diperoleh $r_n|r_{n-2}$. Dengan melanjutkan proses ini, akan diperoleh bahwa $r_n|r_{n-3}$, $r_n|r_{n-4}$, ..., $r_n|r_1$, $r_n|r_b$, $r_n|r_a$. Jadi melalui proses ini didapatkan $r_n|a$ dan $r_n|b$.

Sekarang untuk membuktikan bahwa r_n merupakan elemen yang terbesar, maka $k|a$ dan $k|b$ harus dibuktikan bahwa $k|r_n$.

Misalkan $k|a$ dan $k|b$.

Karena $r_1 = b - aq_1$ di mana $k|r_1$ dan $k|a$, maka diperoleh bahwa $k|r_2$. Dengan melanjutkan proses ini akan diperoleh: $k|r_3$, $k|r_4$, ..., $k|r_n$.

Jadi, r_n merupakan elemen terbesar.

Dengan demikian terbukti bahwa $r_n = (a, b)$.

Lemma 2.1

Jika $a = qb + r$, maka $FPB(a, b) = FPB(b, r)$.

Bukti

Jika $d = FPB(a, b)$, maka $d|a$ dan $d|b$ sehingga $d|(a - qb)$ atau $d|r$. Jadi, d adalah pembagi persekutuan dari b dan r. Di sisi lain, jika sebarang c adalah pembagi persekutuan terbesar dari b dan r, maka $c|(qb + r)$ atau $c|a$. Hal ini mengakibatkatkan c merupakan pembagi persekutuan terbesar dari a dan b

dengan $c \leq d$. Berdasarkan definisi pembagi persekutuan terbesar, maka $d = FPB(a,b) = FPB(b,r)$.

2.1.2 *Extended Euclidean*

Untuk menentukan x dan y yang memenuhi $FPB(a,b) = ax + by$ adalah dengan substitusi balik algoritma *Euclid* atau bisa disebut dengan algoritma *Extended Euclidean* yang merupakan perluasan dari algoritma *Euclid* sebagai berikut:

$r_n = r_{n-2} - q_n r_{n-1}$

$r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2})$

$r_n = (1 + q_n q_{n-1}) r_{n-2} + (q_n) r_{n-3}$

r_n direpresentasikan sebagai kombinasi linear dari r_{n-2} dan r_{n-3}. Dengan meneruskan persamaan tersebut, maka kita behasil mengeliminasi $r_{n-1}, r_{n-2}, \dots, r_2, r_1$sehingga $r_n = FPB(a,b) = ax + by$ dan diketahui nilai x dan y yang memenuhi kombinasi linear tersebut.

Contoh:

Menggunakan algoritma *Euclid*, tentukan $FPB(43{,}12)$.

Berdasarkan algoritma pembagian, diperoleh:

$$43 = 3.12 + 7$$

$$12 = 1.7 + 5$$

$$7 = 1.5 + 2$$

$$5 = 2.2 + 1$$

$$2 = 2.1 + 0$$

Sehingga dapat dinyatakan bahwa $FPB(43,12) = 1$. Kemudian, untuk menyatakan 1 sebagai kombinasi linear dari 43 dan 12, maka diperlukan algoritma pembagian secara mundur (substitusi balik dari algoritma *Euclid*) sebagai berikut:

$1 = 5 - 2.2$

$1 = 5 - 2(7 - 1.5)$

$1 = 5 - 2.7 + 2.5$

$1 = 3.5 - 2.7$

$1 = 3(12 - 1.7) - 2.7$

$1 = 3.12 - 5.7$

$1 = 3.12 - 5(43 - 3.12)$

$1 = -5.43 + 18.12$

Diperoleh $x = -5$ dan $y = 18$.

2.1.3 Bilangan Prima

Bilangan prima didefinisikan sebagai suatu bilangan asli yang tepat mempunyai dua pembagi, sedangkan bilangan yang mempunyai lebih dari dua pembagi disebut sebagai bilangan komposit.

Definisi 2.3

Suatu bilangan bulat $p > 1$ disebut bilangan prima, jika tidak terdapat pembagi d dari p yang memenuhi $1 < d < p$

Contoh:

$2, 3, 5, 7, 11, 13,$ ... adalah bilangan prima. Seluruh bilangan prima adalah bilangan ganjil kecuali 2 yang merupakan bilangan genap.

2.1.4 Relatif Prima

Dua buah bilangan a dan b disebut sebagai relatif prima jika pembagi persekutuan terbesar dari keduanya adalah 1, $FPB(a, b) = 1$.

Contoh:

1. $FPB(11,7)$ adalah:

$$11 = 1.7 + 4$$

$$7 = 1.4 + 3$$

$$4 = 1.3 + 1$$

$$3 = 3.1 + 0$$

Bilangan-bilangan prima 11 dan 7 adalah relatif prima, karena $FPB(11,7) = 1$

2. $FPB(24,13)$ adalah:

$$24 = 1.13 + 11$$

$$13 = 1.11 + 2$$

$$11 = 5.2 + 1$$

$$2 = 2.1 + 0$$

Bilangan 24 dan 13 adalah relatif prima, karena $FPB(24,13) = 1$.

2.1.5 Aritmatika Modulo

Aritmatika modulo merupakan sisa hasil bagi dari dua bilangan bulat positif. Misalkan a dan m adalah bilangan bulat positif $(a, m > 0)$, maka $a\ (mod\ m)$ yang dibaca dengan "a *modulo* m" akan menghasilkan hasil bagi (q) dan sisa bagi (r) yang dinotasikan dengan $a\ (mod\ m) = r$, sehingga $a = mq + r$. Bilangan m disebut sebagai modulus atau modulo.

Contoh:

1. $24\ (mod\ 5) = 4$, sehingga $24 = 4 * 5 + 4$.
2. $5\ (mod\ 8) = 5$, sehingga $5 = 0 * 8 + 5$.

2.1.6 Algoritma *Lehmann*

Algoritma *Lehmann* adalah salah satu algoritma yang digunakan untuk menguji bilangan prima. Langkah-langkah pada algoritma *Lehmann* adalah sebagai berikut :

1. Membangkitkan bilangan acak $n, 1 \leq n \leq p$ (p adalah bilangan prima yang diuji keprimaannya).
2. Menghitung $n^{\frac{p-1}{2}}\ (mod\ p)$.
3. Apabila $n^{\frac{p-1}{2}} \not\equiv 1$ atau $-1\ (mod\ p)$, maka p tidak prima.
4. Jika $n^{\frac{p-1}{2}} \equiv 1$ atau $-1\ (mod\ p)$, maka peluang p prima adalah 50%.
5. Mengulangi langkah kedua sebanyak t kali dengan nilai n yang berbeda. Jika hasil perhitungannya sama dengan 1 atau -1, namun tidak selalu sama dengan 1, naka peluang p adalah bilangan prima memiliki kesalahan tidak lebih dari $\frac{1}{2}^t$.

Pengujian dengan algoritma *Lehmann* dapat menggunakan bilangan acak yang dipilih dari nilai terkecil agar proses perhitungan lebih cepat.

Contoh:

Ujilah keprimaan dari bilangan $p = 31$ menggunakan algoritma *Lehmann***.**

$a = 1 \rightarrow 1^{\frac{31-1}{2}}\ (mod\ 31) \equiv 1\ (mod\ 31)$

$a = 2 \rightarrow 2^{\frac{31-1}{2}}\ (mod\ 31) \equiv 1\ (mod\ 31)$

$a = 3 \rightarrow 3^{\frac{31-1}{2}} \ (mod\ 31) \not\equiv 1 \ (mod\ 31)$

$a = 4 \rightarrow 4^{\frac{31-1}{2}} \ (mod\ 31) \equiv 1 \ (mod\ 31)$

$a = 5 \rightarrow 5^{\frac{31-1}{2}} \ (mod\ 31) \equiv 1 \ (mod\ 31)$

$a = 6 \rightarrow 6^{\frac{31-1}{2}} \ (mod\ 31) \not\equiv 1 \ (mod\ 31)$

$a = 7 \rightarrow 7^{\frac{31-1}{2}} \ (mod\ 31) \equiv 1 \ (mod\ 31)$

$a = 8 \rightarrow 8^{\frac{31-1}{2}} \ (mod\ 31) \equiv 1 \ (mod\ 31)$

Jadi, 31 adalah bilangan prima karena memenuhi syarat $n^{\frac{p-1}{2}} \equiv 1$ atau $-1(mod\ p)$ sebanyak 6 kali yang sama atau sama dengan $\frac{1}{2}$ dari banyaknya perhitungan $(1 \leq n \leq 31)$.

2.1.7 Kongruensi

Definisi 2.4

Jika sebuah bilangan bulat m yang tidak nol, membagi selisih $a - b$, maka dapat dikatakan a kongruen dengan b modulo m, dan ditulis: $a \equiv b \ (mod\ m)$.

Jika $a - b$ tidak dibagi m, maka dapat dikatakan a tidak kongruen dengan b modulo m, dan ditulis $a \not\equiv b \ (mod\ m)$ (Irawan *et al*., 2014). Apabila $m > 0$ dan $m|a - b$, maka terdapat suatu bilangan bulat t sehingga $a - b = mt$.

Contoh

- $18 \equiv 2 \ (mod\ 4)$, karena $(18 - 2)$dapat terbagi oleh 4
- $8 \not\equiv 18 \ (mod\ 7)$, karena $(8 - 18)$ tidak dapat terbagi oleh 7

Teorema 2.6

Jika a, b dan c adalah bilangan bulat dan m bilangan asli, maka berlaku:

1. Refleksi $a \equiv a \ (mod\ m)$
2. Simetris, jika $a \equiv b \ (mod\ m)$ maka $b \equiv a \ (mod\ m)$
3. Transitif, jika $a \equiv b \ (mod\ m)$dan $b \equiv c \ (mod\ m)$ maka $a \equiv c \ (mod\ m)$

Bukti

1. Jika m≠ 0 maka $m|0$ yang dapat ditulis dengan $(m|a-a)$. Menurut definisi 2.3, maka berlaku $a \equiv a \ (mod\ m)$ untuk semua bilangan bulat a dan $m \neq 0$.
2. Berdasarkan definisi 2.3, apabila $a \equiv b \ (mod\ m)$ maka berarti $m|a-b$. Menurut definisi 2.3, ada keterbagian bilangan bulat t sehingga:

   $m|a-b$ dapat dinyatakan

   $$a - b = tm$$
   $$\Leftrightarrow -(a-b) = -tm$$
   $$\Leftrightarrow b - a = (-t)m$$

   Menurut definisi 2.3, hal ini berarti $b \equiv a \ (mod\ m)$.
3. $a \equiv b \ (mod\ m)$ berarti $m|a-b$ (menurut definisi 2.3)

   $b \equiv c \ (mod\ m)$ berarti $m|b-c$ (menurut definisi 2.3)

   Menurut definisi 2.3, ada keterbagian bilangan bulat t_1 dan t_2 sehingga:

   $m|a-b$ dapat dinyatakan $a - b = t_1 m$

   $m|b-c$ dapat dinyatakan $b - c = t_2 m$

   Kedua persamaan dijumlahkan sehingga diperoleh:

   $$a - c = (t_1 + t_2)m$$

   Hal ini menurut definisi 2.3 dapat ditulis dengan $a \equiv c \ (mod\ m)$.

Teorema 2.7

Jika a, b dan c adalah bilangan bulat dan n bilangan asli, maka berlaku

1. Jika $a \equiv b \ (mod\ m)$, maka $a + c \equiv b + c \ (mod\ m)$
2. Jika $a \equiv b \ (mod\ m)$, maka $ac \equiv bc \ (mod\ m)$

Bukti

1. Berdasarkan definisi 2.3 $a \equiv b \ (mod\ m)$, maka $n|a - b$, menurut definisi 2.3 ada bilangan bulat t sehingga $a - b \ = tm$

$$\Leftrightarrow \ (a - b) + 0 = tm$$

$$\Leftrightarrow (a - b) + (c - c) = tm$$

$$\Leftrightarrow \ (a + c) - (b + c) = tm$$

Sehingga berdasarkan definisi 2.3 diperoleh $a + c \equiv b + c(mod\ m)$

2. Menurut definisi 2.3 $a \equiv b \ (mod\ m)$ maka $m|a - b$, menurut definisi 2.3 ada bilangan t sehingga $a - b \ = tm$

$$\Leftrightarrow \ (a - b)c = (tm)c$$

$$\Leftrightarrow \ ac - bc \ = (tc)m$$

Sehingga diperoleh $ac \equiv bc \ (mod\ m)$.

Definisi 2.5 Sistem Residu

Jika $a \equiv b \ (mod\ m)$, maka b disebut residu dari x modulo m. Himpunan $a_1, a_2, a_3, \dots, a_m$disebut sebagai sistem residu lengkap modulo m, jika untuk setiap bilangan bulat b ada suatudan hanya satu a_i sehingga $b \equiv a_i \ (mod\ m)$.

Berdasarkan definisi 2.4, jelas bahwa ada tak terhingga banyak sistem residu lengkap modulo m, seperti $0, 1, 2, \dots, m - 1, m$. Himpunan m-buah bilangan bulat- bilangan bulat ini dikatakan membentuk residu lengkap modulo m

jika dan hanya jika tidak ada dua bilangan bulat yang kongruen dalam himpunan tersebut yang kongruen modulo m.

Teorema 2.8

Jika $b \equiv c \ (mod\ m)$, maka $(b, m) = (c, m)$

Bukti

$b \equiv c \ (mod\ m)$ berarti $m|b - c$. Berdasarkan teorema 2.2 pada keterbagian sehingga:

Jika $(b, m)|m$ dan $m|b - c$, maka $(b, m)|(b - c)$

Jika $(b, m)|b$ dan $(b, m)|b - c$, maka $(b, m)|c$

Jadi, jika $(b, m)|m$ dan $(b, m)|c$, maka (b, m), (b, m) adalah pembagi persekutuan m dan c.

Ini berarti $(b, m)|(c, m)$.....(1)

$c \equiv b \ (mod\ m)$ berarti $m|(c - b)$

Menurut teorema 2.2 pada keterbagian sehingga:

Jika $(c, m)|m$ dan $m|c - b$, maka $(c, m)|(c, b)$

Jika $(c, m)|c$ dan $(c, m)|c - b$, maka $(c, m)|b$

Jadi, jika $(c, m)|m$ dan $(c, m)|b$, maka (c, m), (c, m) adalah pembagi persekutuan m dan b.

Ini berarti $(c, m)|(b, m)$.....(2)

Jadi, dari (1) dan (2) menunjukkan bahwa:

$$(b, m) = (c, m)$$

2.1.8 Kongruensi Linier

Definisi 2.6

Misalkan $s_1, s_2, s_3, \cdots, s_m$ adalah suatu sistem residu lengkap modulo m. Banyaknya selesaian dari $f(x) \equiv 0 \ (mod\ m)$ adalah banyaknya s_i yang memenuhi $f(s_i) \equiv 0 \ (mod\ m)$.

Definisi 2.7

Kongruensi sederhana berderajat satu disebut kongruensi linier yang berbentuk $ax \equiv b \ (mod\ m)$; dengan $a, b, m \in Z, a \neq 0$ dan $m > 0$

Teorema 2.9

Kongruensi linier $ax \equiv b \ (mod\ m)$ dapat diselesaikan hanya jika $d = (a, m)$ membagi b, dan pada kasus ini memiliki d selesaian. Bila a dan m relatif prima atau $d = 1$, maka kongruensi memiliki satu selesaian.

Bukti

Kongruensi $ax \equiv b \ (mod\ m)$ mempunyai selesaian, berarti $m|ax - b$.

Andaikan $d \nmid b$.

$d = (a, m) \rightarrow d|a \rightarrow d|x$

$d|ax$ dan $d \nmid b \rightarrow d \nmid ax - b$

$d = (a, m) \rightarrow d|m$

$d|m$ dan $d \nmid b \rightarrow m \nmid ax - b$

$m \nmid ax - b$ bertentangan dengan $m|ax - b$. Jadi, $d|b$.

Diketahui $d|b$, dan $d = (a, m) \rightarrow d|a$ dan$d|m$

$d|a,\ d|m,$ dan $d|b \rightarrow a/d, m/d,$ dan $b/d \in Z$

$ax \equiv b \ (mod\ m) \rightarrow m|ax - b$

$m|ax - b$ dan $a/d, m/d,$ dan $b/d \rightarrow m/d|\ ax/d - b/d$

$m/d|\, ax/d - b/d \rightarrow \frac{ax}{d} \equiv b/d \ (mod\ m/d)$

Misal selesaian kongruensi dari $ax/d \equiv b/d \ (mod\ m/d)$ adalah $x = x_0;\ x_0 < m/d$, maka sebarang selesaiannya berbentuk: $x = x_0 k.m/d\,; k \in Z$; yaitu $x_0,\ x_0 + m/d\,, x_0 + 2m/d\,, \ldots, x_0 + (d-1)m/d$ yang seluruhnya memenuhi kongruensi dan seluruhnya mempunyai d selesaian.

Jika a dan m relatif prima, $d = (a,m) = 1$, maka selesaiannya didapat $x = x_0$ yang memenuhi kongruensi dan mempunyai satu selesaian

Teorema 2.10 Kongruensi Simultan

Kongruensi simultan $x \equiv a\ (mod\ m),\ x \equiv b\ (mod\ n)$ dapat diselesaikan hanya jika $a \equiv b\ \big(mod\ (m,n)\big)$ dan memiliki selesaian tunggal yaitu $x \equiv x_0\ \big(mod\ (m,n)\big)$.

Bukti

Diketahui kongruensi $x \equiv a\ (mod\ m),\ x \equiv b\ (mod\ n)$.

Kongruensi pertama $x \equiv a\ (mod\ m) \rightarrow x = a + mk; k \in Z$, kemudian dengan kongruensi kedua harus memenuhi:

$a + mk \equiv b\ (mod\ n)$, atau $mk \equiv b - a\ (mod\ n)$.

Menurut teorema 2.7, $mk \equiv b - a\ (mod\ n)$ dapat diselesaikan jika $d|b - a$; $d = (m,n)$, atau dengan kata lain kondisi $a \equiv b\ (mod\ (m,n))$ harus dipenuhi. $d = (m,n) \rightarrow d|m$ dan $d|n$.

Jika $d|m$, $d|n$, dan $d|b - a$, maka $m/d, n/d, (b-a)/d \in Z$.

$m/d, n/d, (b-a)/d \in Z$ dan $mk \equiv b - a\ (mod\ n)$ mengakibatkan

$mk/d \equiv (b-a)/d\ (mod\ n/d)$.

Dari teorema 2.7, jika $d = (m,n)$, maka $(m/d\,, n/d) = 1$.

$(m/d\,, n/d) = 1$ dan $mk/d \equiv (b-a)/d \pmod{n/d} \rightarrow mk/d \equiv (b-a)/d \pmod{n/d}$ mempunyai satu penyelesaian.

Misalkan penyelesaiannya adalaha $k \equiv k_0$ sehingga selesaiannya adalah

$k \equiv k_0 \pmod{n/d}$ atau

$k \equiv k_0 + n/d\,.r; r \in Z$

Karena $x = a + mk$ dan $k \equiv k_0 + n/d\,.r$, maka

$$x = a + mk$$

$= a + m(k_0 + n/d\,.r)$

$= (a + mk_0) + (m\,n/d\,.r)$

$= (a + mk_0) + (m,n).r$; karena $(m,n)(m,n) = mn$

$= x_0 + (m,n).r$; sebab $x_0 = a + mk_0$ sehingga $x = x_0 \pmod{(m,n)}$.

Teorema 2.11 ***Chinese Remainder Theorem*** **(CRT)**

Jika $m_1, m_2, \ldots, m_r \in Z$ dan $(m_i, m_j) = 1$ untuk $i \neq j$, maka kongruensi simultan

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

mempunyai selesaian $x \equiv \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \pmod{m}$.

Bukti

Misalkan $M = m_1 m_2 \cdots m_r$.

$\frac{m}{m_j} (j = 1, 2, \ldots, r)$ adalah bilangan bulat yang tidak memuat m_j.

Jika $\left(\frac{m}{m_j}\right) = 1$ maka terdapat bilangan bulat b_j sedemikian hingga:

$\left(\frac{m}{m_j}\right) b_j = 1 \pmod{m_j}$ yang mempunyai satu penyelesaian.

Karena $\left(\frac{m}{m_j}\right)$ masih memuat m_i, maka untuk $i = j$ berlaku:$\left(\frac{m}{m_j}\right) b_j = 0\ (mod\ m_i)$.

Dengan mengambil $x \equiv \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \pmod{m}$, maka

$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \cdots + \frac{m}{m_i} b_i a_i + \cdots + \frac{m}{m_r} b_r a_r.$

Dalam modulo $m_i (i = 1, 2, \ldots, r)$, x_0 dapat dinyatakan dengan:

$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \cdots + \frac{m}{m_i} b_i a_i + \cdots + \frac{m}{m_r} b_r a_r$

$x_0 = \frac{m}{m_1} b_1 a_1\ (mod\ m_i) + \frac{m}{m_2} b_2 a_2\ (mod\ m_i) + \cdots + \frac{m}{m_i} b_i a_i\ (mod\ m_i) + \cdots +$

$\frac{m}{m_r} b_r a_r\ (mod\ m_i)$.

Karena $\left(\frac{m}{m_j}\right) b_j = 1\ (mod\ m_j)$ dan untuk $i = j$ berlaku $\left(\frac{m}{m_j}\right) b_j$, maka:

$\frac{m}{m_1} b_1 \equiv 0\ (mod\ m_i)$, $\frac{m}{m_2} b_2 \equiv 0\ (mod\ m_i)$, ..., $\frac{m}{m_i} b_i \equiv 1\ (mod\ m_i)$, ..., $\frac{m}{m_r} b_r \equiv$

$0\ (mod\ m_i)$ sehingga:

$\frac{m}{m_1} b_1 a_1 \equiv 0\ (mod\ m_i)$, $\frac{m}{m_2} b_2 a_2 \equiv 0\ (mod\ m_i)$, ..., $\frac{m}{m_i} b_i a_i \equiv a_i\ (mod\ m_i)$, ...,

$\frac{m}{m_r} b_r a_r \equiv 0\ (mod\ m_i)$.

Jadi, $x_0 \equiv 0\ (mod\ m_i) + 0\ (mod\ m_i) + \cdots + a_i\ (mod\ m_i) + \cdots + 0\ (mod\ m_i)$

$x_0 \equiv a_i\ (mod\ m_i)$

Karena $i = 1, 2, \ldots, r$, maka $x_0 \equiv a_1\ (mod\ m_1)$, $x_0 \equiv a_2\ (mod\ m_2)$, ..., $x_0 \equiv$

$a_r\ (mod\ m_r)$.

Berarti x_0 memenuhi semua kongruensi $x_0 \equiv a_i\ (mod\ m_i)$ atau x_0 merupakan penyelesaian persekutuan dari semua kongruensi $x_0 \equiv a_i\ (mod\ m_i)$.

Karena $(m_i, m_j) = 1$ untuk $i = j$, maka $x_0 \equiv a_i\ (mod\ [m_1, m_2, \ldots, m_r])$, sebab $[m_1, m_2, \ldots, m_r] = m_1, m_2, \ldots, m_r = m$ sehingga $x_0 \equiv a_i\ (mod\ m)$.

Jadi, selesaian persekutuan kongruensi linier simultan adalah:

$$x \equiv \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \pmod{m}.$$

$$M_k = \frac{M}{m_k} = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r$$

yang sama dengan M, tetapi faktor m_k nya dihilangkan.

Diketahui bahwa $FPB(m_i, m_j) = 1$ dengan $i \neq j$ (artinya, m_i dan m_j relatif prima). Dengan demikian, $FPB(M_k, m_k) = 1$.

2.1.9 Residu Kuadrat

Definisi 2.8

Jika m bilangan bulat positif dan a adalah bilangan bulat, a dikatakan residu kuadratis dari m jika $(a, m) = 1$ dan kongruensi $x^2 \equiv a \ (mod\ m)$ mempunyai selesaian. Jika kongruensi $x^2 \equiv a \ (mod\ m)$ tidak mempunyai selesaian, maka a merupakan bukan kuadratis residu dari m.

Contoh

Tentukan bilangan kuadratis dari 11.

Untuk menghitung kuadrat-kuadrat dari bilangan $1, 2, 3, 4, 5, \ldots, 10$, diperoleh sebagai berikut:

$$1^2 \equiv 10^2 \equiv 1 \ (mod\ 11)$$

$$2^2 \equiv 9^2 \equiv 4 \ (mod\ 11)$$

$$3^2 \equiv 8^2 \equiv 9 \ (mod\ 11)$$

$$4^2 \equiv 7^2 \equiv 5 \ (mod\ 11)$$

$$5^2 \equiv 6^2 \equiv 3 \ (mod\ 11)$$

Dengan demikian, residu kuadratis dari 11 adalah $1, 3, 4, 5$, dan 9. Bilangan bulat $2, 6, 7, 8$, dan 10 bukanlah residu kuadratis dari 11.

Lemma 2.2

Misalkan p adalah bilangan prima ganjil dan a bilangan bulat yang tidak habis dibagi oleh p, maka kongruensi $x^2 \equiv a\ (mod\ p)$ yang tidak mempunyai penyelesaian atau mempunyai tepat dua yang tidak kongruen modulo p.

Bukti

Jika $x^2 \equiv a\ (mod\ p)$ mempunyai penyelesaian, misalkan $x = x_0$ maka kita dapat menunjukkan bahwa $x = -x_0$ merupakan penyelesaian kongruen yang kedua. Karena $(-x_0)^2 = x_0^2 \equiv a\ (mod\ p)$, kita lihat $-x_0$ merupakan penyelesaian. Ingat bahwa $x_0 \neq -x_0\ (mod\ p)$, maka kita mempunyai $2x_0 \equiv 0\ (mod\ p)$. Hal ini tidak mungkin, karena p ganjil dan $p|x_0$ (karena $x_0^2 \equiv a\ (mod\ p)$ dan $p|a$).

Untuk menunjukkan bahwa tidak terdapat lebih dari dua penyelesaian yang kongruen, dimisalkan $x = x_0$ dan $x = x_1$ keduanya merupakan penyelesaian dari $x^2 \equiv a\ (mod\ p)$. Maka kita mempunyai $x_0^2 \equiv x_1^2 \equiv a\ (mod\ p)$, sehingga $x_0^2 - x_1^2 = (x_0 + x_1)(x_0 - x_1) \equiv 0\ (mod\ p)$, menurut teorema pembagian $p|(x_0 + x_1)$ atau $p|(x_0 - x_1)$, sehingga $x_1 \equiv x_0\ (mod\ p)$,

Dengan demikian, terbukti jika terdapat penyelesaian dari $x^2 \equiv a\ (mod\ p)$, maka akan terdapat dua tepat penyelesaian yang tidak kongruen modulo p.

Teorema 2.12

Jika p bilangan prima ganjil, maka terdapat tepat $\frac{p-1}{2}$ residu kuadrat dari p dan $\frac{p-1}{2}$ bukan residu kudratis dari p diantara bilangan bulat $1, 2, \dots, p-1$.

Bukti

Untuk mencari semua residu kuadrat dari p diantara bilangan bulat $1, 2, 3, \dots, p-1$, terlebih dahulu kita menghitung residu positif terkecil modulo p terhadap kuadrat-kuadrat dari bilangan bulat $1, 2, 3, \dots, p-1$. Karena terdapat sebanyaka $(p-1)$ buah kuadrat yang diperhatikan dan karena setiap kongruensi $x^2 \equiv a \ (mod\ p)$ mempunyai tidak atau dua penyelesaian haruslah terdapat tepat $\frac{p-1}{2}$ residu kuadrat dari p diantara bilangan bulat $1, 2, 3, \dots, p-1$. Sisanya sebanyak $p-1-\frac{p-1}{2} = \frac{p-1}{2}$ bilangan bulat positif yang kurang dari $p-1$ bukan merupakan residu kuadratis dari p.

Definisi 2.9

Misalkan p bilangan prima ganjil dan a bilangan bulat yang tidak habis dibagi oleh p. Simbol *Legendre* $\frac{a}{p}$.

Didefinisikan $\left[\frac{a}{p}\right] = \begin{cases} 1 \text{ jika } a \text{ residu kuadratis dari } p \\ -1 \text{ jika } a \text{ bukan residu kuadratis dari } p \end{cases}$

Teorema 2.13 Kriteria *Euler*

Misalkan p bilangan prima ganjil dan $p|a$ dengan a bilangan bulat positif, maka $\left[\frac{a}{p}\right] \equiv a^{\frac{p-1}{2}} \ (mod\ p)$.

Bukti

Andaikan $\left[\frac{a}{p}\right] = 1$, maka kongruensi $x^2 \equiv a \ (mod\ p)$ mempunyai penyelesaian, misalkan $x = x_0$. Dengan menggunakan teorema kecil Fermat yang menyatakan jika p adalah bilangan prima dan $p|a$, maka $a^{p-1} \equiv 1 \ (mod\ p)$, sehingga kita akan lihat bahwa $a^{\frac{p-1}{2}} = (x_0^2)^{\frac{p-1}{2}} = x^{\beta-1} \equiv 1 \ (mod\ p)$. Perhatikan bahwa untuk kasus $\left[\frac{a}{p}\right] = -1$. Karena, jika $\left[\frac{a}{p}\right] = 1$, kita tahu bahwa $\left[\frac{a}{p}\right] \equiv a^{\frac{p-1}{2}} \ (mod\ p)$. Maka

kongruensi $x^2 \equiv a\ (mod\ p)$ tidak punya penyelesaian. Untuk setiap bilangan bulat i sehingga $1 \leq i \leq p-1$ terdapat bilangan bulat j yang tunggal dengan dengan $1 \leq j \leq p-1$, sedemikian sehingga $ij \equiv a\ (mod\ p)$. Selanjutnya, karena kongruensi $x^2 \equiv a\ (mod\ p)$ tidak punya penyelesaian dan kita tahu bahwa $i \neq j$. Maka kita dapat mengelompokkan bilangan bulat $1, 2, \dots, p-1$ ke dalam $\frac{p-1}{2}$ pasang yang masing-masing mempunyai hasil kali sama dengan a. Dari perkalian pasangan ini diperoleh $(p-1)! \equiv a^{\frac{p-1}{2}}\ (mod\ p)$, karena teorema Wilson mengatakan bahwa $(p-1)! = -1\ (mod\ p)$, maka kita lihat bahwa $-1! \equiv a^{\frac{p-1}{2}}\ (mod\ p)$. Dengan demikian, $\left[\frac{a}{p}\right] \equiv a^{\frac{p-1}{2}}\ (mod\ p)$.

Lemma 2.3 Akar Kuadrat Modulo p

Misalkan p adalah bilangan prima dan $a^2 \equiv 1\ (mod\ p)$. Maka, $a \equiv \pm 1\ (mod\ p)$.

Bukti

$a^2 \equiv 1\ (mod\ p)$ berarti $p|a^2 - 1 = (a+1)(a-1)$.

Dengan demikian, untuk $p|a-1$ yang artinya $a \equiv 1\ (mod\ p)$ atau $p|a+1$ yang berarti $a \equiv -1\ (mod\ p)$.

2.1.10 Kriptografi

Kriptografi merupakan suatu ilmu matematika yang digunakan untuk mengamankan suatu pesan atau data. Menurut Menezes (1996) kriptografi adalah suatu ilmu yang mempelajari metode matematika yang berhubungan dengan aspek keamanan informasi meliputi kerahasiaan, otentikasi, dan integritas data. Terdapat empat hal terpenting dalam kriptografi, yaitu pesan asli (*plaintext*) yang dapat dibaca dan dimengerti maknanya, kunci (*cryptography key*), pesan yang tersandi

($ciphertext$), dan proses enkripsi dan dekripsi. Enkripsi merupakan proses penyandian atau mengubah *plaintext* menjadi *ciphertext*, sedangkan dekripsi merupakan proses mengubah *ciphertext* menjadi *plaintext.* Enkripsi dan dekripsi juga merupakan suatu fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut (Ollinka, 2021). Misalkan P merupakan *plaintext* dan C merupakan *ciphertext*, maka:

Fungsi enkripsi (E) memetakan P ke C:

$E(P) = (C)$

dan fungsi dekripsi (D) memetakan C ke P:

$D(C) = (P)$.

Kriptografi memiliki empat tujuan mendasar dalam mengamankan suatu pesan sebagai berikut (Munir, 2006):

1. Kerahasiaan (*confidentiality*), data atau pesan hanya bisa diterima dan diakses oleh phak tertentu saja.
2. Otentikasi (*authentication*), pengirim yang menjadi perantara dan penerima mengetahui pengirim pesan yang sebenarnya.
3. Integritas data (*integrity*), pesan yang dikirimkan dan sampai kepada penerimanya sangat terjaga tanpa ada sabotase isi pesan.
4. Ketiadaan penyangkalan (*nonrepudiation*), upaya sebagai pencegahan adanya sifat saling mengingkari antara pengirim maupun penerima bahwa mereka telah mengirim atau menerima pesan/informasi.

Kunci (*cryptography key*) berperan penting sebagai pengendali jalannya suatu algoritma kriptografi. Berdasarkan kuncinya, algoritma kriptografi dibagi menjadi dua jenis, yaitu:

1. Algoritma Simetris

   Algoritma simetris adalah algoritma yang hanya menggunakan satu kunci dalam proses enkripsi maupun dekripsinya. Contoh algoritma simetris adalah *Blowfish*, DES, AES, XOR, dan CBC. Kelebihan yang dimiliki pada algoritma simetris adalah waktu pada proses enkripsi maupun dekripsinya lebih cepat dibanding algoritma asimetris. Tingkat keamanan yang dimiliki algoritma ini bergantung pada kuncinya, sehingga apabila kunci yang digunakan bocor atau diketahui orang lain, maka orang yang tidak berhak menerimanya dapat mengetahui isi pesan rahasia yang dikirimkan.

2. Algoritma Asimetris

   Algoritma asimetris adalah algoritma yang mempunyai dua kunci, yaitu kunci publik yang digunakan untuk proses enkripsi pesan dan kunci privat yang digunakan pada proses dekripsi pesan (Ollinka, 2021). Contoh dari algoritma asimetris adalah RSA, ElGamal, DSA, dan Rabin.

2.1.11 *Hybrid Cryptosystem*

Hybrid Cryptosystem adalah algoritma kriptografi yang memanfaatkan dengan menggabungkan keunggulan yang dimiliki algoritma simetris dan algoritma asimetris. Pada skema proses enkripsinya (*hybrid encryption*) dilakukan dengan dua cara, yaitu teknik enkripsi kunci publik terhadap *symmetric key* sehingga menghasilkan *shared key* yang akan dikirim kepada penerima dan teknik enkripsi *symmetric key* yang digunakan untuk mengenkripsi pesan asli (*plaintext)* yang menghasilkan *ciphertext* yang ditujukan kepada penerima. Pada proses

dekripsinya (*hybrid decryption*), dilakukan juga dengan dua cara, yaitu teknik dekripsi kunci publik terhadap *shared key* sehingga menghasilkan *symmetric key* dan teknik dekripsi *symmetric key* terhadap *ciphertext* menggunakan *symmetric key* sehingga menghasilkan pesan asli (*plaintext*).

2.1.12 Algoritma *Cipher Block Chaining*

Algoritma *Cipher Block Chaining* (CBC) adalah algoritma yang menerapkan mekanisme umpan balik pada sebuah blok (Wijayanto, 2021). Pada proses enkripsinya, *plaintext* diubah ke dalam bentuk blok dengan panjang yang sama dan blok yang *current* di-XOR-kan dengan blok *ciphertext* dari hasil enkripsi sebelumnya, kemudian hasil peng-XOR-an akan masuk dalam proses enkripsi blok selanjutnya. Dalam algoritma CBC, terdapat kasus khusus pada *block cipher* pertama yang belum memiliki ciphertext sebelumnya, sehingga diperlukan suatu *Initial Vector* (*IV*) yang akan digunakan dalam pengoperasian awal algoritma CBC. IV yang disimbolkan dengan C_0 ini juga akan digunakan pada proses dekripsi blok *ciphertext* pertama sehingga menghasilkan blok *plaintext* yang akan digunakan pada dekripsi blok *ciphertext* selanjutnya. Nilai dari IV dapat dinyatakan sebagai konstanta dan tidak bersifat rahasia (Wijayanto, 2021). Algoritma CBC secara sistematis dapat dinyatakan sebagai berikut:

Enkripsi: $C_i = Ek(P_i \oplus C_{i-1}) = (P_i \oplus C_{i-1}) \oplus K;\ i = 1, 2, \dots, m$

Dekripsi: $P_i = Dk(C_i \oplus C_{i-1}) = (C_i \oplus C_{i-1}) \oplus K; i = 1, 2, \dots, m$

Proses enkripsi algoritma CBC dapat diuraikan sebagai berikut::

$C_i = Ek(P_i \oplus C_{i-1})$ (Rumus Enkripsi)

$C_i = (P_i \oplus C_{i-1}) \oplus K$ (Rumus Enkripsi)

$C_i = P_i \oplus (C_{i-1} \oplus K)$ (Sifat Asosiatif terhadap operasi $\oplus$)

Akan ditunjukkan bahwa persamaan dekripsi algoritma CBC merupakan invers dari persamaan enkripsinya menggunakan sifat-sifat dari operasi XOR sebagai berikut:

$P_i = Dk(C_i \oplus C_{i-1})$ (Rumus Dekripsi)

$P_i = (C_i \oplus C_{i-1}) \oplus K$ (Rumus Dekripsi)

$P_i = C_i \oplus (C_{i-1} \oplus K)$ (Sifat Asosiatif terhadap operasi $\oplus$)

sehingga:

$P_i = \big(P_i \oplus (C_{i-1} \oplus K)\big) \oplus (C_{i-1} \oplus K)$ (Substitusi $C_i = P_i \oplus (C_{i-1} \oplus K)$)

$P_i = P_i \oplus (C_{i-1} \oplus K) \oplus (C_{i-1} \oplus K)$ (Sifat Asosiatif terhadap operasi $\oplus$)

$P_i = P_i$ (Sifat identitas operasi $\oplus$)

Dengan demikian, terbukti bahwa dekripsi algoritma CBC merupakan invers dari enkripsi algoritma CBC.

2.1.13 Algoritma *Rabin*

Algoritma *Rabin* merupakan turunan dari algoritma RSA. Algoritma *Rabin* menggunakan pemfaktoran bilangan untuk mengamankan pesan dan akan menghasilkan empat kemungkinan dari hasil dekripsinya, sehingga pnerima perlu menentukan *plaintext* mana yang benar (Ollinka, 2021). Pada algoritma *Rabin*, terdapat dua kunci yang berbeda, yaitu kunci publik dan kunci privat. Kunci publik dapat diketahui dan disebarkan secara umum, sedangkan kunci privat bersifat rahasia dan hanya diketahui oleh pengguna. Kunci publik akan digunakan dalam proses enkripsi dan kunci privat digunakan dalam proses dekripsi dalam algoritma *Rabin*. Algoritma Rabin bergantung pada kesulitan memfaktorkan

bilangan besar (Budiman, 2019). Jika kunci yang digunakan semakin besar, maka semakin sulit algoritma Rabin disusupi oleh pihak yang tidak diinginkan. Proses enkripsi menggunakan algoritma *Rabin* adalah sebagai berikut (Ollinka, 2021):

1. Proses pembangkitan kunci
    a. Menentukan bilangan prima p dan q yang merupakan kunci privat untuk memfaktorkan kunci publik dengan syarat:
    $p \equiv q \equiv 3\ (mod\ 4)$ atau $p\ (mod\ 4) = 3$ dan $q\ (mod\ 4) = 3$.
    b. Menghitung nilai kunci publik (n) dengan $n = p * q$.
2. Proses Enkripsi
    a. Mengubah nilai *plaintext* (m) menjadi biner berdasarkan tabel ASCII.
    b. Menambahkan m dengan nilai biner m itu sendiri (*redundant information*).
    c. Mengubah hasil penggandaan m menjadi nilai desimal.
    d. Menghitung nilai *ciphertext* dengan persamaan sebagai berikut:
    $$c = (m^2)\ (mod\ n)$$
    e. Mendapatkan *cipher*text.

Berdasarkan prosedur pembangkitan kunci, diperoleh kunci publik adalah n yang diperoleh dari persamaan $n = p.q$ di mana p dan q merupakan kunci privat yang memenuhi kekongruenan $p \equiv q \equiv 3\ (mod\ 4)$. Rosen (2011) menyatakan bahwa proses enkripsi algoritma *Rabin* dilakukan dengan menggunakan persamaan $c = m^2(mod\ n)$, sehingga persamaan yang digunakan untuk proses dekripsi algoritma Rabin adalah $m^2 \equiv c\ (mod\ n)$, di mana $0 < c < n$ dan $(c, n) = 1$. Berdasarkan definisi 2.8, maka kongruensi $m^2 \equiv c\ (mod\ n)$ mempunyai selesaian $m = m_0$. Karena $n = p.q$, maka:

$$m^2 \equiv c \ (mod\ p)$$

$$m^2 \equiv c \ (mod\ q)$$

Selanjutnya, akan ditunjukkan bahwa terdapat empat akar kuadrat modulo n. Misalkan $m_0 \equiv m_1 \ (mod\ p), 0 < m_1 < p$ dan $m_0 \equiv m_2 \ (mod\ q), 0 < m_2 < q$. Berdasarkan Lemma 2.2, $m^2 \equiv c \ (mod\ p)$ mempunyai dua solusi tepat yang tidak kongruen modulo p yang disebut sebagai:

$$m \equiv m_1 \ (mod\ p) \text{ dan } m \equiv p - m_1 \ (mod\ p)$$

Hal ini juga berlaku untuk $m^2 \equiv c \ (mod\ q)$, sehingga:

$$m \equiv m_2 \ (mod\ q) \text{ dan } m \equiv q - m_2 \ (mod\ q)$$

Dari teorema 2.11 *Chinese Remainder Theorem*, maka terdapat empat solusi yang tidak kongruen dengan modulo n dari kongruensi $m^2 \equiv c \ (mod\ n)$, yaitu:

1. $m \equiv m_1 \ (mod\ p)$

   $m \equiv m_2 \ (mod\ q)$

2. $m \equiv m_1 \ (mod\ p)$

   $m \equiv q - m_2 \ (mod\ q)$

3. $m \equiv p - m_1 \ (mod\ p)$

   $m \equiv m_2 \ (mod\ q)$

4. $m \equiv p - m_1 \ (mod\ p)$

   $m \equiv q - m_2 \ (mod\ q)$

Selanjutnya, karena $p \equiv q \equiv 3 \ (mod\ 4)$, maka solusi dari $m^2 \equiv c \ (mod\ p)$ dan $m^2 \equiv c \ (mod\ q)$ adalah

$$m \equiv \pm c^{\frac{(p+1)}{4}} \ (mod\ p) \text{ dan } m \equiv \pm c^{\frac{(q+1)}{4}} \ (mod\ q)$$

Dengan kriteria *Euler*, kita tahu bahwa:

$$c^{\frac{(p-1)}{2}} \equiv \left(\frac{c}{p}\right) = 1\ (mod\ p) \text{ dan } c^{\frac{(q-1)}{2}} \equiv \left(\frac{c}{q}\right) = 1\ (mod\ q)$$

Sebelumnya, kita telah mengasumsikan bahwa $m^2 \equiv c\ (mod\ pq)$ mempunyai sebuah solusi, maka c adalah residu kuadrat dari p dan q, sehingga:

$$\left(c^{\frac{(p+1)}{4}}\right)^2 = c^{\frac{(p+1)}{2}} = c^{\frac{(p-1)}{2}}.c \equiv c\ (mod\ p)$$

dan

$$\left(c^{\frac{(q+1)}{4}}\right)^2 = c^{\frac{(q+1)}{2}} = c^{\frac{(q-1)}{2}}.c \equiv c\ (mod\ q)$$

sehingga kita bisa menyatakan nilai akar kuadrat dari c terhadap p dan q sebagai:

$$m_p = c^{\frac{(p+1)}{4}}\ (mod\ p) \text{ dan } m_q = c^{\frac{(q+1)}{4}}\ (mod\ q).$$

Kemudian, kita akan mencari nilai Y_p dan Y_q yang merupakan persekutuan pembagi terbesar atau $FPB(p,q)$ menggunakan algoritma *Extended Euclidean.* Dengan solusi-solusi yang sudah kita dapatkan diatas, maka kita bisa mencari akar kuadrat dari c modulo n menggunakan *Chinese Remainder Theorem* dengan persamaan sebagai berikut:

$$r \equiv \left(Y_p.p.m_q + Y_q.q.m_p\right)\ (mod\ n)$$

$$s \equiv \left(Y_p.p.m_q - Y_q.q.m_p\right)\ (mod\ n)$$

$$t \equiv \left(-\left(Y_p.p.m_q\right) + Y_q.q.m_p\right)\ (mod\ n)$$

$$u \equiv \left(-\left(Y_p.p.m_q\right) - Y_q.q.m_p\right)\ (mod\ n)$$

Dengan demikian, langkah-langkah untuk proses dekripsi algoritma *Rabin* adalah sebagai berikut:

1. Menentukan nilai Y_p dan Y_q yang merupakan pembagi terbesar atau FPB dari *p* dan *q* menggunakan algoritma *Extended Euclidean*.

$$Y_p * p + Y_q * q = gc\,d(p,q) \Leftrightarrow Y_p * p + Y_q * q = 1$$

2. Menghitung nilai akar kuadrat *ciphertext* terhadap p dan q dengan rumus berikut:

$$m_p = \left(c^{\left(\frac{p+1}{4}\right)}\right) \ (mod\ p)$$

$$m_q = \left(c^{\left(\frac{q+1}{4}\right)}\right) \ (mod\ q)$$

dengan m_p adalah akar kuadrat *ciphertext* terhadap p dan m_q adalah akar kuadrat *ciphertext* terhadap *q.*

3. Menghitung nilai $r, s, t,$ dan u menggunakan *Chinese Remainder Theorem* dengan persamaan sebagai berikut:

$$v = Y_p * p * m_q$$

$$w = Y_p * q * m_p$$

sehingga:

$$r = (v + w)\ (mod\ n)$$

$$s = (v - w)\ (mod\ n)$$

$$t = (-v + w)\ (mod\ n)$$

$$u = (-v - w)\ (mod\ n)$$

4. Mengubah nilai desimal $r, s, t,$ dan u ke bentuk biner dan nilai biner dibagi menjadi dua bagian sama panjang. Kemudian, membandingkan kedua bagian. Apabila dari kedua bagian menghasilkan bentuk biner yang sama, maka akan didapatkan *plaintext*.

2.1.14 Bit-String

Dalam perkembangan algoritma kriptografi, terdapat dua jenis kriptografi, yaitu kriptografi klasik dan kriptografi modern. Pada kriptografi klasik, sistem

yang digunakan untuk menjalankan algoritma kriptografi adalah transposisi dan permutasi karakter dari teks asli (Ariyus, 2008). Pada kriptografi modern, karakter teks asli dikonversikan ke bentuk suatu urutan digit biner (bits), yaitu 0 dan 1 yang digunakan dalam skema *encoding American Standart Code for Information Interchange* (ASCII). Urutan bit inilah yang akan mewakili teks asli yang akan dienkripsi untuk mendapatkan teks-kode dalam bentuk urutan bit. Pada ASCII, diperlukan 8 bit untuk mendapatkan stu karakter dan blok kode mempunyai 64 bit untuk satu blok.

Terdapat dua metode yang dapat digunakan pada algoritma enkripsi, yaitu aliran kode dan blok kode. Pada aliran kode, urutan bit pada proses enkripsi menggunakan teknik *bit-by-bit* dan bit pada teks asli tidak sama dengan bit yang ada pada teks kode. Sedangkan pada blok kode, blok teks asli dan blok kode memiliki ukuran yang sama dan menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya (Ariyus, 2008). Setiap blok terdiri dari banyak bit, misalnya satu blok terdiri dari 64 bit atau 128 bit. Contoh, pada sekuen 12 bit: 100111010110. Apabila dipecah menjadi 3 blok, maka akan didapat 100 111 010 110. Bit-string dengan panjang 3 akan menghadirkan bilangan bulat dari 0 sampai 7 dengan urutan 4 7 2 6. Yang terpenting dalam bit-string adalah mengamati bahwa bit-string yang sama dapat mewakili urutan angka yang bergantung pada ukuran blok yang diinginkan.

$000 = 0, 001 - 1, 010 = 2, 011 = 3, 100 = 4, 101 = 5, 110 = 6, 111 = 7.$

String binari adalah operasi pada algoritma kode. Untuk mengkombinasikan dua bit pada string binari diperlukan suatu metode yang

disebut sebagai *Exclusive OR* dan bisa ditulis dengan XOR atau $\oplus$ yang digambarkan sebagai berikut:

$$0 \oplus 0 = 1, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0.$$

Hukum-hukum yang terkait dengan operasi XOR adalah:

1. $A \oplus A = 0$ (Hukum identitas)
2. $A \oplus B = B \oplus A$ (Hukum komutatif)
3. $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ (Hukum asosiatif)

2.2 Kajian Integrasi Topik Dengan Al-Qur'an

Amanah secara etimologi berasal dari bentuk *mashdar* pada kata kerja *amina-ya'manu-amana(tan*) yang berarti tenang, aman, dan tentram. Dalam hal ini, amanah merupakan sifat manusia yang apabila dijalankan dengan baik oleh seseorang maka ia dapat disebut sebagai "*al-Amin*", yang dapat dipercaya atau jujur dalam melakukan tanggung jawabnya (Fatimah, 2019). Secara terminologi, salah satu ulama bernama al-Maraghi memberikan pandangan tentang definisi amanah yang terdiri atas tiga bagian. Pertama, amanah merupakan tanggung jawab hamba dengan *Rabb*-nya dalam melaksanakan segala perintah-Nya dan menjauhi larangan-Nya. Kedua, amanah hamba terhadap sesamanya. Ketiga, amanah hamba terhadap dirinya sendiri (Haqqi, 2018).

Dalam surah Al-Anfal 27 yang artinya (LPMQ, 2022):

"Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui."

Ibn Katsīr menyebutkan riwayat dari kitab Ṣaḥīh Bukhārī dan Ṣaḥīh Muslim yang artinya: "Ada sebuah kisah tentang Hāṭib bin Abu Balṭa`ah r.a. bahwa dia pernah menulis surat kepada orang-orang Quraisy untuk memberitahukan mereka tentang tujuan Rasulullah saw. terhadap mereka di tahun kemenangan atas kota Makkah, maka Allah Swt. memperlihatkan hal itu kepada Rasul-Nya, lalu Rasulullah saw. mengirim suatu pasukan untuk mengejar dan mengambil surat tersebut. Lalu, Hāṭib dihadapkan kepad Rasulullah saw. dan dia mengakui perbuatannya. Pada saat itu, 'Umar bin Khaṭṭāb r.a. bangun dan berkata, "Wahai Rasulullah bolehkan aku memenggal batang lehernya karena dia telah berkhianat terhadap Allah, Rasul-Nya dan kaum mukminin?" Rasulullah saw. bersabda (Ad-Dimasyqi, 2005):

"Biarkanlah dia, karena sesungguhnya dia telah ikut dalam perang Badar. Tahukah kamu, mudah-mudahan Allah memperlihatkan ahli Badar dan Dia berfirman, "Berbuatlah sesuka kalian, sesungguhnya Aku telah memberikan ampunan bagi kalian."

Ibn Katsīr menyatakan bahwa pendapat yang benar adalah ayat tersebut bermakna umum, meskipun ayat tersebut turun karena suatu sebab yang khusus. Menurut jumhur ulama, yang dijadikan patokan adalah keumuman lafadz, bukan kekhususan sebab. Perbuatan khianat mencakup semua dosa kecil dan dosa besar, baik berakibat pada diri sendiri maupun pada orang lain. Ali bin Abi Ṭalḥah meriwayatkan dari Ibn 'Abbās r.a. bahwa sehubungan dengan firman Allah Swt. dalam surah Al-Anfal ayat 27 yang artinya,

"...Dan janganlah kamu mengkhianati amanah yang dipercayakan kepadamu."

Amanah adalah amal-amal perbuatan yang telah Allah Swt. percayakan kepada hamba-hamba-Nya, yaitu hal-hal yang fardu. Ibn 'Abbās r.a. berkata, "Janganlah kamu mengkhianati, yaitu janganlah kamu membatalkannya." Ibn

„Abbās r.a. juga berkata dalam riwayat yang lain berkenaan firman Allah tersebut, "Yaitu dengan meninggalkan perintah-Nya dan melakukan kemaksiatan terhadap-Nya. Ibn 'Abbās r.a. mengartikan: wa takhūnū amānātikum, amanah ialah amal perbuatan yang diamanahkan (diwajibkan) Allah Swt. atas hamba-Nya. Lā takhūnū: jangan kamu kurangi, jangan kamu teledor, dan jangan kamu mengabaikannya. Mengkhianati Rasul ialah meninggalkan sunnahnya dan melanggar larangannya.

Dengan demikian, amanah yang telah dijelaskan pada surah Al-Anfal ayat 27 bahwa amanah harus disampaikan kepada ahlinya dan berkaitan dengan konsep kriptografi dalam mengamankan suatu pesan teks rahasia agar tetap terjaga kerahasiaan isi pesan teks tersebut hingga sampai kepada penerima pesan.

2.3 Kajian Topik Dengan Teori Pendukung

Teori pendukung dalam penyusunan penelitian ini, seperti algoritma CBC yang merupakan kriptografi simetris dan algoritma *Rabin* yang merupakan kriptografi asimetris. Pada algoritma CBC membahas mengenai XOR untuk proses enkripsi dan dekripsinya. Proses enkripsi dilakukan dengan cara mengubah *plaintext* ke dalam bentuk blok dengan panjang yang sama dan blok yang *current* di-XOR-kan dengan blok *ciphertext* dari hasil enkripsi sebelumnya, kemudian hasil peng-XOR-an akan masuk dalam proses enkripsi blok selanjutnya. Dalam pengoperasian awal enkripsi, memerlukan suatu *Initial Vector* (IV) yang merupakan konstanta yang akan digunakan. IV yang disimbolkan dengan C_0 ini juga akan digunakan pada proses dekripsi blok *ciphertext* pertama sehingga

menghasilkan blok *plaintext* yang akan digunakan pada dekripsi blok *ciphertext* selanjutnya.

Pada algoritma Rabin, membahas tentang teori bilangan yang terdiri dari keterbagian, relatif prima, algoritma Lehmann untuk menguji bilangan prima, *Euclidean*, dan *Chinese Remainder Theorem.* Pada proses pembangkitan kunci, nilai p dan q ditentukan dari bilangan prima acak sebagai kunci privat dari algoritma *Rabin.* Kemudian, membangkit*kan* kunci publik (n) yang dilakukan dengan cara mengalikan p dan q. Selanjutnya, menambahkan *plaintext* (m) dengan nilai biner m itu sendiri (*redundant information*) dan mengubah hasil penggandaan m menjadi nilai desimal. Hasil enkripsi dari m diperoleh dengan menghitung rumus $c = (m^2)\ (mod\ n)$. Pada proses dekripsi, algoritma *Euclidean* digunakan untuk mencari FPB dari nilai p dan q. Kemudian, menghitung nilai akar kuadrat m terhadap p dan q dengan rumus $m_p = \left(c^{\left(\frac{p+1}{4}\right)}\right)\ (mod\ p)$ dan $m_q = \left(c^{\left(\frac{q+1}{4}\right)}\right)\ (mod\ q)$, di mana m_p adalah akar kuadrat *ciphertext* terhadap *p* dan m_q adalah akar kuadrat *ciphertext* terhadap q. Untuk menentukan empat kemungkinan dari hasil enkripsi algoritma *Rabin*, akan digunakan *Chinese Remainder Theorem* dengan persamaan sebagai berikut:

$$v = Y_p * p * m_q$$

$$w = Y_p * q * m_p$$

sehingga:

$$r = (v + w)\ (mod\ n)$$

$$s = (v - w)\ (mod\ n)$$

$$t = (-v + w)\ (mod\ n)$$

$$u = (-v - w)\ (mod\ n)$$

Nilai desimal $r, s, t,$ dan u diubah ke bentuk biner dan nilai biner akan dibagi menjadi dua bagian sama panjang. Selanjutnya, membandingkan kedua bagian. Apabila dari kedua bagian menghasilkan bentuk biner yang sama, maka akan didapatkan *plaintext*.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Pada penelitian ini, peneliti menggunakan jenis penelitian deskriptif dengan melakukan studi kepustakaan untuk mendapatkan berbagai informasi yang relevan terkait dengan pembahasan. Diawali dengan mencari informasi dari jurnal, artikel, tugas akhir, dan buku tentang algoritma CBC dan algoritma *Rabin*.

3.2 Pra Penelitian

Pada tahap pra penelitian, peneliti mempelajari dan mengkaji beberapa teori yang mendukung proses enkripsi dan dekripsi algoritma CBC dan algoritma Rabin sebagai berikut:

1. Algoritma XOR untuk membantu proses enkripsi dan dekripsi pada algoritma CBC.
2. Algoritma *Lehmann* untuk membantu dalam memilih bilangan prima sebagai kunci privat pada algoritma Rabin.
3. Algoritma *Extended Euclidean* untuk mencari nilai FPB dari kunci privat pada algoritma *Rabin*.
4. *Chinese Remainder Theorem* untuk menghitung empat kemungkinan hasil dekripsi pada algoritma Rabin.

3.3 Tahapan Penelitian

Adapun langkah-langkah yang dilakukan peneliti untuk mengetahui proses enkripsi dan dekripsi dalam mengamankan pesan teks menggunakan algoritma CBC dan *Rabin* sebagai *Hybrid Cryptosystem* yaitu:

3.3.1 Proses Enkripsi *Hybrid Cryptosystem* Menggunakan Algoritma CBC Dan Algoritma *Rabin*

1. Menentukan karakter alfabet kapital yang akan digunakan sebagai *plaintext.*
2. Menentukan nilai jumlah bit pada setiap blok. Pada penelitian ini, setiap blok memiliki dua karakter alfabet kapital.
3. Menentukan kunci simetri CBC dan *Initial Vector* (C_0) secara acak dan masing-masing berupa dua karakter alfabet kapital sesuai dengan panjang blok yang telah ditentukan sebelumnya.
4. Melakukan proses enkripsi algoritma CBC terhadap *plaintext* menggunakan kunci simetris CBC beserta *Initial Vector* (C_0), sehingga menghasilkan *cipher*text yang akan diterima oleh penerima pesan. Adapun proses enkripsinya sebagai berikut:
   a. Mengelompokkan *plaintext* ke dalam blok sesuai dengan jumlah bit per kelompok yang sudah ditentukan sebelumInitial Vectornya, yaitu dua karakter huruf untuk setiap bloknya.
   b. Melakukan proses enkripsi sebagai berikut:

$$C_i = Ek(P_i) \oplus C_{i-1}$$

   c. Menggeser 4 bit *plaintext* dari kiri.

d. Mendapatkan *ciphertext* C.

5. Menentukan nilai p dan q yang terdiri dari bilangan prima acak sebagai kunci privat dari algoritma *Rabin.*
6. Membangkitkan kunci publik (n) dengan persamaan berikut:

$$n = p * q$$

7. Melakukan proses enkripsi menggunakan algoritma kunci publik *Rabin* terhadap kunci simetris CBC dan *Initial Vector*, sehingga diperoleh *cipherkey* yang akan diberikan kepada penerima dengan langkah sebagai berikut:
   a. Kunci simetris CBC dan *Initial Vector* akan menjadi *plaintext* (m) dalam proses enkrispsi algoritma *Rabin.*
   b. Mengubah *plaintext* ke bentuk biner berdasarkan pada tabel ASCII.
   c. Menambahkan m dengan nilai biner m itu sendiri (*redundant information*).
   d. Mengubah hasil penggandaan m menjadi nilai desimal.
   e. Menghitung nilai *ciphertext* dengan persamaan sebagai berikut:

$$c = (m^2)\ (mod\ n)$$

   f. Mendapatkan *cipher*text dari algoritma *Rabin* yang selanjutnya akan disebut sebagai *cipherkey.*

3.3.2 Proses Dekripsi *Hybrid Cryptosystem* Menggunakan Algoritma CBC Dan Algoritma *Rabin*

1. Melakukan proses dekripsi pesan dengan algoritma *Rabin* menggunakan kunci privat terhadap *cipherkey*, sehingga diperoleh kunci simetris CBC dan *Initial Vector*.

   a. Menentukan nilai Y_p dan Y_q yang merupakan pembagi terbesar atau FPB dari *p* dan *q* menggunakan algoritma *Extended Euclidean*.

   $Y_p * p + Y_q * q = FPB(p, q) \Leftrightarrow Y_p * p + Y_q * q = 1$

   b. Menghitung nilai akar kuadrat *cipherkey* terhadap p dan q dengan rumus berikut:

   $$m_p = \left(c^{\left(\frac{p+1}{4}\right)}\right) \ (mod\ p)$$

   $$m_q = \left(c^{\left(\frac{q+1}{4}\right)}\right) \ (mod\ q)$$

   $m_p =$ akar kuadrat *cipherkey* terhadap *p*

   $m_q =$ akar kuadrat *cipherkey* terhadap *q*

   c. Menghitung nilai $r, s, t, \text{dan}\, u$ menggunakan *Chinese Remainder Theorem* dengan persamaan sebagai berikut:

   $$v = Y_p * p * m_q$$

   $$w = Y_p * q * m_p$$

   sehingga:

   $$r = (v + w) \ (mod\ n)$$

   $$s = (v - w) \ (mod\ n)$$

   $$t = (-v + w) \ (mod\ n)$$

   $$u = (-v - w) \ (mod\ n)$$

d. Mengubah nilai desimal $r, s, t,$ dan u ke bentuk biner dan nilai biner dibagi menjadi dua bagian sama panjang. Kemudian, membandingkan kedua bagian. Apabila dari kedua bagian menghasilkan bentuk biner yang sama, maka akan didapatkan hasil dekripsinya yang merupakan kunci simetris CBC dan *Initial Vector*.

2. Melakukan dekripsi pesan pada *ciphertext* dengan algoritma simetris CBC menggunakan kunci simetris CBC dan *Initial Vector*, sehingga diperoleh *plaintext* dengan langkah sebagai berikut:

   a. Mengelompokkan *ciphertext* C ke dalam blok sesuai dengan jumlah bit per kelompok yang sudah ditentukan sebelumnya, yaitu dua karakter huruf untuk setiap bloknya.

   b. Menggeser 4 bit *ciphertext* dari kanan.

   c. Melakukan proses dekripsi sebagai berikut:

$$P_i = Dk(C_i) \oplus C_{i-1}$$

   d. Mendapatkan *plaintext.*

BAB IV
HASIL DAN PEMBAHASAN

Pada bab ini akan membahas tentang proses enkripsi dan dekripsi pesan teks menggunakan algoritma CBC dan algoritma Rabin sebagai *Hybrid Cryptosystem*.

4.1 Proses Enkripsi *Hybrid Cryptosystem* Menggunakan Algoritma CBC Dan Algoritma *Rabin*

Proses enkripsi dari *Hybrid Cryptosystem* terdiri dari dua tahap, yakni melakukan proses enkripsi terhadap *plaintext* menggunakan algoritma CBC dan melakukan proses enkrispsi terhadap kunci dari algoritma CBC menggunakan algoritma Rabin. Adapun tahapan-tahapan yang dilakukan untuk proses enkripsi Algoritma CBC dan Algoritma *Rabin* sebagai berikut:

1. Menentukan karakter alfabet kapital yang akan digunakan sebagai *plaintext* dan menentukan nilai jumlah bit pada setiap blok. Pada penelitian ini, *plaintext* yang digunakan adalah “Matematika UINMA” yang dikelompokkan menjadi delapan blok dengan masing-masing blok memiliki dua karakter berupa biner berjumlah enam belas bit.

   Tabel 4.1 *Plaintext* Pada Proses Enkripsi *Hybrid Cryptosystem*

Plaintext	**Karakter**	**Biner**
P_1	Ma	01001101 01100001
P_2	te	01110100 01100101
P_3	ma	01101101 01100001

P_4	ti	01110100 01101001
P_5	ka	01101011 01100001
P_6	(Spasi)U	00100000 01010101
P_7	IN	01001001 01001110
P_8	MA	01001101 01000001

2. Menentukan kunci simetri CBC dan *Initial Vector* (C_0) secara acak dan masing-masing berupa dua karakter khusus.

   Tabel 4.2 Kunci Algoritma *CBC* dan *Initial Vector*

Jenis	**Karakter**	**Biner**
Kunci simetri CBC (K)	In	01001001 01101110
Initial Vector (C_0)	Or	01001111 01110000

3. Melakukan proses enkripsi algoritma CBC terhadap *plaintext* menggunakan kunci simetris CBC beserta *Initial Vector* (C_0), sehingga akan menghasilkan *cipher*text yang akan diterima oleh penerima pesan. Adapun proses enkripsinya sebagai berikut:.

   $C_i = Ek(P_i) \oplus C_{i-1}$

   $C_1 = \text{Blok } P_1 \oplus C_0$

   $= 01001101\ 01100001 \oplus 01001111\ 01110000$

   $= 00000010\ 00010001$

   $= (\text{Blok } P_1 \oplus C_0) \oplus K$

   $= 00000010\ 00010001 \oplus 01001001\ 01101110$

$= 01001011\ 01111111$

Geser empat bit ke kiri: $10110111\ 11110100$

$C_2 = \text{Blok } P_2 \oplus C_1$

$= 01110100\ 01100101 \oplus 10110111\ 11110100$

$= 11000011\ 10010001$

$= (\text{Blok } P_2 \oplus C_1) \oplus K$

$= 11000011\ 10010001 \oplus 01001001\ 01101110$

$= 10001010\ 11111111$

Geser empat bit ke kiri: $10101111\ 11111000$

$C_3 = \text{Blok } P_3 \oplus C_2$

$= 01101101\ 01100001 \oplus 10101111\ 11111000$

$= 11000010\ 10011001$

$= (\text{Blok } P_3 \oplus C_2) \oplus K$

$= 11000010\ 10011001 \oplus 01001001\ 01101110$

$= 10001011\ 11110111$

Geser empat bit ke kiri: $10111111\ 01111000$

$C_4 = \text{Blok } P_4 \oplus C_3$

$= 01110100\ 01101001 \oplus 10111111\ 01111000$

$= 11001011\ 00010001$

$= (\text{Blok } P_4 \oplus C_3) \oplus K$

$= 11001011\ 00010001 \oplus 01001001\ 01101110$

$= 10000010\ 01111111$

Geser empat bit ke kiri: $00100111\ 11111000$

$C_5 = \text{Blok } P_5 \oplus C_4$

$= 01101011\ 01100001 \oplus 00100111\ 11111000$

$= 01001100\ 10011001$

$= (\text{Blok } P_5 \oplus C_4) \oplus K$

$= 01001100\ 10011001 \oplus 01001001\ 01101110$

$= 00000101\ 11110111$

Geser empat bit ke kiri: 01011111 01110000

$C_6 = \text{Blok } P_6 \oplus C_5$

$= 00100000\ 01010101 \oplus 01011111\ 01110000$

$= 01111111\ 00100101$

$= (\text{Blok } P_6 \oplus C_5) \oplus K$

$= 01111111\ 00100101 \oplus 01001001\ 01101110$

$= 00110110\ 01001011$

Geser empat bit ke kiri: 01100100 10110011

$C_7 = \text{Blok } P_7 \oplus C_6$

$= 01001001\ 01001110 \oplus 01100100\ 10110011$

$= 00101101\ 11111101$

$= (\text{Blok } P_7 \oplus C_6) \oplus K$

$= 00101101\ 11111101 \oplus 01001001\ 01101110$

$= 01100100\ 10010011$

Geser empat bit ke kiri: 01001001 00110110

$C_8 = \text{Blok } P_8 \oplus C_7$

$= 01001101\ 01000001 \oplus 01001001\ 00110110$

$= 00000100\ 01110111$

$= (\text{Blok } P_8 \oplus C_7) \oplus K$

$= 00000100\ 01110111 \oplus 01001001\ 01101110$

$= 01001101\ 00011001$

Geser empat bit ke kiri: $11010001\ 10010100$

Dengan demikian, hasil enkripsi yang diperoleh adalah:

$C_1 = 10110111\ 11110100$

$C_2 = 10101111\ 11111000$

$C_3 = 10111111\ 01111000$

$C_4 = 00100111\ 11111000$

$C_5 = 01011111\ 01110000$

$C_6 = 01100100\ 10110011$

$C_7 = 01001001\ 00110110$

$C_8 = 11010001\ 10010100$

4. Selanjutnya, melakukan proses enkripsi terhadap kunci simetri CBC dan *Initial Vector* menggunakan algoritma *Rabin*. Kunci simetri CBC dan *Initial Vector* akan berperan sebagai *plaintext* dalam proses enkripsi algoritma *Rabin* dan hasil enkripsi ini selanjutnya akan disebut sebagai *cipherkey*.
5. Langkah pertama yang dilakukan dalam proses enkripsi algoritma *Rabin* adalah pembangkitan kunci dengan menentukan nilai *p* dan *q* yang terdiri dari bilangan prima acak sebagai kunci privat dari algoritma *Rabin*. Nilai p dan q harus memenuhi kongruensi $p \equiv q \equiv 3\ (mod\ 4)$. Pada penelitian ini, terdapat dua kasus dengan nilai p dan q yang berbeda, yaitu:
   a. Kasus 1: $p = 131$ dan $q = 151$.
   b. Kasus 2: $p = 127$ dan $q = 191$.

6. Selanjutnya, melakukan pembangkitan kunci publik (n) dengan persamaan sebagai berikut:

$$n = p * q$$

   a. Kasus 1: $n = 131 * 151 = 19781$.

   b. Kasus 2: $n = 127 * 191 = 24257$.

7. Mengubah *plaintext* ke bentuk biner berdasarkan pada tabel ASCII. Kunci simetri CBC dan *Initial Vector* merupakan *plaintext* yang akan dienkripsi menggunakan algorima *Rabin*. Berikut adalah *plaintext* yang digunakan pada enkripsi algoritma *Rabin*:

   $m_1 = I = 73_{10} = 01001001_2 = 1001001_2$

   $m_2 = n = 110_{10} = 01101110_2 = 1101110_2$

   $m_3 = O = 79_{10} = 01001111_2 = 1001111_2$

   $m_4 = r = 112_{10} = 01110000_2 = 1110000_2$

8. Menambahkan m dengan nilai biner m itu sendiri (*redundant information*).

   $m_1 = 1001001 \mid 1001001$

   $m_2 = 1101110 \mid 1101110$

   $m_3 = 1001111 \mid 1001111$

   $m_4 = 1110000 \mid 1110000$

9. Mengubah hasil penggandaan m menjadi nilai desimal.

   $m_1 = 10010011001001_2 = 9417$

   $m_2 = 11011101101110_2 = 14190$

   $m_3 = 10011111001111_2 = 10191$

   $m_4 = 11100001110000_2 = 14448$

10. Menghitung nilai *ciphertext* dengan persamaan sebagai berikut:

$$c = (m^2)\ (mod\ n)$$

a. Kasus 1 dengan $p = 131$, $q = 151$, dan $n = 19781$.

$c_1 = (m_1^2)\ (mod\ n) = 9417^2\ (mod\ 19781) = 1666$

$c_2 = (m_2^2)\ (mod\ n) = 14190^2\ (mod\ 19781) = 5301$

$c_3 = (m_3^2)\ (mod\ n) = 10191^2\ (mod\ 19781) = 6231$

$c_4 = (m_4^2)\ (mod\ n) = 14448^2\ (mod\ 19781) = 15592$

b. Kasus 2 dengan $p = 127$, $q = 191$, dan $n = 24257$.

$c_1 = (m_1^2)\ (mod\ n) = 9417^2\ (mod\ 24257) = 20554$

$c_2 = (m_2^2)\ (mod\ n) = 14190^2\ (mod\ 24257) = 23000$

$c_3 = (m_3^2)\ (mod\ n) = 10191^2\ (mod\ 24257) = 12264$

$c_4 = (m_4^2)\ (mod\ n) = 14448^2\ (mod\ 24257) = 13219$

11. Mendapatkan *cipher*text dari algoritma *Rabin*, yaitu:

a. Kasus 1: $1666, 5301, 6231,$ dan 15592.

b. Kasus 2: $20554, 23000, 12264,$ dan 13219.

4.2 Proses Dekripsi *Hybrid Cryptosystem* Menggunakan Algoritma CBC Dan Algoritma *Rabin*

1. Melakukan proses dekripsi pesan dengan algoritma *Rabin* menggunakan kunci privat terhadap *cipherkey*. Adapun langkah-langkahnya sebagai berikut:

a. Menentukan nilai Y_p dan Y_q yang merupakan FPB dari p dan q menggunakan algoritma *Extended Euclidean*.

$$Y_p * p + Y_q * q = gc\,d(p, q) \Leftrightarrow Y_p * p + Y_q * q = 1$$

(i) Kasus 1 dengan $p = 131$ dan $q = 151$. Berdasarkan algoritma pembagian, $FPB(131,151)$:

$$151 = 1.131 + 20$$

$$131 = 6.20 + 11$$

$$20 = 1.11 + 9$$

$$11 = 1.9 + 2$$

$$9 = 4.2 + 1$$

$$2 = 2.1 + 0$$

Sehingga dapat dinyatakan bahwa $FPB(131,151) = 1$. Kemudian, untuk menyatakan 1 sebagai kombinasi linear dari 131 dan 151, maka diperlukan algoritma *Extended Euclidean* (substitusi balik dari algoritma *Euclid*) sebagai berikut:

$1 = 9 - 4.2$

$1 = 9 - 4(11 - 1.9)$

$1 = 9 - 4.11 + 4.9$

$1 = 5.9 - 4.11$

$1 = 5(20 - 1.11) - 4.11$

$1 = 5.20 - 9.11$

$1 = 5.20 - 9(131 - 6.20)$

$1 = 59.20 - 9.131$

$1 = 59(151 - 1.131) - 9.131$

$1 = -68.131 + 59.151$

Diperoleh $Y_p = -68$ dan $Y_q = 59$.

(ii) Kasus 2 dengan $p = 127$ dan $q = 191$. Berdasarkan algoritma pembagian, $FPB(127, 191)$:.

$$191 = 1.127 + 64$$

$$127 = 1.64 + 63$$

$$64 = 1.63 + 1$$

$$63 = 63.1 + 0$$

Sehingga dapat dinyatakan bahwa $FPB(127, 191) = 1$. Kemudian, untuk menyatakan 1 sebagai kombinasi linear dari 127 dan 191, maka diperlukan algoritma *Extended Euclidean* (substitusi balik dari algoritma *Euclid*) sebagai berikut:

$1 = 64 - 1.63$

$1 = 64 - 1(127 - 1.64)$

$1 = 2.64 - 1.127$

$1 = 2(191 - 1.127) - 1.127$

$1 = -3.127 + 2.191$

Diperoleh $Y_p = -3$ dan $Y_q = 2$.

b. Menghitung nilai akar kuadrat *cipherkey* terhadap p dan q dengan rumus berikut:

$$m_p = \left(c^{\left(\frac{p+1}{4}\right)}\right) \ (mod\ p)$$

$$m_q = \left(c^{\left(\frac{q+1}{4}\right)}\right) \ (mod\ q)$$

sehingga:

(i) Kasus 1 dengan $p = 131$ dan $q = 151$.

$$m_{p1} = \left(c_1^{\left(\frac{p+1}{4}\right)}\right) (mod\ p) = 1666^{\frac{131+1}{4}} (mod\ 131) = 15$$

$$m_{q1} = \left(c_1^{\left(\frac{q+1}{4}\right)}\right) (mod\ q) = 1666^{\frac{151+1}{4}} (mod\ 151) = 55$$

$$m_{p2} = \left(c_2^{\left(\frac{p+1}{4}\right)}\right) (mod\ p) = 5301^{\frac{131+1}{4}} (mod\ 131) = 89$$

$$m_{q2} = \left(c_2^{\left(\frac{p+1}{4}\right)}\right) (mod\ q) = 5301^{\frac{151+1}{4}} (mod\ 151) = 4$$

$$m_{p3} = \left(c_3^{\left(\frac{p+1}{4}\right)}\right) (mod\ p) = 6231^{\frac{131+1}{4}} (mod\ 131) = 27$$

$$m_{q3} = \left(c_3^{\left(\frac{p+1}{4}\right)}\right) (mod\ q) = 6231^{\frac{151+1}{4}} (mod\ 151) = 74$$

$$m_{p4} = \left(c_4^{\left(\frac{p+1}{4}\right)}\right) (mod\ p) = 15592^{\frac{131+1}{4}} (mod\ 131) = 38$$

$$m_{q4} = \left(c_4^{\left(\frac{p+1}{4}\right)}\right) (mod\ q) = 15592^{\frac{151+1}{4}} (mod\ 151) = 103$$

(ii) Kasus 2 dengan $p = 127$ dan $q = 191$.

$$m_{p1} = \left(c_1^{\left(\frac{p+1}{4}\right)}\right) (mod\ p) = 20554^{\frac{127+1}{4}} (mod\ 127) = 19$$

$$m_{q1} = \left(c_1^{\left(\frac{q+1}{4}\right)}\right) (mod\ q) = 20554^{\frac{191+1}{4}} (mod\ 191) = 133$$

$$m_{p2} = \left(c_2^{\left(\frac{p+1}{4}\right)}\right) (mod\ p) = 23000^{\frac{127+1}{4}} (mod\ 127) = 34$$

$$m_{q2} = \left(c_2^{\left(\frac{p+1}{4}\right)}\right) (mod\ q) = 23000^{\frac{191+1}{4}} (mod\ 191) = 135$$

$$m_{p3} = \left(c_3^{\left(\frac{p+1}{4}\right)}\right) (mod\ p) = 12264^{\frac{127+1}{4}} (mod\ 127) = 31$$

$$m_{q3} = \left(c_3^{\left(\frac{p+1}{4}\right)}\right) (mod\ q) = 12264^{\frac{191+1}{4}} (mod\ 191) = 68$$

$$m_{p4} = \left(c_4^{\left(\frac{p+1}{4}\right)}\right) (mod\ p) = 13219^{\frac{127+1}{4}} (mod\ 127) = 30$$

$$m_{q4} = \left(c_4^{\left(\frac{p+1}{4}\right)}\right) (mod\ q) = 13219^{\frac{191+1}{4}} (mod\ 191) = 68$$

c. Menghitung nilai $r, s, t,$ dan u menggunakan *Chinese Remainder Theorem* dengan persamaan sebagai berikut:

$$v = Y_p * p * m_q$$

$$w = Y_p * q * m_p$$

sehingga:

$$r = (v + w)\ (mod\ n)$$

$$s = (v - w)\ (mod\ n)$$

$$t = (-v + w)\ (mod\ n)$$

$$u = (-v - w)\ (mod\ n)$$

maka kita memperoleh:

(i) Kasus 1 dengan $p = 131$ dan $q = 151$.

$v_1 = Y_p * p * m_{q1} = -68.131.55 = -489940$

$w_1 = Y_q * q * m_{p1} = 59.151.15 = 133635$

$v_2 = Y_p * p * m_{q2} = -68.131.4 = -35632$

$w_2 = Y_q * q * m_{p2} = 59.151.89 = 792901$

$v_3 = Y_p * p * m_{q3} = -68.131.74 = -659192$

$w_3 = Y_q * q * m_{p3} = 59.151.27 = 240543$

$v_4 = Y_p * p * m_{q4} = -68.131.103 = -917524$

$w_4 = Y_q * q * m_{p4} = 59.151.38 = 338542$

sehingga:

$r_1 = (v_1 + w_1)\ (mod\ n)$

$= (-489940 + 133635)(mod\ 19781)$

$= 19534$

$s_1 = (v_1 - w_1)\ (mod\ n)$

$= (-489940 - 133635)(mod\ 19781)$

$= 9417$

$t_1 = (-v_1 + w_1)\ (mod\ n)$

$= (-(-489940) + 133635)(mod\ 19781)$

$= 10364$

$u_1 = (-v_1 - w_1)\ (mod\ n)$

$= (-(-489940) - 133635)\ (mod\ 19781)$

$= 247$

$r_2 = (v_2 + w_2)\ (mod\ n)$

$= (-35632 + 792901)(mod\ 19781)$

$= 5591$

$s_2 = (v_2 - w_2)\ (mod\ n)$

$= (-35632 - 792901)(mod\ 19781)$

$= 2269$

$t_2 = (-v_2 + w_2)\ (mod\ n)$

$= (-(-35632) + 792901)(mod\ 19781)$

$= 17512$

$u_2 = (-v_2 - w_2)\ (mod\ n)$

$= (-(-35632) - 792901)(mod\ 19781)$

$= 14190$

$r_3 = (v_3 + w_3)\ (mod\ n)$

$= (-659192 + 240543)(mod\ 19781)$

$= 16533$

$s_3 = (v_3 - w_3)\ (mod\ n)$

$= (-659192 - 240543)(mod\ 19781)$

$= 10191$

$t_3 = (-v_3 + w_3)\ (mod\ n)$

$= (-(-659192) + 240543)(mod\ 19781)$

$= 9590$

$u_3 = (-v_3 - w_3)\ (mod\ n)$

$= (-(-659192) - 240543)(mod\ 19781)$

$= 3248$

$r_4 = (v_4 + w_4)\ (mod\ n)$

$= (-917524 + 338542)(mod\ 19781)$

$= 14448$

$s_4 = (v_4 - w_4)\ (mod\ n)$

$= (-917524 - 338542)(mod\ 19781)$

$= 9918$

$t_4 = (-v_4 + w_4)\ (mod\ n)$

$= (-(-917524) + 338542)(mod\ 19781)$

$= 9863$

$u_4 = (-v_4 - w_4)\ (mod\ n)$

$= (-(-917524) - 338542)(mod\ 19781)$

$= 5333$

(ii) Kasus 2 dengan $p = 127$ dan $q = 191$

$v_1 = Y_p * p * m_{q1} = -3.127.133 = -50673$

$w_1 = Y_q * q * m_{p1} = 2.191.19 = 7258$

$v_2 = Y_p * p * m_{q2} = -3.127.135 = -51435$

$w_2 = Y_q * q * m_{p2} = 2.191.34 = 12988$

$v_3 = Y_p * p * m_{q3} = -3.127.68 = -25908$

$w_3 = Y_q * q * m_{p3} = 2.191.31 = 11842$

$v_4 = Y_p * p * m_{q4} = -3.127.68 = -25908$

$w_4 = Y_q * q * m_{p4} = 2.191.30 = 11460$

sehingga:

$r_1 = (v_1 + w_1)\ (mod\ n)$

$= (-50673 + 7258)(mod\ 24257)$

$= 5099$

$s_1 = (v_1 - w_1)\ (mod\ n)$

$= (-50673 - 7258)(mod\ 24257)$

$= 14840$

$t_1 = (-v_1 + w_1)\ (mod\ n)$

$= (-(-50673) + 7258)(mod\ 24257)$

$= 9417$

$u_1 = (-v_1 - w_1)\ (mod\ n)$

$= (-(-50673) - 7258)(mod\ 24257)$

$= 19158$

$r_2 = (v_2 + w_2)\ (mod\ n)$

$= (-51435 + 12988)(mod\ 24257)$

$= 10067$

$s_2 = (v_2 - w_2)\ (mod\ n)$

$= (-51435 - 12988)(mod\ 24257)$

$= 8348$

$t_2 = (-v_2 + w_2)\ (mod\ n)$

$= (-(-51435) + 12988)(mod\ 24257)$

$= 15909$

$u_2 = (-v_2 - w_2)\ (mod\ n)$

$= (-(-51435) - 12988)(mod\ 24257)$

$= 14190$

$r_3 = (v_3 + w_3)\ (mod\ n)$

$= (-25908 + 11842)(mod\ 24257)$

$= 10191$

$s_3 = (v_3 - w_3)\ (mod\ n)$

$= (-25908 - 11842)(mod\ 24257)$

$= 10764$

$t_3 = (-v_3 + w_3)\ (mod\ n)$

$= (-(-25908) + 11842)(mod\ 24257)$

$= 13493$

$u_3 = (-v_3 - w_3)\ (mod\ n)$

$= (-(-25908) - 11842)(mod\ 24257)$

$= 14066$

$r_4 = (v_4 + w_4)\ (mod\ n)$

$= (-25908 + 11460)(mod\ 24257)$

$= 9809$

$s_4 = (v_4 - w_4)\ (mod\ n)$

$= (-25908 - 11460)(mod\ 24257)$

$= 11146$

$t_4 = (-v_4 + w_4)\ (mod\ n)$

$= (-(-25908) + 11460)(mod\ 24257)$

$= 13111$

$u_4 = (-v_4 - w_4)\ (mod\ n)$

$= (-(-25908) - 11460)(mod\ 24257)$

$= 14448$

d. Selanjutnya, nilai desimal $r, s, t,$ dan u diubah ke bentuk biner dan nilai biner dibagi menjadi dua bagian sama panjang.

(i) Kasus 1 dengan $p = 131$ dan $q = 151$

$r_1 = 19534 = 1001100 \mid 01001110$

$s_1 = 9417 = 1001001 \mid 1001001$

$t_1 = 10364 = 101000 \mid 01111100$

$u_1 = 247 = 1111 \mid 0111$

$r_2 = 5591 = 101011 \mid 1010111$

$s_2 = 2269 = 100011 \mid 011101$

$t_2 = 17512 = 1000100 \mid 01101000$

$u_2 = 14190 = 1101110 \mid 1101110$

$r_3 = 16533 = 1000000 \mid 10010101$

$s_3 = 10191 = 1001111 \mid 1001111$

$t_3 = 9590 = 1001010 \mid 1110110$

$u_3 = 3248 = 1100010 \mid 110000$

$r_4 = 14448 = 1110000 \mid 1110000$

$s_4 = 9918 = 1001101 \mid 0111110$

$t_4 = 9863 = 1001101 \mid 0000111$

$u_4 = 5333 = 101001 \mid 1010101$

Kemudian, bandingkan kedua bagian. Apabila dari kedua bagian menghasilkan bentuk biner yang sama, maka akan didapatkan hasil dekripsinya yang merupakan kunci simetris CBC dan *Initial Vector*. Hasil dari proses dekripsi algoritma *Rabin* di atas adalah:

$s_1 = 1001001 = 73_{10} = I$

$u_2 = 1101110 = 110_{10} = n$

$s_3 = 1001111 = 79_{10} = O$

$r_4 = 1110000 = 112_{10} = r$

(ii) Kasus 2 dengan $p = 127$ dan $q = 191$

$r_1 = 5099 = 1001111 \mid 101011$

$s_1 = 14840 = 1110011 \mid 1111000$

$t_1 = 9417 = 1001001 \mid 1001001$

$u_1 = 19158 = 1001010 \mid 11010110$

$r_2 = 10067 = 1001110 \mid 1010011$

$s_2 = 8348 = 1000001 \mid 0011100$

$t_2 = 15909 = 1111100 \mid 0100101$

$u_2 = 14190 = 1101110 \mid 1101110$

$r_3 = 10191 = 1001111 \mid 1001111$

$s_3 = 10764 = 1010100 \mid 0001100$

$t_3 = 13493 = 1101001 \mid 0110101$

$u_3 = 14066 = 1101101 \mid 1110010$

$r_4 = 9809 = 1001101 \mid 010001$

$s_4 = 11146 = 1010111 \mid 0001010$

$t_4 = 13111 = 1100110 \mid 0110111$

$u_4 = 14448 = 1110000 \mid 1110000$

Kemudian, bandingkan kedua bagian. Apabila dari kedua bagian menghasilkan bentuk biner yang sama, maka akan didapatkan hasil dekripsinya yang merupakan kunci simetris CBC dan *Initial Vector*. Hasil dari proses dekripsi algoritma *Rabin* di atas adalah:

$t_1 = 1001001 = 73_{10} = I$

$u_2 = 1101110 = 110_{10} = n$

$r_3 = 1001111 = 79_{10} = O$

$u_4 = 1110000 = 112_{10} = r$

Kedua kasus memperoleh hasil dekripsi yang sama. Dengan demikian, kita memperoleh “In” sebagai kunci simetri CBC dan “Or” sebagai *intial vector*. Hasil dekripsi tersebut akan digunakan untuk mendekripsikan *ciphertext* menggunakan algoritma CBC.

2. Melakukan dekripsi pesan terhadap *ciphertext* dengan algoritma simetris CBC menggunakan kunci simetris CBC, sehingga akan mendapatkan *plaintext* dengan langkah sebagai berikut:

   a. Menggeser 4 bit *ciphertext* ke kanan.

   $C_1 = 10110111\ 11110100 \rightarrow C_1' = 01001011\ 01111111$

   $C_2 = 10101111\ 11111000 \rightarrow C_2' = 10001010\ 11111111$

   $C_3 = 10111111\ 01111000 \rightarrow C_3' = 10001011\ 11110111$

   $C_4 = 00100111\ 11111000 \rightarrow C_4' = 10000010\ 01111111$

   $C_5 = 01011111\ 01110000 \rightarrow C_5' = 00000101\ 11110111$

   $C_6 = 01100100\ 10110011 \rightarrow C_6' = 00110110\ 01001011$

   $C_7 = 01001001\ 00110110 \rightarrow C_7' = 01100100\ 10010011$

   $C_8 = 11010001\ 10010100 \rightarrow C_8' = 01001101\ 00011001$

   b. Melakukan proses dekripsi sebagai berikut:

   $$P_i = Dk(C_i) \oplus C_{i-1}$$

   $P_1 = \text{Blok } C_1' \oplus C_0$

   $= 01001011\ 01111111 \oplus 01001111\ 01110000$

   $= 00000100\ 00001111$

   $= (\text{Blok } C_1' \oplus C_0) \oplus K$

   $= 00000100\ 00001111 \oplus 01001001\ 01101110$

   $= 01001101\ 01100001$

   $= Ma$

   $P_2 = \text{Blok } C_2' \oplus C_1$

   $= 10001010\ 11111111 \oplus 10110111\ 11110100$

   $= 00111101\ 00001011$

$= (\text{Blok } C_2' \oplus C_1) \oplus K$

$= 00111101\ 00001011 \oplus 01001001\ 01101110$

$= 01110100\ 01100101$

$= te$

$P_3 = \text{Blok } C_3' \oplus C_2$

$= 10001011\ 11110111 \oplus 10101111\ 11111000$

$= 00100100\ 00001111$

$= (\text{Blok } C_3' \oplus C_2) \oplus K$

$= 00100100\ 00001111 \oplus 01001001\ 01101110$

$= 01101101\ 01100001$

$= ma$

$P_4 = \text{Blok } C_4' \oplus C_3$

$= 10000010\ 01111111 \oplus 10111111\ 01111000$

$= 00111101\ 00000111$

$= (\text{Blok } C_4' \oplus C_3) \oplus K$

$= 00111101\ 00000111 \oplus 01001001\ 01101110$

$= 01110100\ 01101001$

$= ti$

$P_5 = \text{Blok } C_5' \oplus C_4$

$= 00000101\ 11110111 \oplus 00100111\ 11111000$

$= 00100010\ 00001111$

$= (\text{Blok } C_5' \oplus C_4) \oplus K$

$= 00100010\ 00001111 \oplus 01001001\ 01101110$

$= 01101011\ 01100001$

$= ka$

$P_6 = \text{Blok } C_6' \oplus C_5$

$= 00110110\ 01001011 \oplus 01011111\ 01110000$

$= 01101001\ 00111011$

$= (\text{Blok } C_6' \oplus C_5) \oplus K$

$= 01101001\ 00111011 \oplus 01001001\ 01101110$

$= 00100000\ 01010101$

$= (spasi)U$

$P_7 = \text{Blok } C_7' \oplus C_6$

$= 01100100\ 10010011 \oplus 01100100\ 10110011$

$= 00000000\ 00100000$

$= (\text{Blok } C_7' \oplus C_6) \oplus K$

$= 00000000\ 00100000 \oplus 01001001\ 01101110$

$= 01001001\ 01001110$

$= IN$

$P_8 = \text{Blok } C_8' \oplus C_7$

$= 01001101\ 00011001 \oplus 01001001\ 00110110$

$= 00000100\ 00101111$

$= (\text{Blok } C_8' \oplus C_7) \oplus K$

$= 00000100\ 00101111 \oplus 01001001\ 01101110$

$= 01001101\ 01000001$

$= MA$

c. Mendapatkan *plaintext*, yaitu “Matematika UINMA”.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan diatas, maka didapatkan kesimpulan sebagai berikut:

1. Proses enkripsi pesan teks menggunakan algoritma CBC dan algoritma *Rabin* sebagai *hybrid cryptosystem* terbagi menjadi dua proses, yaitu enkripsi terhadap *plaintext* menggunakan algoritma CBC dan enkripsi terhadap kunci simetri CBC menggunakan algoritma *Rabin*. Pada proses enkripsi algoritma CBC, *plaintext* yang telah ditentukan berdasarkan karakter tabel ASCII akan dikelompokkan menjadi blok-blok yang setiap blok-nya berisi dua karakter. Kemudian, menentukan *Initial Vector* (C_0) dan kunci simetri CBC. Persamaan yang digunakan untuk mengenkripsi *plaintext* menggunakan algoritma CBC adalah $C_i = Ek(P_i \oplus C_{i-1})$. Selanjutnya, melakukan proses enkripsi terhadap kunci simetri CBC dan *Initial Vector* menggunakan algoritma Rabin. Pertama, menentukan kunci privat p dan q dengan syarat $p \equiv q \equiv 3\ (mod\ 4)$. Kemudian, pembangkitan kunci publik n dengan persamaan $n = p.q$. Setelah itu, melakukan proses enkripsi terhadap kunci simetri CBC dan *Initial Vector* yang disimbolkan dengan m. Hasil enkripsi ini akan menghasilkan *cipherkey* dengan persamaan $c = m^2\ (mod\ n)$. Hasil enkripsi keduanya akan diterima oleh penerima pesan. Dengan demikian, pesan teks dan kunci simetri CBC dan *intial vector* yang akan disampaikan kepada penerima pesan terjamin aman.
2. Proses dekripsi pesan teks menggunakan algoritma CBC dan algoritma *Rabin* sebagai *hybrid cryptosystem* terbagi menjadi dua proses, yaitu dekripsi terhadap *cipherkey* menggunakan algoritma *Rabin* dan dekripsi terhadap *ciphertext* menggunakan algoritma CBC. Hal pertama yang dilakukan pada proses dekripsi *cipherkey* adalah mencari Y_p dan Y_q yang merupakan kombinasi linier dari kunci privat p dan q sehingga $GCD(p,q) = Y_p.p + Y_q.q$ menggunakan algoritma *Extended Euclidean*. Kemudian, mencari nilai akar kuadrat dari *cipherkey* terhadap p dan q menggunakan persamaan:

$$m_p = \left(c^{\left(\frac{p+1}{4}\right)}\right) \ (mod\ p)$$

$$m_q = \left(c^{\left(\frac{q+1}{4}\right)}\right) \ (mod\ q)$$

Selanjutnya, menghitung nilai $r, s, t,$ dan u menggunakan *Chinese Remainder Theorem* dengan persamaan:

$$v = Y_p * p * m_q$$

$$w = Y_p * q * m_p$$

sehingga:

$$r = (v + w)\ (mod\ n)$$

$$s = (v - w)\ (mod\ n)$$

$$t = (-v + w)\ (mod\ n)$$

$$u = (-v - w)\ (mod\ n)$$

Nilai desimal $r, s, t,$ dan u selanjutnya diubah ke bentuk biner dan nilai biner dibagi menjadi dua bagian sama panjang. Apabila dari kedua bagian menghasilkan bentuk biner yang sama, maka akan didapatkan kunci simetri CBC dan *Initial Vector*. Kunci tersebut akan digunakan untuk mendekripsikan *ciphertext*. Persamaan yang digunakan untuk mendekripsikan *ciphertext* menggunakan algoritma CBC adalah $P_i = Dk(C_i \oplus C_{i-1})$. Dengan demikian, penerima pesan dapat mengetahui isi pesan asli atau *plaintext*.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, maka saran untuk penelitian selanjutnya, yaitu:

1. Pada penelitian ini, proses enkripsi dan dekripsi hanya dilakukan pada pesan teks, yang diharapkan untuk penelitian selanjutnya dapat melakukan proses enkripsi dan dekripsi dengan beberapa jenis *file* lainnya.
2. Pada penelitian ini, proses enkripsi dan dekripsi hanya dilakukan secara manual, yang diharapkan untuk penelitian selanjutnya dapat menerapkannya menggunakan program *python* atau lainnya.
3. Diharapkan adanya modifikasi algoritma yang lebih variatif dan mudah diimplementasikan, sehingga waktu yang diperlukan untuk proses enkripsi

dan dekripsi pesan lebih singkat.

DAFTAR PUSTAKA

Ad-Dimasyqi, A. A. F. I. I. K. (2005). *Tafsir Ibnu Kasir Juz 9*. Bandung: Sinar Baru Algensindo.

Al-Qur'an dan Terjemahannya. (2019). Kementrian Agama Republik Indonesia. Jakarta: Lajnah Pentashihan Mushaf Al-Qur'an (LPMQ).

Ariyus, D. (2008). *Pengantar Ilmu Kriptogradi Teori, Analisis dan Implementasi* (F. S. Suyantoro (ed.); 1st ed.). CV Andi Offset.

Budiman, M. A., D. Rachmawati, and R. Utami. 2019. "The Cryptanalysis of the Rabin Public Key Algorithm Using the Fermat Factorization Method." *Journal of Physics: Conference Series* 1235(1).

Fatimah. (2019). Nilai-Nilai Amanah Dalam Al-Qur'an (Suatu Pendekatan Dengan Pendekatan Tafsir Maudhu'iy). *Al-Riwayah: Jurnal Kependidikan* 11(April): 123–46.

Haqqi, S. L. (2018). Penafsiran Ibn Katsīr Tentang Ayat-ayat Amanah dalam Tafsir Al-qur`an Al-'aẓī m (Kajian Tematis Ayat-Ayat Amanah). *Skripsi Universitas Islam Negeri Syarif Hidayatullah Jakarta*: 83.

Irawan, W. H., Hijriyah, N. ., & Habibi, A. R. (2014). *Pengantar Teori Bilangan.* UIN Malang Press.

Kurniawan, A. (2008). *Konsep dan Implementasi Cryptography dengan .Net.* Jakarta:Dian Rakyat.

Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC press.

Munir, R. (2006). *Kriptografi*. Bandung: Informatika Bandung.

Ollinka, Y. U. (2021). *Algoritma Gronsfeld Cipher dan Algoritma Rabin sebagai Hybrid Cryptosystem dalam Pengamanan Dokumen PDF*. Skripsi. Medan: Universitas Sumatera Utara

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.

Rosen, K. H. (2011). *Elementary Number Theory & Its Applications (Sixth Edition).* Massachusetts : Addison-Wesley.

Rosmala, D. et all. (2012). Implementasi Mode Operasi Cipher Block Chaining (CBC). No.2 (3): 55–66.

Suhandinata, S. et al. 2019. Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma RSA. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)* 6(1): 1–10.

Wijayanto, S. N. (2021). *Implementasi Algoritma Rail Fence dan Cipher Block Chaining pada Pengamanan Pesan Text.* Skripsi. Malang: Universitas Islam Negeri Maulana Malik Ibrahim Malang

LAMPIRAN

Lampiran 1 Tabel ASCII

Kode ASCII (desimal)	**Kode ASCII (Biner)**	**Karakter**
00	00000000	NULL
01	00000001	SOH
02	00000010	STX
03	00000011	ETX
04	00000100	EOT
05	00000101	ENQ
06	00000110	ACK
07	00000111	BEL
08	00001000	BS
09	00001001	HT
10	00001010	LF
11	00001011	VT
12	00001100	FF
13	00001101	CR
14	00001110	SO
15	00001111	SI
16	00010000	DLE
17	00010001	DC1
18	00010010	DC2
19	00010011	DC3
20	00010100	DC4
21	00010101	NAK

22	00010110	SYN
23	00010111	ETB
24	00011000	CAN
25	00011001	EM
26	00011010	SUB
27	00011011	ESC
28	00011100	FS
29	00011101	GS
30	00011110	RS
31	00011111	US
32	00100000	space
33	00100001	!
34	00100010	"
35	00100011	#
36	00100100	$
37	00100101	%
38	00100110	&
39	00100111	'
40	00101000	(
41	00101001	)
42	00101010	*
43	00101011	+
44	00101100	,
45	00101101	-
46	00101110	.
47	00101111	/
48	00110000	0
49	00110001	1
50	00110010	2
51	00110011	3
52	00110100	4

53	00110101	5
54	00110110	6
55	00110111	7
56	00111000	8
57	00111001	9
58	00111010	:
59	00111011	;
60	00111100	<
61	00111101	=
62	00111110	>
63	00111111	?
64	01000000	@
65	01000001	A
66	01000010	B
67	01000011	C
68	01000100	D
69	01000101	E
70	01000110	F
71	01000111	G
72	01001000	H
73	01001001	I
74	01001010	J
75	01001011	K
76	01001100	L
77	01001101	M
78	01001110	N
79	01001111	O
80	01010000	P
81	01010001	Q
82	01010010	R
83	01010011	S

84	01010100	T
85	01010101	U
86	01010110	V
87	01010111	W
88	01011000	X
89	01011001	Y
90	01011010	Z
91	01011011	[
92	01011100	\
93	01011101	]
94	01011110	^
95	01011111	_
96	01100000	`
97	01100001	a
98	01100010	b
99	01100011	c
100	01100100	d
101	01100101	e
102	01100110	f
103	01100111	g
104	01101000	h
105	01101001	i
106	01101010	j
107	01101011	k
108	01101100	l
109	01101101	m
110	01101110	n
111	01101111	o
112	01110000	p
113	01110001	q
114	01110010	r

115	01110011	s
116	01110100	t
117	01110101	u
118	01110110	v
119	01110111	w
120	01111000	x
121	01111001	y
122	01111010	z
123	01111011	{
124	01111100	|
125	01111101	}
126	01111110	~
127	01111111	DEL
128	10000000	Ç
129	10000001	ü
130	10000010	é
131	10000011	â
132	10000100	ä
133	10000101	à
134	10000110	å
135	10000111	ç
136	10001000	ê
137	10001001	ë
138	10001010	è
139	10001011	ï
140	10001100	î
141	10001101	ì
142	10001110	Ä
143	10001111	Å
144	10010000	É
145	10010001	æ

146	10010010	Æ
147	10010011	ô
148	10010100	ö
149	10010101	ò
150	10010110	û
151	10010111	ù
152	10011000	ÿ
153	10011001	Ö
154	10011010	Ü
155	10011011	ø
156	10011100	£
157	10011101	Ø
158	10011110	×
159	10011111	*ƒ*
160	10100000	á
161	10100001	í
162	10100010	ó
163	10100011	ú
164	10100100	ñ
165	10100101	Ñ
166	10100110	ª
167	10100111	º
168	10101000	¿
169	10101001	®
170	10101010	¬
171	10101011	½
172	10101100	¼
173	10101101	¡
174	10101110	«
175	10101111	»
176	10110000	▒

177	10110001	▒
178	10110010	▓
179	10110011	│
180	10110100	┤
181	10110101	Á
182	10110110	Â
183	10110111	À
184	10111000	©
185	10111001	╣
186	10111010	║
187	10111011	╗
188	10111100	╝
189	10111101	¢
190	10111110	¥
191	10111111	┐
192	11000000	└
193	11000001	┴
194	11000010	┬
195	11000011	├
196	11000100	─
197	11000101	┼
198	11000110	ã
199	11000111	Ã
200	11001000	╚
201	11001001	╔
202	11001010	╩
203	11001011	╦
204	11001100	╠
205	11001101	═
206	11001110	╬
207	11001111	¤

208	11010000	ð
209	11010001	Ð
210	11010010	Ê
211	11010011	Ë
212	11010100	È
213	11010101	ı
214	11010110	Í
215	11010111	Î
216	11011000	Ï
217	11011001	┘
218	11011010	┌
219	11011011	█
220	11011100	▄
221	11011101	¦
222	11011110	Ì
223	11011111	▀
224	11100000	Ó
225	11100001	ß
226	11100010	Ô
227	11100011	Ò
228	11100100	õ
229	11100101	Õ
230	11100110	µ
231	11100111	þ
232	11101000	Þ
233	11101001	Ú
234	11101010	Û
235	11101011	Ù
236	11101100	ý
237	11101101	Ý
238	11101110	¯

239	11101111	´
240	11110000	≡
241	11110001	±
242	11110010	‗
243	11110011	¾
244	11110100	¶
245	11110101	§
246	11110110	÷
247	11110111	¸
248	11111000	°
249	11111001	¨
250	11111010	·
251	11111011	¹
252	11111100	³
253	11111101	²
254	11111110	■
255	11111111	nbsp

RIWAYAT HIDUP

Irbah Nafiah, dilahirkan di Kabupaten Batang pada tanggal 28 Juni 2000. Memiliki nama panggilan Irbah. Bertempat tinggal di Jalan Joyosuko Timur Gang 1 No. 8B, Merjosari, Kecamatan Lowokwaru, Kota Malang. Merupakan putri ketiga dari pasangan Bapak Suparman dan Ibu Kasmonah serta memiliki satu Kakak perempuan yang bernama Lailatul Fitriani dan Kakak laki-laki yang bernama Mukhammad Ghufron Novianto.

Jenjang pendidikannya dimulai sejak bersekolah di TK Masyitoh Batang yang lulus pada tahun 2006, kemudian melanjutkan pendidikan di SDN Kauman 02 Batang yang lulus pada tahun 2012. Pendidikan selanjutnya ditempuh di SMPN 3 Batang yang lulus pada tahun 2015. Kemudian, melanjutkan Pendidikan di SMA Trensains Tebuireng 2 Jombang yang lulus pada tahun 2018. Pada jenjang perguruan tinggi ia melanjutkan pendidikannya dengan berkuliah di UIN Maulana Malik Ibrahim Malang dengan mengambil program studi Matematika di Fakultas Sains dan Teknologi. Selama menjadi mahasiswa, penulis berperan aktif dalam kepengurusan organisasi daerah Persatuan Mahasiswa Keresidenan Pekalongan se-Malang Raya periode 2019 dan kepengurusan DEMA Fakultas Sains dan Teknologi periode 2021.

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 : Irbah Nafiah
NIM : 18610052
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Algoritma *Cipher Block Chaining* dan Algoritma *Rabin* sebagai *Hybrid Cryptosystem* pada Pengamanan Pesan Teks
Pembimbing I : Prof. Dr. H. Turmudi, M.Si., Ph.D
Pembimbing II : Mohammad Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1.	14 Juni 2022	Konsultasi Bab 1 dan 2	1.
2.	21 Juni 2022	Revisi Bab 1 dan 2	2.
3.	22 Juni 2022	Konsultasi Kajian Agama	3.
4.	23 September 2022	Konsultasi Bab 3	4.
5.	04 Oktober 2022	Revisi Bab 3	5.
6.	14 Oktober 2022	ACC Bab 1,2,3	6.
7.	24 November 2022	Konsultasi Bab 4 dan 5	7.
8.	06 Desember 2022	Revisi Bab 4 dan 5	8.
9.	13 Desember 2022	Konsultasi Kajian Agama	9.
10.	31 Maret 2023	ACC BAB 4 dan 5	10.
11.	08 Mei 2023	ACC Keseluruhan	11.

Malang, 8 Mei 2023
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP.197411292000122005