PENGAMANAN PESAN TEKS MENGGUNAKAN KRIPTOGRAFI HIBRIDA *CIPHER BLOCK CHAINING* (*CBC*) DAN *MERKLE-HELLMAN KNAPSACK*

SKRIPSI

OLEH
CHOFIFAH ALFIN NOVIANTI
NIM. 18610057

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

PENGAMANAN PESAN TEKS MENGGUNAKAN KRIPTOGRAFI HIBRIDA *CIPHER BLOCK CHAINING* (*CBC*) DAN *MERKLE-HELLMAN KNAPSACK*

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
CHOFIFAH ALFIN NOVIANTI
NIM. 18610057

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

PENGAMANAN PESAN TEKS MENGGUNAKAN KRIPTOGRAFI HIBRIDA *CIPHER BLOCK CHAINING* (*CBC*) DAN *MERKLE-HELLMAN KNAPSACK*

SKRIPSI

Oleh
Chofifah Alfin Novianti
NIM. 18610057

Telah Disetujui Untuk Diuji

Malang, 16 Juni 2023

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si	Mohammad Nafie Jauhari, M.Si
NIDT. 19900311 20160801 1 057	NIDT. 19870218 20160801 1 056

Mengetahui,
Ketua Program Studi Matematika

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

PENGAMANAN PESAN TEKS MENGGUNAKAN KRIPTOGRAFI HIBRIDA *CIPHER BLOCK CHAINING* (*CBC*) DAN *MERKLE-HELLMAN KNAPSACK*

SKRIPSI

Oleh
Chofifah Alfin Novianti
NIM. 18610057

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 26 Juni 2023

Ketua Penguji	:	Juhari, M.Si	.....
Anggota Penguji 1	:	Hisyam Fahmi, M.Kom	.....
Anggota Penguji 2	:	Muhammad Khudzaifah, M.Si	.....
Anggota Penguji 3	:	Muhammad Nafie Jauhari, MSi	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 00 5

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	: Chofifah Alfin Novianti
NIM	: 18610057
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Pengamanan Pesan Teks Menggunakan Kriptografi Hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack*

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran 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,

Yang membuat pernyataan

Chofifah Alfin Novianti

NIM. 18610057

MOTO DAN PERSEMBAHAN

"and He found you lost and guided you"

"dan Dia mendapatimu sebagai seorang yang bingung, lalu Dia memberikan petunjuk" (Q.S. Ad-Dhuha:7)

Skripsi ini penulis persembahkan untuk:
Kedua orang tua penulis bapak Imam Kambali dan ibu Jamiah Rehani yang selalu mendoakan dan mendukung seiring proses mengerjakan skripsi ini. Kakak penulis Rosy Pramediat Pangestu dan adik penulis M. Tsalis Al Ayyubi yang senantiasa memberikan motivasi dan semangat.

KATA PENGANTAR

Assalamua'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt atas rahmat, taufik, serta hidayah-Nya sehingga penulis mampu menyelesaikan penyusunan skripsi dengan judul "Pengamanan Pesan Teks Menggunakan Kriptografi Hibrida *Cipher Block Chaining* (CBC) Dan *Merkle-Hellman Knapsack*" sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim.

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak. Untuk itu ucapan terima kasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya penulis sampaikan terutama 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.
3. Dr. Elly Susanti, M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing I yang telah banyak memberikan arahan, nasehat, dan motivasi kepada penulis.
5. Mohammad Nafie Jauhari, M.Si, selaku dosen pembimbing II yang telah banyak memberikan arahan dan nasehat kepada penulis.

6. Juhari, M.Si, selaku dosen ketua penguji dalam ujian skripsi dan telah memberikan bimbingan dan pengerahan kepada penulis.
7. Hisyam Fahmi, M.Kom, selaku dosen anggota penguji 1 dalam ujian skripsi dan telah memberikan bimbingan dan pengerahan kepada penulis.
8. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim.
9. Kedua orang tua beserta kakak dan adik penulis yang telah memberikan semangat dan motivasi kepada penulis.
10. Seluruh teman-teman mahasiswa Program Studi Matematika angkatan 2018.

Penulis berharap, semoga skripsi ini dapat memberikan manfaat bagi penulis dan pembaca.

Wassalamu'alaikum Wr.Wb.

Malang, 26 Juni 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

ABSTRAK

Novianti, Chofifah Alfin. 2023. **Pengamanan Pesan Teks Menggunakan Kriptografi Hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack*.** Skripsi. Program Studi Matematika. Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si (II) Mohammad Nafie Jauhari, M.si

Kata Kunci: *Cipher Block Chaining* (*CBC*), *Merkle-Hellman Knapsack*, Kriptografi

Pesan rahasia merupakan pesan yang hanya boleh dilihat oleh orang yang berhak. Dalam pengirimannya diperlukan suatu prosedur agar pesan rahasia dapat terjaga yang disebut sebagai kriptografi. Pada penelitian ini menggunakan kriptografi hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack*. Tujuan penelitian ini yaitu untuk mengetahui proses enkripsi dan dekripsi dari kriptografi hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack*. Tahapan dalam penelitian ini menggunakan pendekatan kualitatif dengan metode kajian Pustaka. Pada proses enkripsi dengan *CBC*, plainteks dienkripsi terlebih dahulu dan menghasilkan cipherteks. Selanjutnya kunci dan *Initialization Vector* (*IV*) dari *CBC* dienkripsi menggunakan *Merkle-Hellman Knapsack* dengan membangkitkan kunci publik terlebih dahulu dan menghasilkan *cipherkey*. Kebalikan dari enkripsi, pada proses dekripsi *cipherkey* terlebih dahulu didekripsi menggunakan *Merkle-Hellman Knapsack* dengan menghitung balikan modulo $n \bmod m$. Proses dekripsi dilanjutkan dengan mendekripsi cipherteks menggunakan *CBC*. Hasil dari pesan yang diamankan menggunakan kriptografi hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack* memiliki tingkat keamanan lebih tinggi dibandingkan dengan hanya menggunakan satu algoritma kriptografi saja. Adapun untuk kedepannya, penelitian ini dapat digunakan untuk memperluas pengetahuan mengenai pengamanan pesan teks menggunakan kriptografi hibrida algoritma *CBC* dan *Merkle-Hellman Knapsack*.

ABSTRACT

Novianti, Chofifah Alfin. 2023. **Securing Text Messages Using Hybrid Cryptography Cipher Block Chaining (CBC) and Merkle-Hellman Knapsack.** Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Supervisors: (I) Muhammad Khudzaifah, M.Si (II) Mohammad Nafie Jauhari, Msi

Keywords: Cipher Block Chaining (CBC), Cryptography, Merkle-Hellman Knapsack

A secret message is a message that can only be seen by those who are entitled. In its delivery, a procedure is needed to keep the secret message secure, which is called cryptography. This research uses hybrid cryptography Cipher Block Chaining (CBC) and Merkle-Hellman Knapsack. The purpose of this research is to find out the encryption and decryption process of hybrid cryptography Cipher Block Chaining (CBC) and Merkle-Hellman Knapsack. The stages in this research use a qualitative approach with the library research method. In the encryption process with CBC, plaintext is encrypted first and the result called ciphertext. Furthermore, the key and Initialization Vector (IV) from CBC are encrypted using Merkle-Hellman Knapsack by generating a public key first and producing cipherkey. In the decryption process cipherkey is first decrypted using Merkle-Hellman Knapsack by calculating the inverse modulo $n \bmod m$. The decryption process continues by decrypting ciphertext using CBC. The result of securing messages using hybrid cryptography Cipher Block Chaining (CBC) and Merkle-Hellman Knapsack has a higher level of security than using only one cryptographic algorithm. As for the future, this research can be used to expand knowledge about securing text messages using hybrid cryptography algorithm CBC and Merkle-Hellman Knapsack.

.مستخلص البحث

نوفيانتي ، خفيفة ألفين. ٢٠٢٣. أمان الرسائل النصية باستخدام *Cipher Block (CBC) Chaining* و *Merkle-Hellman Knapsack*. البحث العلمي. قسم الرياضيات. كلية العلوم والتكنولوجيا ، جامعة الإسلامية الحكومية مولانا مالك إبراهيم مالانج. المستشار المشرف (١) محمد خديفة ،الماجستير (٢) محمد نافع جوهري، الماجستير

الكلمات المفتاحية: التشفير ، *Cipher Block Chaining(CBC)* ، *Merkle-Hellman Knapsack*

الرسالة السرّية هي الرسالة التى تعرف للأشخاص المعيّن ، يلزم إجراء حتى يمكن الاحتفاظ بالرسائل السرية ، وهو ما يُعرف باسم التشفير. في هذه الدراسة يستخدم التشفير الهجين، *Cipher (CBC) Block Chaining* و *Merkle-Hellman Knapsack*. الغرض من هذه الدراسة هو تحديد عمليات التشفير وفك تشفير *Cipher Block Chaining(CBC)* والتشفير الهجين *Merkle-Hellman Knapsack*. استخدمت مراحل هذه الدراسة نهجًا نوعيًا مع طريقة مراجعة الأدبيات. في عملية التشفير باستخدام *CBC* ، ثم يتم تشفير المفتاح وناقل التهيئة (IV) من *CBC* باستخدام *Merkle-Hellman Knapsack* عن طريق إنشاء المفتاح العام أولاً وإنشاء مفتاح التشفير. على عكس التشفير ، في عملية فك التشفير ، يتم أولاً فك تشفير مفتاح التشفير باستخدام *Merkle-Hellman Knapsack* عن طريق حساب النمط العكسي $n \bmod m$. تستمر عملية فك التشفير عن طريق فك تشفير النص المشفر باستخدام *CBC*. نتائج الرسائل المؤمنة باستخدام تشفير هجين *Cipher Block Chaining(CBC)* و *Merkle-Hellman Knapsack* تتمتع بمستوى أعلى من الأمان مقارنة باستخدام خوارزمية تشفيرفقط. بالنسبة للمستقبل ، يمكن استخدام هذا البحث لتوسيع المعرفة حول أمن الرسائل النصية باستخدام خوارزميات التشفير الهجين *CBC* و *Merkle-Hellman Knapsack*.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Salah satu sifat dasar manusia adalah berkomunikasi dengan satu sama lain. Cara berkomunikasi terus mengalami perkembangan, salah satunya dengan komunikasi melalui pesan. Pesan merupakan suatu informasi yang dapat dibaca dan dipahami artinya serta memiliki berbagai macam bentuk seperti simbol, gambar, dan tulisan. Dalam pembagiannya, pesan dapat dibagi menjadi beberapa bagian, seperti pesan untuk satu orang, banyak orang, suatu golongan, dan pesan rahasia. Pesan rahasia sendiri adalah pesan yang tidak boleh diketahui oleh siapapun kecuali orang yang berhak menerimanya. Terdapat banyak ancaman dan gangguan dalam pengiriman pesan rahasia. Oleh karena itu diperlukan suatu prosedur agar pesan rahasia dapat dijaga kerahasiaannya.

Sebuah prosedur yang umum digunakan disebut sebagai kriptografi. Kriptografi adalah ilmu yang menekuni metode-metode matematika yang bersangkutan dengan keamanan pesan (Ariyus, 2008). Pesan yang akan dikirimkan terlebih dahulu disandikan oleh pengirim pesan. Terdapat dua proses yang digunakan untuk menyandikan pesan, yaitu enkripsi dan dekripsi pesan. Enkripsi adalah proses merubah pesan asli (plainteks) menjadi pesan yang tidak dapat dipahami (cipherteks). Sedangkan, dekripsi merupakan kebalikan dari enkripsi, yaitu pesan yang telah dienkripsi akan dikembalikan ke bentuk asal pesan (plainteks). Menjaga kerahasian dan keamanan pesan merupakan suatu amanat yang penting agar isi dari pesan dapat tersampaikan dengan baik kepada yang

berhak. Pentingnya menjaga amanat telah tercantum dalam firman Allah SWT surat Al-Anfal ayat 27:

Artinya:"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" (Q.S. Al-Anfal:27).

Sesuai dengan ayat di atas, menjaga amanat dapat diartikan sebagai menjaga kerahasiaan pesan yang akan disampaikan kepada penerima pesan. Dalam ilmu matematika, merahasiakan pesan dibutuhkan sebuah metode kriptografi yang diharapkan pesan yang dikirimkan dapat terjaga kerahasiaannya. Kriptografi yang digunakan dalam penelitian ini adalah kriptografi hibrida, yaitu penggabungan antara algoritma kriptografi simestris dan asimetris agar mendapatkan hasil lebih kuat daripada hanya menggunakan satu algoritma.

Cipher Block Chaining (*CBC*) adalah algoritma kriptografi *block cipher* yang prosesnya menggunakan plainteks/cipherteks yang berbentuk blok-blok bit (atau blok *byte*) (Ariyus, 2006). Rangkaian bit terbagi menjadi beberapa blok yang panjangnya telah ditentukan. Enkripsi dan dekripsi akan dilakukan di setiap bloknya dengan kunci yang sama. Metode ini menerapkan mekanisme umpan-balik pada sebuah blok. Untuk pengoperasian blok pertama, digunakan sebuah *Initialization Vector* (IV) yang dibangkitkan secara acak. Cipherteks yang dihasilkan kemudian di-XOR-kan dengan blok pada proses selanjutnya. Hal ini dilakukan agar blok pesan yang sama akan menghasilkan cipherteks yang berbeda, sehingga proses kriptanalisis menjadi lebih sulit. Selanjutnya akan digunakan algoritma *Merkle-Hellman Knapsack* yang merupakan algoritma kriptografi asimetris, di mana terdapat dua kunci yang akan digunakan yaitu, kunci publik (*public key*) dan kunci rahasia (*private key*). Mekanisme pengerjaan *Merkle-*

Hellman Knapsack adalah dengan menentukan *key generation* dari barisan *superincreasing.* Barisan *superincreasring* merupakan barisan di mana setiap nilai di dalam barisan lebih besar daripada jumlah semua nilai sebelumnya.

Beberapa penelitian sebelumnya telah dilakukan oleh peneliti sebelumnya. Dalam penelitian Rosmala (2012) algoritma *Cipher Block Chaining* (*CBC*) digunakan untuk proses enkripsi dan dekripsi pada pengamanan data, seperti bentuk pesan teks, dokumen, dan gambar, karena dalam penerapannya digunakan digit biner, sehingga pada proses enkripsi pesan tidak dapat terbaca serta waktu yang diperlukan cukup singkat. Penelitian lain tentang aplikasi penggunaan *Merkle-Hellman Knapsack* dalam pengamanan pesan teks. Pada penelitian Hidayat (2016) algoritma *Merkle-Hellman Knapsack* digunakan untuk proses dekripsi dan enkripsi teks. Penggunaan algoritma ini dinilai memiliki ukuran kunci yang lebih kecil dibandingkan dengan algoritma *Rivest Shamir Adleman* (RSA) dan memiliki kemampuan keamanan yang kuat dengan panjang kunci yang pendek. Dalam penelitian Sulaiman (2019) menyatakan bahwa *XOR Cipher* dapat dikombinasikan dengan kriptografi *Merkle-Hellman Knapsack* untuk meningkatkan pengamanan pesan teks. Kombinasi ini dinilai lebih aman penggunaannya untuk mengamankan pesan teks. Hal ini dikarenakan dalam proses enkripsi pesan, dilakukan dua kali dengan metode kriptografi yang berbeda dan diperlukan kode ASCII dalam proses penyandian pesan. Berdasarkan permasalahan di atas, peneliti tertarik untuk melakukan penelitian yang berjudul "Pengamanan Pesan Teks Menggunakan Kriptografi Hibrida *Cipher Block Chaining* (*CBC*) Dan *Merkle-Hellman Knapsack*".

1.2 Rumusan Masalah

Berdasarkan latar belakang dari penelitian tersebut, maka rumusan masalah penelitian ini sebagai berikut:

1. Bagaimanakah proses enkripsi pesan teks menggunakan kriptografi hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack*?
2. Bagaimanakah proses dekripsi pada pesan teks menggunakan kriptografi hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack?*

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan sebelumnya, maka tujuan penelitian ini sebagai berikut:

1. Mengetahui proses enkripsi pesan teks menggunakan kriptografi hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack.*
2. Mengetahui proses dekripsi pesan teks menggunakan kriptografi hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack.*

1.4 Manfaat Penelitian

Adapun beberapa manfaat yang pada penelitian ini, adalah sebagai berikut:

1. Mengimplementasikan algoritma hibrida menggunakan algoritma *CBC* dan *Merkle-Hellman Knapsack*.
2. Menambah pengetahuan lebih dalam mengenai pengamanan pesan teks menggunakan kriptografi hibrida algoritma *CBC* dan *Merkle-Hellman Knapsack*.
3. Memperbanyak bahan literasi dan informasi yang melingkupi kriptografi.

1.5 Batasan Masalah

Batasan masalah yang akan dibahas dalam penelitian ini adalah penggunaan 53 karakter yang terdiri dari huruf alfabet (A-Z dan a-z), angka, serta penggunaan tanda pagar (#) sebagai spasi.

1.6 Definisi Istilah

1. Plainteks adalah pesan berupa teks yang jelas (*cleartext)*, dapat berupa gambar, audio, dan video.
2. Cipherteks adalah pesan yang telah tersandi.
3. Enkripsi adalah proses menyandikan plainteks menjadi cipherteks.
4. Dekripsi adalah proses mengembalikan cipherteks menjadi plainteks semula.
5. ASCII singkatan dari *American Standard Code for Information Interchange* digunakan untuk merubah teks asli menjadi sebuah urutan digit biner, yaitu 0 dan 1.
6. *Initialization Vector (IV)* adalah suatu blok bit acak yang diperlukan untuk enkripsi pesan.
7. XOR *(Exlusive OR)* adalah metode penggabungan operasi dua bit.
8. *Superincreasing* adalah barisan di mana setiap nilai di dalam barisan lebih besar daripada jumlah semua nilai sebelumnya.

BAB II

KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Keterbagian

Definisi 2.1

Misalkan a dan b adalah dua bilangan bulat dengan syarat $a \neq 0$. Dapat dinyatakan bahwa a habis membagi b (a *divides* b) jika terdapat bulangan bulat c sedemikian sehingga $b = ac$. Keterbagian dapat dinotasikan sebagai $a|b$ dibaca dengan "a membagi b" atau "b habis dibagi a" atau "a faktor b" atau "b kelipatan dari a". Apabila a tidak membagi b, ditulis dengan $a \nmid b$. Apabila $a|b$ dan $0 < a < b$, maka a disebut pembagi sejati dari b (Irawan, dkk, 2014).

Contoh

$4|12$, karena terdapat $3 \in \mathbb{Z}$ sehingga $12 = 4 \cdot 3$

$5 \nmid 13$, karena tidak ada $g \in \mathbb{Z}$ sehingga $13 = 5g$

2.1.2 Faktor Persekutuan Terbesar

Definisi 2.2

Misalkan a dan b adalah dua bilangan bulat bukan nol. Pembagi bersama terbesar (FPB) dari a dan b adalah bilangan bulat terbesar d sedemikan sehingga $d|a$ dan $d|b$, dapat dinyatakan sebagai FPB $(a, b) = d$.

Contoh

Faktor pembagi $56 = 1, 2, 4, 7, 8, 14, 28, 56$

Faktor pembagi $42 = 1, 2, 3, 7, 21, 42$

Faktor pembagi bersama dari 56 dan 42 adalah $1, 2, 7$

FPB $(56, 42) = 7$

Teorema 2.1

Misalkan $a, b, c \in \mathbb{Z}$. Jika c adalah FPB dari a dan b, maka $c|(a + b)$.

Bukti

Karena c adalah FPB dari a dan b, maka $c|a$ dan $c|b$. Karena $c|a$ dan $c|b$, maka berarti $a = cd_1$ dan $b = cd_2$ untuk suatu bilangan bulat d_1, d_2. Jumlah dari a dan b adalah

$$a + b = cd_1 + cd_2 = c(d_1 + d_2)$$

Dapat dilihat bahwa c habis membagi $a + b$.

Contoh

FPB dari 56 dan 42 adalah 7, maka menurut Teorema 1, 7 habis membagi $56 + 42 = 98$, atau $9|(56 + 36)$.

Teorema 2.2

Misalkan $a, b, c \in \mathbb{Z}$. Jika c adalah FPB dari a dan b, maka $c|(a - b)$.

Bukti

Karena c adalah FPB dari a dan b, maka $c|a$ dan $c|b$. Karena $c|a$ dan $c|b$, maka berarti $a = cd_1$ dan $b = cd_2$ untuk suatu bilangan bulat d_1, d_2. pengurangan dari a dan b adalah

$$a - b = cd_1 - cd_2 = c(d_1 - d_2)$$

Dapat dilihat bahwa c habis membagi $a - b$.

Contoh

FPB dari 56 dan 42 adalah 7, maka menurut Teorema 2, 7 habis membagi $56 - 42 = 14$, atau $9|(56 - 36)$.

Teorema 2.3

Misalkan $a, b, c \in \mathbb{Z}$. Jika $c|a$, maka $c|ab$.

Bukti

Karena $c|a$, maka terdapat $d \in \mathbb{Z}$, sehingga $c = ad$.

Perhatikan bahwa untuk sebarang $e \in \mathbb{Z}$, berlaku

$$c \cdot e = (a \cdot d)e = a(de)$$

Jadi, $c \cdot e = a \cdot b$ untuk sebarang $b = d \cdot e \in \mathbb{Z}$.

Dapat dilihat bahwa jika c membagi habis ab.

Contoh

FPB dari 56 dan 42 adalah 7, maka menurut Teorema 3, 7 habis membagi $56 \cdot 42 = 2352$, atau $9|(56 \cdot 36)$.

2.1.3 Aritmatika Modulo

Aritmatika modulo memiliki peran penting dalam perhitungan bilangan bulat, khususnya pada aplikasi kriptografi. Operator yang digunakan pada aritmatika modulo adalah mod. Operator mod menghasilkan hasil sisa pembagian. Misalnya 46 dibagi 7 menghasilkan 6 dan sisa 4, sehingga dapat ditulis $46\ mod\ 7 = 4$ (Munir, 2016).

Definisi 2.3

Misalkan a aadalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a\ mod\ m$ memberikan sisa jika a dibagi m. Dengan kata lain, $a\ mod\ m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$.

2.1.4 Kongruensi

Cara lain mempelajari keterbagian dalam bilangan bulat dapat menggunakan kongruensi.

Definisi 2.4

Misalkan bilangan bulat x bukan nol, membagi selisih $a - b$, maka dapat dikatakan a kongruen dengan b modulo x, dan ditulis $a \equiv b \ (mod\ x)$. Jika x tidak membagi $a - b$, maka dapat dikatakan a tidak kongruen dengan $b\ mod\ x$, dan ditulis $a \not\equiv b \ (mod\ x)$. Jika $x > 0$ dan $x|(a - b)$ terdapat $y \in \mathbb{Z}$, sehingga $a - b = xy$ atau $a = xy + b$ (Irawan, dkk, 2014). Kekongruenan $a \equiv b \ (mod\ x)$ dapat pula dituliskan dalam hubungan $a = b + km$, yang mana k adalah bilangan bulat. Pembuktiannya sebagai berikut:

Menurut definisi 2.4, $a \equiv b \ (mod\ x)$ jika x membagi selisih $(a - b)$, menurut definisi 2.1 pada keterbagian terdapat bilangan bulat k sedemikian sehingga $a - b = km$ atau $a = b + km$.

Teorema 2.4

Misalkan $a, b,$ dan c adalah bilangan bulat dan x adalah bilangan asli, maka berlaku:

1. Refleksi $a \equiv a \ (mod\ x)$.
2. Simetris, jika $a \equiv b \ (mod\ x)$, maka

   $b \equiv a \ (mod\ x)$ dan $a - b = 0 \ (mod\ x)$ adalah pernyataan yang ekuivalen.
3. Transitif, jika $a \equiv b \ (mod\ x)$ dan $b \equiv a \ (mod\ x)$ maka $a \equiv c \ (mod\ x)$ (Irawan, dkk, 2014).

Bukti

1. Jika $t \not\equiv 0$ maka $t|0$ dapat dituliskan sebagai $t|a - a$.

Menurut definisi berlaku $a \equiv b\ (mod\ t)$, untuk semua bilangan bulat t dan $t \neq 0$.

2. $a \equiv b\ (mod\ t)$ berarti $m|a-b$, menurut definisi terdapat keterbagian bilangan bulat y sehingga

   $t|a-b$ dapat dinyatakan $a-b=yt$

   $\Leftrightarrow -(-a-b)=-yt$

   $\Leftrightarrow b-a=(-y)t$

   Menurut definisi, $b \equiv a\ (mod\ t)$ berarti $t|a-b$ dapat dinyatakan $a-b=yt$, untuk setiap $(a-b)-0=yt$ maka $(a-b) \equiv 0\ (mod\ t)$.

3. Menurut definisi terdapat bilangan bulat y_1 dan y_2 sehingga

   $t|a-b$ dapat dinyatakan $a-b=y_1t$

   $t|b-c$ dapat dinyatakan $b-c=y_2t$

   Kedua persamaan (3.1) dan (3.2) dijumlahkan sehingga diperoleh

   $a-c=(y_1+y_2)t$.

   Sesuai definisi, maka diperoleh $a \equiv c\ (mod\ t)$.

Teorema 2.5

Jika $a \equiv b\ (mod\ t)$, maka $a+c \equiv b+c\ (mod\ t)$.

Bukti

$a \equiv b\ (mod\ t)$ berarti $t|a-b$

Menurut definisi, keterbagian ada bilangan bulat y sehingga

$t|a-b$ dapat dinyatakan $a-b=yt$

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

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

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

Sesuai definisi, maka diperoleh $a + c \equiv b + c \ (mod\ t)$

2.1.5 Bilangan Prima

Bilangan prima adalah bilangan asli lebih dari satu yang tepat memiliki dua faktor, yaitu satu dan dirinya sendiri (Irawan, dkk, 2014). Sedangkan bilangan asli yang memiliki lebih dari 2 faktor disebut sebagai bilangan komposit.

Definisi 2.5

Bilangan bulat $p > 1$ disebut bilangan prima atau prima, jika pembaginya hanya 1 dan p.

2.1.6 Relatif Prima

Dikatakan relatif prima apabila dua bilangan bulat a dan b memiliki FPB$(a, b) = 1$ (Munir, 2005). Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n sehingga

$$ma + nb = 1$$

Contoh

Faktor pembagi $11 = 1, 11$

Faktor pembagi $21 = 1, 3, 7, 21$

Faktor pembagi bersama 11 dan 21 adalah 1.

Jadi, 11 dan 21 relatif prima karena FPB$(11,21) = 1$, atau dapat ditulis

$$2 \cdot 11 + (-1) \cdot 21 = 1$$

dengan $m = 2$ dan $n = -1$. Tetapi 15 dan 5 bukanlah relatif prima karena FPB$(15,5) = 5 \neq 1$ sehingga 15 dan 5 tidak dapat dinyatakan dalam $m \cdot 15 + n \cdot 5 = 1$ (Munir, 2005).

2.1.7 Algoritma

Algoritma adalah suatu prosedur atau metode logis dan sistematis digunakan dalam memecahkan masalah tertentu. Menurut Sukamto tahun 2010, algoritma adalah sebuah solusi penyelesaian masalah yang harus dipecahkan oleh komputer. Algoritma harus dibuat secara teratur agar komputer mengerti dan dapat mengeksekusinya. Selain digunakan dalam memecahkan masalah dalam komputer, algoritma juga dapat diterapkan dalam kehidupan sehari-hari yang membutuhkan langkah-langkah untuk pemecahannya.

2.1.8 Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani, "*cryptós*" berarti rahasia dan "*gráphein*" berarti tulisan. Secara harfiah kriptografi berarti tulisan rahasia. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari suatu tempat ke tempat lain (Ariyus, 2008). Kata "seni" dalam definisi di atas berasal dari fakta sejarah bahwa pada masa awal kriptografi setiap orang memiliki teknik yang berbeda dalam menjaga rahasia. Teknik-teknik yang berbeda menjadikan setiap pesan yang ditulis memiliki nilai estetikanya sendiri. Oleh karena itu, kriptografi pun berkembang menjadi sebuah seni merahasiakan pesan (Munir, 2009).

Dalam kriptografi, terdapat dua teknik yang digunakan yaitu enkripsi dan dekripsi. Enkripsi adalah teknik dimana pesan asli (plainteks) diubah menjadi pesan acak (*ciphertext*) menggunakan kunci enkripsi yang hanya diketahui oleh pengaman pesan. Sedangkan dekripsi adalah kebalikan dari enkripsi yaitu teknik untuk mendapatakan kembali pesan asli dengan kunci dekripsi.

Sebelum adanya komputer, kriptografi hanya menggunakan pensil dan kertas saja. Algoritma yang digunakan hanyalah algoritma kriptogafi klasik dengan enkripsi dan dekripsi dilakukan terhadap karakter dalam pesan dimana hanya satu kunci yang digunakan dalam enkripsi dan dekripsinya (Munir, 2019). Dua teknik dasar yang digunakan pada kriptografi klasik adalah

1. Teknik Substitusi: setiap karakter pada pesan awal (plainteks) diganti dengan karakter lain.
2. Teknik Transposisi: permutasi karakter digunakan pada teknik ini (Ariyus, 2006).

Setelah adanya komputer kriptografi berkembang menjadi kriptografi modern. Dalam kriptografi modern, pesan awal dikonversi menjadi bentuk biner, yaitu 0 dan 1. ASCII merupakan skema enkoding yang umum digunakan untuk merubah pesan asli menjadi bentuk digit biner. Urutan bit yang mewakili pesan asli (plainteks) kemudain dienkripsi untuk mendapatkan pesan acak (*ciphertext*). Kriptografi modern dibagi menjadi dua bentuk dasar yaitu

1. *Stream Cipher* (*cipher* alir): merupakan algoritma yang mengenkripsi plainteks menjadi teks kode bit per bit (1 bit setiap kali transformasi.
2. *Block Cipher* (*cipher* blok): merupakan suatu algoritma yang masukan dan keluarannya berupa satu blok dan setiap blok terdiri dari beberapa bit (1 blok terdiri dari 64 bit atau 128 bit). (Ariyus, 2008).

2.1.9 Algoritma Kriptografi

Menurut definisi terminologinya, algoritma adalah urutan langkah-langkah logis untuk menyelesaikan masalah yang disusun secara sistematis. Algoritma

kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut (Ariyus, 2006). Algoritma kriptografi terdiri dari tiga fungsi dasar yaitu

1. Enkripsi: Enkripsi merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dapat dikirimkan terjaga kerahasiaan pesan asli (plainteks). Pesan asli diruba menjadi pesan acak yang tidak dapat dimengerti.
2. Dekripsi: Dekripsi merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (plainteks). Tentu algoritma yang digunakan untuk deskripsi berbeda dengan yang digunakan untuk enkripsi.
3. Kunci: kunci yang dimaksud di sini adalah kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua, kunci pribadi dan kunci umum.

2.1.10 Block Cipher

Pada *cipher* ini, bit-bit plainteks yang akan dibagi menjadi blok-blok bit dengan panjang yang sama. Enkripsi setiap blok bit plainteks menggunakan bit-bit kunci yang memiliki panjang yang sama dengan blok bit plainteks. Dekripsi dilakukan dengan cara yang sama dengan ekripsi, proses dekripsi menggunakan blok bit cipherteks yang didekripsi dengan blok bit yang sama.

2.1.11 Bit String pada Kriptografi Modern

Pada pengoperasian kriptografi modern, plainteks perlu dikonversi menjadi suatu digit biner, 0 dan 1. Schema encoding yang umum digunakan adalah ASCII

(*American Standart Code for Information Interchange*). Urutan bit yang akan mewakili plainteks kemudian dienkripsi untuk mendapatkan *ciphertext* dalam bentuk urutan bit. Terdapat dua tipe algoritma kritpgrafi modern, tipe pertama adalah aliran kode, dimana urutan bit untuk dienkripsi digunakan *byte by byte*. Tipe yang kedua adalah algoritma blok kode dimana urutan bit dibagi menjadi beberapa blok. Untuk mendapatkan satu karakter ASCII diperlukan 8 bit biner dan 64 bit blok kode untuk satu blok. Sebagai contoh urutan 12 bit: 100111001111 yang dipecah menjadi 4 blok maka akan mendapatkan 1001 1100 1111. Cara umum untuk menulis bit string dengan menggunakan notasi *Hexadecimal* (*HEX*). Untuk HEX string dibagi dalam bentuk blok yang berukuran empat sebagai berikut:

$0000 = 0,\ 0001 = 1,\ 0010 = 2,\ 0011 = 3,$

$0100 = 4,\ 0101 = 5,\ 0110 = 6,\ 0111 = 7,$

$1000 = 8,\ 1011 = 9,\ 1111 = A,\ 1011 = B,$

$1100 = C,\ 1101 = D,\ 1110 = D,\ 1111 = F.$

Binari string merupakan bagian operasi algoritma cipher, maka pemahaman terhadap metode kombinasi dua bit yang disebut *Exclusive OR* diperlukan. *Exclusive OR* dinotasikan dengan $\oplus$. Operasi XOR mengkombinasikan dua bit string dengan panjang yang sama. Dengan penambahan modulo 2 dan digambarkan sebagai berikut $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$ (Ariyus, 2006).

2.1.12 *Cipher Block Chaining* (CBC)

Cipher Block Chaining (*CBC*) adalah algoritma kriptografi yang prosesnya menggunakan plainteks/cipherteks yang berbentuk blok-blok bit (atau blok *byte*). Rangkaian bit terbagi menjadi beberapa blok yang panjangnya telah ditentukan. Enkripsi dan dekripsi akan dilakukan di setiap bloknya dengan kunci yang sama.

Metode ini menerapkan mekanisme umpan-balik pada sebuah blok. Dengan CBC, cipherteks tidak hanya bergantung pada kunci yang digunakan, tetapi bergantung pada seluruh blok plainteks sebelumnya. Secara matematis, enkripsi dengan metode CBC adalah

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

Sebuah *iniltialization vector (IV)* yang dibangkitkan secara acak digunakan untuk pengoperasian blok pertama karena tidak adanya C_0. Jadi, $C_0 = IV$. Jadi, untuk m buah blok plainteks, enkripsinya adalah

$$C_1 = E_K(P_1 \oplus IV)$$

$$C_2 = E_K(P_1 \oplus C_1)$$

$$C_3 = E_K(P_1 \oplus C_2)$$

$$\vdots$$

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

Sedangkan untuk dekripsi, blok plainteks pertama diperoleh dari meng-XOR-kan IV dengan hasil dekripsi terhadap blok cipherteks pertama. Sehingga, IV tidak perlu dirahasiakan. Secara matematis, dekripsi dengan teknik CBC dinyatakan sebagai berikut

$$P_1 = D_K(C_1) \oplus IV$$

$$P_2 = D_K(C_2) \oplus C_1$$

$$P_3 = D_K(C_3) \oplus C_2$$

$$\vdots$$

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

2.1.13 Algoritma Knapsack

Keamanan algoritma *knapsack* didasari oleh sulitnya memecahkan persoalan *knapsack (knapsack problem)*. *Knapsack* artinya karung/kantung. Barang-barang yang termuat dalam karung hanya terbatas sampai batas kapasitas maksimum karung. Jika total barang melebihi kapasitas karung, maka hanya beberapa barang yang dapat masuk ke dalam karung.

Knapsack Problem

Diberikan bobot *knapsack* adalah M. Diketahui n adalah barang yang bobotnya $w_1, w_2, w_3, \dots, w_n$. Tentukan nilai b_i sedemikian hingga

$$M = w_1 b_1 + w_2 b_2 + \cdots + w_n b_n \tag{2.9}$$

Dalam hal ini, b_i memiliki nilai 0 atau 1. Jika nilai $b_i = 1$, berarti barang i dimasukkan ke dalam *knapsack*, sebaliknya jika $b_i = 0$, barang i tidak dimasukkan. Misalnya untuk $M = 15, w_1 = 5, w_2 = 3, w_3 = 8, w_4 = 2, w_5 = 7$, maka salah satu solusinya adalah $15 = 1 \cdot 5 + 0 \cdot 3 + 1 \cdot 8 + 1 \cdot 2 + 0 \cdot 7$.

Dalam teori algoritma, persoalan *knapsack* termasuk dalam kelompok *NP-Complete*. Persoalan yang termasuk dalam *NP-Complete* tidak dapat dipecahkan dalam orde waktu polinomial.

Algoritma *Knapsack* Sederhana

Algoritma kriptografi *knapsack* memiliki ide dasar yang mengkodekan pesan sebagai rangkaian penyelesaian dari persoalan *knapsack*. Dalam persoalan *knapsack* kunci privat didapat dari setiap bobot w_i, sedangkan b_i dinyatakan sebagai bit-bit plainteks.

Superincreasing Knapsack

Superincreasing knapsack adalah persoalan *knapsack* yang dapat dipecahkan dalam waktu polinomial atau $O(n)$. Pemecahan persoalan ini dapat dilakukan dengan mudah namun tidak disukai untuk dijadikan sebagai algoritma kriptografi yang mudah. *Superincreasing knapsack* merupakan algoritma yang lemah, karena dekripsi cipherteks dilakukan secara mudah untuk menghasilkan plainteks dalam waktu polinomial. Dari segi komputasi, kelompok *superincreasing knapsack* dapat dimodifikasi menjadi barisan *non-superincreasing knapsack* atau *normal knapsack* adalah kelompok algoritma ini sulit dipecahkan karena membutuhkan waktu dalam orde eksponensial untuk pemecahannya.

2.1.14 *Merkle-Hellman Knapsack*

Superincreasing knapsack dapat dimodifikasi menjadi barisan *non-superincreasing knapsack* dengan menggunakan kunci publik dan kunci privat. Kunci publik didapatkan dari barisan non-*superincreasing* sedangkan kunci privat didapatkan dari barisan *superincreasing*. Hasil modifikasi ini ditemukan oleh Martin Hellman dan Ralph Merlke pada tahun 1978 sehingga dinamai dengan algoritma *Merkle-Hellman Knapsack*. Algoritma ini dilakukan dengan perhitungan aritmatika modulo. (Munir, 2019)

Algoritma ini memiliki tiga tahapan mekanisme. Tahap pertama adalah proses pembangkitan kunci publik dan kunci privat, kedua tahap enkripsi, dan ketiga tahap dekripsi. Mekanisme algoritma *Merkle-Hellman Knapsack* antara lain:

1. Menentukan barisan *superincreasing*, $w = (w_1, w_2, \dots, w_n)$, nilai n, dan m di mana $FPB(n, m) = 1$ dan m memiliki angka yang lebih besar dari jumlah semua elemen di dalam barisan w.

2. Mengalikan setiap elemen w dengan $n\ mod\ m$ atau dengan persamaan

   $\beta_i = w_i \cdot n\ mod\ m$

3. Didapatkan β_i merupakan kunci publik, sedangkan w adalah kunci privat.

4. Melakukan proses enkripsi dengan rumus:

   $c = \sum_{i=1}^{n} \alpha_i \beta_i$

   keterangan:

   c = cipherteks

   β_i = kunci publik

   α_i = kode biner

5. Tahapan dekripsi dilakukan dengan rumus:

   $c = \sum_{i=1}^{n} \alpha_i w_i$

   Sebelum melakukan dekripsi, mula-mula hitung terlebih dahulu n^{-1}, yaitu balikan $n\ mod\ m$. Menggunakan kekongruenan maka didapatkan:

   $n \equiv 1\ (mod\ m)$

   $n \cdot n^{-1} \equiv 1\ (mod\ m)$ (invers dari n adalah n^{-1})

   $\Leftrightarrow n \cdot n^{-1} = 1 + km$ (Definisi 2.4)

   $\Leftrightarrow n^{-1} = \frac{1+km}{n}$ (Kedua ruas dibagi n)

2.2 Kajian Keislaman dalam Kriptografi

Masalah keamanan merupakan sebuah aspek penting dalam sebuah sistem informasi. Jika pesan terganggu maka semua hal yang terkait dengan informasi tersebut tidak dapat dilakukan dengan baik. Sudah semestinya menjaga pesan dilakukan dengan baik dan benar. Menjaga kerahasian dan keamanan pesan merupakan hal yang sangat penting agar isi dari pesan hanya diketahui oleh orang

yang berhak dan bertanggung jawab. Sesuai dengan definisinya, kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan. Allah telah berfirman dalam al-Quran mengenai pentingnya menjaga amanat dalam QS. An-Nisa' ayat 58 yang berbunyi:

> *Artinya:"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat" (Q.S An-Nisa':58)*

Berdasarkan ayat di atas, menurut Wahbah az-Zuhaili perintah mengenai wajibnya menjaga amanah untuk setiap muslim haruslah dipahami. Amanah yang dimaksud adalah semua amanah yang ada, baik untuk hak diri sendiri, atau yang berhubungan dengan hak orang lain, maupun yang berhubungan dengan hak Allah. Menjaga amanah adalah wajib dan menyampaikan amanah haruslah kepada yang berhak. Bentuk amanah yang berkaitan dengan cara menjalankan perintah-perintah-Nya, meninggalkan segala larangan-Nya, dan menggunakan hati serta anggota tubuh untuk mendekatkan diri kepada Allah. Adapun bentuk amanah yang berhubungan dengan diri sendiri adalah dengan cara melakukan sesuatu yang bermanfaat baik di dunia maupun akhirat. Sedangkan bentuk amanah yang berkaitan dengan orang lain adalah dengan mengembalikan barang titipan, memberi nasehat, dan tidak menyebarkan rahasia orang lain (Al-Munir, 2013).

Menjaga dan melaksanakan amanah adalah wajib, terutama jika orang berhak terhadap amanah menuntutnya. Sesungguhnya Allah Maha Mengetahui. Allah mengetahui apakah pembawa pesan melaksanakan amanah atau mengkhianati amanah.

Diriwayatkan oleh Imam Muslim dari Abu Hurairah bahwa Rasulullah SAW bersabda yang artinya:

"*(Di hari Kiamat) semua hak akan diberikan kepada pihak yang memang berhak. Bahkan kumpulan kambing akan dihukum qishash akibat tandukannya" (HR. Muslim).*

Berdasarkan penjelasan QS.An-Nisa ayat 58 bahwa Allah telah menyampaikan kepada hambanya untuk selalu menjaga amanah yang diberikan dan disampaikan kepada yang berhak. Penyampaian pesan dapat dilakukan dengan merahasiakan pesan asli dan harus dilakukan dengan benar penyampaiannya, apabila pesan mengalami kerusakan dalam perjalanan maka pembawa pesan tersebut meninggalkan kewajibannya untuk menjaga amanah.

2.3 Kajian Topik dengan Teori Pendukung

Kemajuan teknologi memberikan manfaat bagi kehidupan manusia. Selain manfaat baik, perkembangan teknologi juga memunculkan banyak dampak negatif, seperti kejahatan komputer yang mencakup pencurian, penipuan, pemerasan, kompetisi, dan lainnya. Jatuhnya informasi ke pihak yang salah, menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, informasi dari perusahaan A tidak boleh diketahui oleh semua orang, hanya beberapa orang yang berhak untuk mengetahui isi informasi tersebut. Dalam menjaga kerahasiaan informasi diperlukan sebuah algortima dan teknik untuk mengamankan informasi tersebut.

Penelitian ini membahas mengenai teknik algoritma untuk menjaga keamanan informasi. Digunakanlah ilmu kriptografi yang dapat mengamankan informasi. Digunakan dua algoritma agar tingkat keamanan pesan asli yang telah dienkripsi tidak mudah diketahui pihak lain. Konsep yang digunakan dalam

kriptografi adalah matematika diskrit yang mengutamakan teori bilangan. Dalam teori bilangan akan melahirkan sifat-sifat bilangan bulat seperti aritmatika modulo, bilangan prima, dan kongruensi. Sifat-sifat ini berlaku dalam algoritma *Merkle-Hellman Knapsack*. Sedangkan algoritma *Cipher Block Chaining* menerapkan sistem kode ASCII dan bit string. Dalam penelitian ini, peneliti akan meneliti pengamanan pesan menggunakan *Merkle-Hellman Knapsack* dan *Cipher Block Chaining* yang dalam pengamanannya memanfaatkan ilmu matematika dalam pembangkitan kunci, proses enkripsi, dan dekripsi. Sehingga, terdapat keterkaitan antara penelitian ini dengan teori pendukung yang terdapat dalam ilmu matematika.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian kualitatif atau studi literatur atau studi pustaka, yaitu teknik pengumpulan data diambil dari mengkaji berbagai sumber literatur seperti artikel, buku, dan lainnya yang menjelaskan mengenai kriptografi hibrida, algoritma *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack.*

3.2 Pra Penelitian

Pada tahap pra penelitian, peneliti mencari, mempelajari, dan mengkaji beberapa teori yang mendukung proses enkripsi dan dekripsi dalam kriptografi hibrida *Cipher Block Chaining* dan *Merkle-Hellman Knapsack*, seperti:

1. Mencari literatur yang menjadi sumber utama penelitian.
2. Mengumpulkan literatur yang mendukung penelitian.
3. Mempelajari dan memahami tentang XOR *Cipher*.
4. Mempelajari dan memahami tentang kriptografi hibrida, algoritma *Cipher Block Chaining*, dan *Merkle-Hellman Knapsack.*

3.3 Tahapan Penelitian

Berikut tahapan-tahapan yang digunakan untuk penelitian ini adalah:

3.3.1 Proses Enkripsi Menggunakan Kriptografi Hibrida *Cipher Block Chaining (CBC)* dan *Merkle-Hellman Knapsack*

1. Menentukan barisan *superincreasing*, bilangan n, dan bilangan m, dengan $FPB(n, m) = 1$
2. Membangkitkan kunci publik dengan persamaan:

$$\beta_i = w_i \cdot n \; mod \; m$$

3. Menentukan pesan awal (plainteks), kunci, dan *Initialization Vector* (IV) dalam bentuk karakter huruf.
4. Mengubah pesan awal (plainteks), kunci, dan *Initialization Vector* (IV) menjadi biner.
5. Melakukan perhitungan menggunakan *Cipher Block Chaining* (*CBC*) dengan persamaan:

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

6. Mendapatkan *ciphertext* dari proses enkripsi *Cipher Block Chaining* (*CBC*).
7. Mengubah *ciphertext* dari proses enkripsi *Cipher Block Chaining* (*CBC*) dirubah menjadi bilangan HEX.
8. Enkripsi kunci dan IV dari CBC dengan kunci publik, lalu dihasilkan kriptogram sebagai hasil enkripsi (*cipherkey*).

3.3.2 Proses Dekripsi Menggunakan Kriptografi Hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack*

1. Dekripsi *cipherkey* menggunakan *Merkle-Hellman Knapsack* dilakukan dengan menggunakan kunci privat.
2. Menghitung balikan n modulo m, sedemikian sehingga

$$n \cdot n^{-1} \equiv 1 \ (mod\ m)$$

3. Kalikan setiap kriptogram dengan $n^{-1}\ mod\ m$, lalu nyatakan hasil kalinya sebagai penjumlahan elemen-elemen kunci privat untuk memperoleh plainteks dengan menggunakan algoritma pencarian solusi *superincreasing* knapsack,
4. Dihasilkan plainteks kunci dan IV dari CBC.
5. Dekripsi cipherteks menggunakan CBC dengan mengubah cipherteks menjadi bentuk biner.
6. Dekripsi dengan persamaan:

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

7. Mendapatkan plainteks dalam bentuk biner yang selanjutnya diubah menjadi huruf alfabet.
8. Didapatkan kembali pesan awal (plainteks).

BAB IV

HASIL DAN PEMBAHASAN

Bab ini akan membahas mengenai proses enkripsi dan dekripsi pesan teks menggunakan kriptografi hibrida algoritma CBC dan *Merkle-Hellman Knapsack*.

4.1 Proses Enkripsi Menggunakan Kriptografi Hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack*

4.1.1 Algoritma Enkripsi Menggunakan Kriptografi Hibrida *Cipher Block Chaining* (*CBC*) dan *Merkle-Hellman Knapsack*

Adapun tahapan-tahapan yang digunakan dalam proses enkripsi CBC dan *Merkle-Hellman Knapsack* sebagai berikut:

1. Penerima membangkitkan kunci *Merkle-Hellman Knapsack* dengan menentukan nilai barisan *superincreasing* (*w*), *n*, dan *m* secara acak. Dimana nilai $FPB(n, m) = 1$. Pembangkitan kunci menggunakan persamaan $\beta_i = w_i \cdot n \bmod m$. Dari pembangkitan kunci akan didapatkan kunci publik dan kunci privat.
2. Pengirim menentukan plainteks $a_1, a_2, a_3, \dots, a_k \in$ P, kunci $b \in$ K, dan IV $c \in$ IV, dengan P, K, IV adalah himpunan plainteks, kunci, dan IV, dan k merupakan panjang karakter.
3. $\forall\ a_1, a_2, a_3, \dots, a_k \in$ P; $b \in$ K; dan $c \in$ IV akan diubah menjadi biner.
4. Enkripsi plainteks menggunakan CBC dengan persamaan $C_i = E_K(P_i \oplus C_{i-1})$. Kunci dan IV akan digunakan dalan tahap ini.

5. Hasil enkripsi CBC akan diubah menjadi heksadesimal. Untuk setiap karakter yang dihasilkan akan diubah menjadi heksadesimal sehingga menghasilkan cipherteks yang akan diterima penerima pesan adapun $d_1, d_2, d_3, \dots, d_p \in C$, dengan d adalah hasil enkripsi CBC dan C adalah himpunan cipherteks dan p panjang karakter dalam heksadesimal.
6. $\forall\, b \in$ K; $c \in$ IV akan dienkripsi menggunakan *Merkle-Hellman Knapsack*.
7. Panjang kunci dan IV dari CBC akan dipecah menjadi blok bit yang panjangnya sama dengan kunci publik. Selanjutnya $\forall\, b \in$ K; $c \in$ IV dikalikan dengan kunci publik.
8. Enkripsi kunci dan IV akan menghasilkan *cipherkey* yang akan diterima oleh penerima pesan.

4.1.2 Simulasi Algoritma Enkripsi Menggunakan Kriptografi Hibrida *Cipher Block Chaining (CBC)* dan *Merkle-Hellman Knapsack*

Berikut proses enkripsi CBC dan *Merkle-Hellman Knapsack* pada pesan teks sebagai berikut:

1. Pembangkitan kunci dilakukan dengan menentukan nilai barisan *superincreasing* (w), n, dan m secara acak. Di mana nilai $FPB(n, m) = 1$. Pada penelitian ini digunakan $w = \{2, 3, 6, 15,\ 27, 78, 131, 304\}$, $n = 97$, dan $m = 575$.
2. Melakukan pembangkitan kunci dengan persamaan $\beta_i = w_i \cdot n \bmod m$. Hasil dari perkalian akan menjadi kunci publik dan barisan *superincreasing* awal akan menjadi kunci privat.

   $\beta_i = w_i \cdot n \bmod m$

β_1 : $2 \cdot 97 \; mod \; 575 = 194$

β_2 : $3 \cdot 97 \; mod \; 575 = 291$

β_3 : $6 \cdot 97 \; mod \; 575 = 7$

β_4 : $15 \cdot 97 \; mod \; 575 = 305$

β_5 : $27 \cdot 97 \; mod \; 575 = 319$

β_6 : $78 \cdot 97 \; mod \; 575 = 91$

β_7 : $131 \cdot 97 \; mod \; 575 = 57$

β_8 : $304 \cdot 97 \; mod \; 575 = 163$

Jadi, kunci publiknya adalah $\{194, 291, 7, 305, 319, 91, 57, 163\}$, sedangkan kunci privatnya adalah $\{2, 3, 6, 15, \; 27, 78, 131, 304\}$.

3. Menentukan karakter alfabet yang akan digunakan sebagai plainteks. Pada penelitian ini, digunakan kalimat "JaLaN#GAjAyana#50" sebagai plainteksnya.

Tabel 4.1 Hasil Perubahan Karakter Plainteks Menjadi Biner Menggunakan Tabel ASCII

Plainteks	**Karakter**	**Biner**
P_1	J	01001010
P_2	a	01100001
P_3	L	01001100
P_4	a	01100001
P_5	N	01001110
P_6	#	00100011
P_7	G	01000111

P_8	A	01000001
P_9	j	01101010
P_{10}	A	01000001
P_{11}	y	01111001
P_{12}	a	01100001
P_{13}	n	01101110
P_{14}	a	01100001
P_{15}	#	00100011
P_{16}	5	00110101
P_{17}	0	00110000

4. Menentukan kunci CBC dan *Initialization Vector* yang akan menjadi C_0 secara acak.

   Tabel 4.2 Hasil Perubahan IV dan Kunci Menjadi Biner Menggunakan Tabel ASCII

Jenis	**Karakter**	**Biner**
Initialization Vector (C_0)	P	01010000
Kunci (K)	R	01010010

5. Melakukan proses enkripsi plainteks dengan CBC. Kunci dan *Initialization Vector* akan digunakan dalan proses ini. Adapun proses enkripsi sebagai berikut:

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

P_1 : 01001010

IV : 01010000 $\oplus$

00011010

K 01010010 $\oplus$

01001000

Geser 1-bit ke kiri: $C_1 = 10010000$

P_2 : 01100001

C_1 : 10010000 $\oplus$

11110001

K 01010010 $\oplus$

10100011

Geser 1-bit ke kiri: $C_2 = 01000111$

P_3 : 01001100

C_2 : 01000111 $\oplus$

00001011

K 01010010 $\oplus$

01011001

Geser 1-bit ke kiri: $C_3 = 10110010$

P_4 : 01100001

C_3 : 10110010 $\oplus$

11010011

K 01010010 $\oplus$

10000001

Geser 1-bit ke kiri: $C_4 = 00000011$

P_5 : 01001110

C_4 : 00000011 $\oplus$

01001101

K 01010010 $\oplus$

00011111

Geser 1-bit ke kiri: $C_5 = 00111110$

P_6 : 00100011

C_5 : 00111110 $\oplus$

00011101

K 01010010 $\oplus$

01001111

Geser 1-bit ke kiri: $C_6 = 10011110$

P_7 : 01000111

C_6 : 10011110 $\oplus$

11011001

K 01010010 $\oplus$

10001011

Geser 1-bit ke kiri: $C_7 = 00010111$

P_8 : 01000001

C_7 : 00010111 $\oplus$

01010110

K 01010010 $\oplus$

00000100

Geser 1-bit ke kiri: $C_8 = 00001000$

P_9 : 01101010

C_8 : 00001000 $\oplus$

01100010

K 01010010 $\oplus$

00110000

Geser 1-bit ke kiri: $C_9 = 01100000$

P_{10} : 01000001

C_9 : 01100000 $\oplus$

00100001

K 01010010 $\oplus$

01110011

Geser 1-bit ke kiri: $C_{10} = 11100110$

P_{11} : 01111001

C_{10} : 11100110 $\oplus$

10011111

K 01010010 $\oplus$

11001101

Geser 1-bit ke kiri: $C_{11} = 10011011$

P_{12} : 01100001

C_{11} : 10011011 $\oplus$

11111010

K 01010010 $\oplus$

10101000

Geser 1-bit ke kiri: $C_{12} = 01010001$

P_{13} : 01101110

C_{12} : 01010001 $\oplus$

00111111

K 01010010 $\oplus$

01101101

Geser 1-bit ke kiri: $C_{13} = 11011010$

P_{14} : 01100001

C_{13} : 11011010 $\oplus$

10111011

K 01010010 $\oplus$

11101001

Geser 1-bit ke kiri: $C_{14} = 11010011$

P_{15} : 00100011

C_{14} : 11010011 $\oplus$

11110000

K 01010010 $\oplus$

10100010

Geser 1-bit ke kiri: $C_{15} = 01000101$

P_{16} : 00110101

C_{15} : 01000101 $\oplus$

01110000

K 01010010 $\oplus$

00100010

Geser 1-bit ke kiri: $C_{16} = 01000100$

P_{17} : 00110000

C_{16} : 01000100 $\oplus$

01110100

K 01010010 $\oplus$

00100110

Geser 1-bit ke kiri: $C_{17} = 01001100$

6. Ubah hasil enkripsi pesan menjadi heksadesimal sehingga menghasilkan cipherteks yang akan diterima oleh penerima pesan.

Tabel 4.3 Hasil Enkripsi Plainteks Perubahan dari Biner ke Heksadesimal Menggunakan Tabel ASCII

	Biner	**Heksadesimal**
C_1	10010000	90
C_2	01000111	47
C_3	10110010	B2
C_4	00000011	03
C_5	00111110	3E
C_6	10011110	9E
C_7	00010111	17
C_8	00001000	08
C_9	01100000	60
C_{10}	11100110	E6
C_{11}	10011011	B5
C_{12}	01010001	1D
C_{13}	11011010	AD
C_{14}	11010011	34
C_{15}	01000101	54
C_{16}	01000100	44
C_{17}	01001100	4C

Hasil enkripsi plainteks adalah:

9047B2033E9E170860E69B51DAD345444C

Penggunaan heksadesimal disebabkan karena penulisan lebih praktis, mudah dibaca, dan memiliki kemungkinan timbul kesalahan yang lebih kecil. Selain itu, tidak digunakannya karakter ASCII sebagai hasil akhir

cipherteks karena tidak semua simbol karakter yang digunakan dapat dituliskan secara jelas.

7. Selanjutnya, akan dilakukan proses enkripsi kunci CBC dan *Initialization Vector* (IV) menggunakan *Merkle-Hellman Knapsack*. Hasil enkripsi disebut sebagai *cipherkey*. Berikut plainteks yang akan digunakan:

   Tabel 4.4 Plainteks IV dan Kunci CBC

			Plainteks
1.	*Initialization Vector*	:	01010000
2.	Kunci CBC	:	01010010

8. Plainteks dipecah menjadi blok bit yang panjangnya sama dengan barisan kunci publik. Mengalikan tiap bit di dalam blok dengan elemen di kunci publik.

   Plainteks 1 (IV) : 01010000

   Kunci publik : 194, 291, 7, 305, 319, 91, 57, 163

   Kriptogram : $(0 \times 194) + (1 \times 291) + (0 \times 7) + (1 \times 305) + (0 \times 319) + (0 \times 91) + (0 \times 57) + (0 \times 163) = 0 + 291 + 0 + 305 + 0 + 0 + 0 + 0 = 596$

   Plainteks 2 (Kunci) : 01010010

   Kunci publik : 194, 291, 7, 305, 319, 91, 57, 163

   Kriptogram : $(0 \times 194) + (1 \times 291) + (0 \times 7) + (1 \times 305) + (0 \times 319) + (0 \times 91) + (1 \times 57) +$

$$(0 \times 163) = 0 + 291 + 0 + 305 + 0 + 0 +$$

$$57 + 0 = 653$$

9. Mendapatkan *cipherkey* untuk IV yaitu 596 dan kunci, yaitu 653.

4.2 Proses Dekripsi Menggunakan Kriptografi Hibrida *Cipher Block Chaining (CBC)* dan *Merkle-Hellman Knapsack*

4.2.1 Algoritma Dekripsi Menggunakan Kriptografi Hibrida *Cipher Block Chaining (CBC)* dan *Merkle-Hellman Knapsack*

1. Mula-mula penerima melakukan proses dekripsi *cipherkey* menggunakan kunci publik dengan *Merkle-Hellman Knapsack* dengan menghitung n^{-1}, dengan persamaan $n \cdot n^{-1} \equiv 1(mod\ m)$.
2. Untuk setiap *cipherkey* akan dikalikan dengan $n^{-1}\ mod\ m$. Penerima pesan akan mendapatkan hasil dekripsi kunci dan IV CBC yang berupa bilangan biner.
3. Dekripsi cipherteks CBC dilakukan dengan mengubah bilangan heksadesimal menjadi biner, $\forall\ d_1, d_2, d_3, \dots, d_p \in C$ diubah menjadi biner. Selanjutnya, digunakan persamaan $P_i = D_k(C_i) \oplus C_{i-1}$ sehingga menghasilkan $a_1, a_2, a_3, \dots, a_k \in P$.
4. $\forall\ a_1, a_2, a_3, \dots, a_k \in P$ diubah menjadi karakter alfabet sehingga penerima mendapatkan plainteks awal yang sesuai dengan pesan yang dikirim oleh pengirim.

4.2.2 Simulasi Algoritma Dekripsi Menggunakan Kriptografi Hibrida *Cipher Block Chaining (CBC)* dan *Merkle-Hellman Knapsack*

Berikut proses dekripsi CBC dan *Merkle-Hellman Knapsack* pada pesan teks sebagai berikut:

1. Melakukan dekripsi *cipherkey* menggunakan kunci publik dengan *Merkle-Hellman Knapsack*. Mula-mula hitung n^{-1}, yaitu balikan dari $n \, mod \, m$. Akan digunakan persamaan:

   $n \cdot n^{-1} \equiv 1(mod\ m)$

   $97 \cdot n^{-1} \equiv 1(mod\ 575)$

   $n^{-1} \equiv \frac{1+575k}{97}, k = 0, 1, 2, 3, \ldots\ldots$

   $n^{-1} = \frac{1+14 \cdot 575}{97}$

   $n^{-1} = 83$

2. Mengalikan setiap kriptogram dengan $n^{-1} \, mod \, m$, lalu menyatakan hasil kalinya sebagai penjumlahan elemen-elemen kunci privat untuk memperoleh kunci dan IV asli menggunakan algoritma pencarian solusi *superincreasing knapsack*.

   Cipherkey 1 : 596

   (IV) $= 596 \cdot 83 \, mod \, 575 = 18$

   Bandingkan hasil dari perhitungan *cipherkey* 1 dengan bobot koresponden dimulai dari terbesar ke terkecil

   Koresponden : $2, 3, 6, 15, 27, 78, 131, 304$

   1. Bandingkan 18 dengan 304. Karena $304 > 18$, maka bernilai 0

2. Bandingkan 18 dengan 131. Karena $131 > 18$, maka bernilai 0
3. Bandingkan 18 dengan 78. Karena $78 > 18$, maka bernilai 0
4. Bandingkan 18 dengan 27. Karena $27 > 18$, maka bernilai 0
5. Bandingkan 18 dengan 15. Karena $15 \leq 18$, maka bernilai 1
6. Bobot total sekarang menjadi $18 - 15 = 3$. Bandingkan 3 dengan 6. Karena $6 > 3$, maka bernilai 0
7. Bandingkan 3 dengan 3. Karena $3 \leq 3$, maka bernilai 1
8. Bobot total sekarang menjadi $3 - 3 = 0$. Bandingkan 0 dengan 2. Karena $2 > 0$, maka bernilai 0

Sehingga dihasilkan biner = 01010000

Cipherkey 2 : 653

(Kunci) $= 653 \cdot 83 \; mod \; 575 = 149$

Bandingkan hasil dari perhitungan *cipherkey* 2 dengan bobot koresponden dimulai dari yang terbesar ke terkecil

Koresponden : $2, 3, 6, 15, 27, 78, 131, 304$

1. Bandingkan 149 dengan 304. Karena $304 > 149$, maka bernilai 0
2. Bandingkan 149 dengan 131. Karena $131 \leq 149$, maka bernilai 1
3. Bobot total sekarang menjadi $149 - 131 = 18$. Bandingkan 18 dengan 78. Karena $78 > 18$, maka bernilai 0
4. Bandingkan 18 dengan 27. Karena $27 > 18$, maka bernilai 0
5. Bandingkan 18 dengan 15. Karena $15 \leq 18$, maka bernilai 1
6. Bobot total sekarang menjadi $18 - 15 = 3$. Bandingkan 3 dengan 6. Karena $6 > 3$, maka bernilai 0

7. Bandingkan 3 dengan 3. Karena $3 \leq 3$, maka bernilai 1
8. Bobot total sekarang menjadi $3 - 3 = 0$. Bandingkan 0 dengan 2. Karena $2 > 0$, maka bernilai 0

Sehingga didapatkan biner = 01010010

3. Didapatkan hasil dekripsi IV yaitu 01010000 dan kunci CBC yaitu 01010010.
4. Melakukan dekripsi cipherteks menggunakan CBC. Mula-mula ubah cipherteks yang berupa bilangan heksadesimal menjadi bilangan biner.

Tabel 4.5 Hasil Perubahan Cipherteks Menjadi Biner Menjadi Biner Menggunakan Tabel ASCII

	Heksadesimal	**Biner**
C_1	90	10010000
C_2	47	01000111
C_3	B2	10110010
C_4	03	00000011
C_5	3E	00111110
C_6	9E	10011110
C_7	17	00010111
C_8	08	00001000
C_9	60	01100000
C_{10}	E6	11100110
C_{11}	B5	10011011
C_{12}	1D	01010001

C_{13}	AD	11011010
C_{14}	34	11010011
C_{15}	54	01000101
C_{16}	44	01000100
C_{17}	4C	01001100

5. Dekripsi pesan dilakukan dengan persamaan:

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

   C_1 : 10010000

   Geser 1-bit ke kanan: $C_1' = 01001000$

   C_1' : 01001000

   K : 01010010 $\oplus$

   00011010

   IV 01010000 $\oplus$

   P_1 : 01001010

   C_2 : 01000111

   Geser 1-bit ke kanan: $C_2' = 10100011$

   C_2' : 10100011

   K : 01010010 $\oplus$

   11110001

   C_1 10010000 $\oplus$

   P_2 : 01100001

C_3 : 10110010

Geser 1-bit ke kanan: $C_3' = 01011001$

C_3' : 01011001

K : 01010010 $\oplus$

00001011

C_2 01000111 $\oplus$

P_3 : 01001100

C_4 : 00000011

Geser 1-bit ke kanan: $C_4' = 10000001$

C_4' : 10000001

K : 01010010 $\oplus$

11010011

C_3 10110010 $\oplus$

P_4 : 01100001

C_5 : 00111110

Geser 1-bit ke kanan: $C_5' = 00011111$

C_5' : 00011111

K : 01010010 $\oplus$

01001101

C_4 00000011 $\oplus$

P_5 : 01001110

C_6 : 10011110

Geser 1-bit ke kanan: $C_6' = 01001111$

C_6' : 01001111

K : 01010010 $\oplus$

00011101

C_5 00111110 $\oplus$

P_6 : 00100011

C_7 : 00010111

Geser 1-bit ke kanan: $C_7' = 10001011$

C_7' : 10001011

K : 01010010 $\oplus$

11011001

C_6 10011110 $\oplus$

P_7 : 01000111

C_8 : 00001000

Geser 1-bit ke kanan: $C_8' = 00000100$

C_8' : 00000100

K : 01010010 $\oplus$

01010110

C_7 00010111 $\oplus$

P_8 : 01000001

C_9 : 01100000

Geser 1-bit ke kanan: $C_9' = 00110000$

C_9' : 00110000

K : 01010010 $\oplus$

01100010

C_8 00001000 $\oplus$

P_9 : 01101010

C_{10} : 11100110

Geser 1-bit ke kanan: $C_{10}' = 01110011$

C_{10}' : 01110011

K : 01010010 $\oplus$

00100001

C_9 01100000 $\oplus$

P_{10} : 01000001

C_{11} : 10011011

Geser 1-bit ke kanan: $C_{11}' = 11001101$

C_{11}' : 11001101

K : 01010010 $\oplus$

10011111

C_{10} 11100110 $\oplus$

P_{11} : 01111001

C_{12} : 01010001

Geser 1-bit ke kanan: $C'_{12} = 10101000$

$C_{12}{}'$: 10101000

K : 01010010 $\oplus$

11111010

C_{11} 10011011 $\oplus$

P_{12} : 01100001

C_{13} : 11011010

Geser 1-bit ke kanan: $C'_{13} = 01101101$

$C_{13}{}'$: 01101101

K : 01010010 $\oplus$

00111111

C_{12} 01010001 $\oplus$

P_{13} : 01101110

C_{14} : 11010011

Geser 1-bit ke kanan: $C'_{14} = 11101001$

$C_{14}{}'$: 11101001

K : 01010010 $\oplus$

10111011

C_{13} 11011010 $\oplus$

P_{14} : 01100001

C_{15} : 01000101

Geser 1-bit ke kanan: $C'_{15} = 10100010$

C_{15}' : 10100010

K : 01010010 $\oplus$

11110000

C_{14} 11010011 $\oplus$

P_{15} : 00100011

C_{16} : 01000100

Geser 1-bit ke kanan: $C'_{16} = 00100010$

C_{16}' : 00100010

K : 01010010 $\oplus$

01110000

C_{15} 01000101 $\oplus$

P_{16} : 00110101

C_{17} : 01001100

Geser 1-bit ke kanan: $C'_{17} = 00100110$

C_{17}' : 00100110

K : 01010010 $\oplus$

01110100

C_{16} 01000100 $\oplus$

P_{17} : 00110000

Hasil dekripsi cipherteks adalah:

01001010 01100001 01001100 01100001 01001110 00100011 01000111 01000001 01101010 01000001 01111001 01100001 01101110 01100001 00100011 00110101 00110000

6. Mengubah biner menjadi alfabet menggunakan tabel ASCII

Tabel 4.6 Hasil dekripsi cipherteks menggunakan CBC

Plainteks	**Biner**	**Karakter**
P_1	01001010	J
P_2	01100001	a
P_3	01001100	L
P_4	01100001	a
P_5	01001110	N
P_6	00100011	#
P_7	01000111	G
P_8	01000001	A
P_9	01101010	j
P_{10}	01000001	A
P_{11}	01111001	y
P_{12}	01100001	a
P_{13}	01101110	n
P_{14}	01100001	a
P_{15}	00100011	#

P_{16}	00110101	5
P_{17}	00110000	0

7. Mendapatkan plainteks, yaitu “JaLaN#GAjAyana#50”.

4.3 Kajian Nilai-Nilai Agama dengan Hasil Penelitian

Seiring berkembangnya teknologi yang pesat, penyandian pesan sangat diperlukan untuk meminimalisir pesan diakses atau diketahui oleh pihak yang tidak bertanggung jawab. Menjaga kerahasiaan pesan termasuk dalam amanah yang harus dijaga dengan sebaik-baiknya. Amanah adalah salah satu sifat mulia yang harus dimiliki oleh setiap manusia sebagai bentuk tanggung jawabnya terhadap sesama makhluk ataupun pencipta, sebagaimana dalam al-Quran surat An-Nisa’ ayat 58 bahwa setiap orang yang diberi amanah wajib untuk menyampaikan kepada yang berhak, selain itu diriwayatkan oleh Ahmad bin Hambal “tidak sempurna iman seseorang yang tidak amanah, dan tidak sempurna agama orang yang tidak menunaikan janji”. Hadits ini memberikan penegasan bahwa amanah dapat menjadi indikator dari kekuatan iman seseorang, karena orang yang beriman akan menjaga amanah sebaik-baiknya.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan yang dilakukan di atas, maka dapatkan kesimpulan sebagai berikut:

1. Terdapat dua proses enkripsi pesan menggunakan kriptografi hibrida CBC dan *Merkle-Hellman Knapsack*, yaitu enkripsi plainteks menggunakan CBC dan enkripsi IV dan kunci CBC menggunakan *Merkle-Hellman Knapsack*. Dalam proses enkripsi plainteks, digunakan persamaan $C_i = E_K(P_i \oplus C_{i-1})$. Selanjutnya pada proses enkripsi IV dan kunci CBC menggunakan M*erkle-Hellman Knapsack*. Pertama, menentukan barisan *superincreasing* yang nantinya akan menjadi kunci privat, nilai n, dan m secara acak. Melakukan pembangkitan kunci dengan persamaan $\beta_i = w_i \cdot n \ mod \ m$. Hasil dari perkalian akan menjadi kunci publik. Kemudian, IV dan kunci CBC dipecah menjadi blok bit yang panjangnya sama dengan barisan kunci publik. Mengalikan tiap bit di dalam blok dengan elemen di kunci publik. Tahap ini akan menghasilkan *cipherkey* yang akan dikirim kepada penerima pesan.
2. Pada proses dekripsi, pertama-tama dilakukan dekripsi terhadap cipherkey dengan *Merkle-Hellman Knapsack* dalam tahap ini akan dilakukan pencarian n^{-1} menggunakan persamaan $n \cdot n^{-1} \equiv 1(mod \ m)$. Setelah mendapatkan n^{-1} masing-masing kriptogram akan dikalikan dengan persamaan $n^{-1} \ mod \ m$. Didapatkan kembali IV dan kunci CBC. Selanjutnya, dekripsi

cipherteks menggunakan persamaan $P_i = D_k(C_i) \oplus C_{i-1}$. Dengan demikian, penerima pesan dapat mengetahui isi dari plainteks.

5.2 Saran

Penelitian ini membahas mengenai pengamanan pesan teks menggunakan kriptografi hibrida CBC dan *Merkle-Hellman Knapsack*. Untuk penelitian selanjutnya disarankan untuk menambahkan karakter baru dan menggunakan nilai pada barisan *superincreasing* yang lebih tinggi pada proses enkripsi dan dekripsi, serta menggunakan kunci dan IV yang lebih panjang. Selain itu, penelitian selanjutnya diharapkan dapat menggunakan kombinasi lain untuk metode kriptografi hibrida.

DAFTAR PUSTAKA

Al-Hikmah, D. A. (2011). *Al-Qur'an dan Terjemahnya.* Bandung: Diponegoro.

Ariyus, D. (2006). *Kriptografi: Keamanan Data dan Komunikasi.* Yogyakarta: Graha Ilmu.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi.* Yogyakarta: Penerbit ANDI.

az-Zuhaili, P. D. (2013). *Tafsir Al-Munir: Akidah, Syariah, & Manhaj Jilid 2.* Depok: Gema Insan.

Hermawan, I., Ahmad, N., & Suhartini, A. (2020). Konsep Amanah dalam Perspektif Pendidikan Islam. *Qalamuna - Jurnal Pendidikan, Sosial, dan Agama*, 141-152.

Hidayat, A., Akmal, & Rosyadi, R. (2016). Cryptography Asymmetris Merkle-Hellman Knapsack Digunakan untuk Enkripsi dan Dekripsi Teks. *Prosiding Seminar Nasional MIPA 2016*, 66-68.

Hidayat, A., Rosyadi, R., & Paulus, E. (2016). Aplikasi Merkle-Hellman Knapsack untuk Kriptografi File Teks. *SENTER 2016: Seminar Nasional Teknik Elektro 2016*, 194-200.

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

Munir, R. (2016). *Matematika Diskrit.* Bandung: Informatika Bandung.

Munir, R. (2019). *Kriptografi.* Bandung: Informatika Bandung.

Pustaka, P. I. (2013). *Kitab Al-Qur'an Al-Fatih dengan Alat Peraga Tajwid Kode Arab.* Tangerang Selatan: Al-Fatih Berkah Cipta.

Rosmala, D., & Aprian, R. (2012). Implementasi Mode Operasi Cipher Block Chaining (CBC) pada Pengamanan Data. *Jurnal Infromatika*, 55-65.

Sadikin, A. (2012). *Kriptografi untuk Keamanan Jaringan.* Yogyakarta: Penerbit ANDI.

Sidik, A. P., & Mayasari, N. (2019). Rancangan Model Algoritma Hybrid Teknik Enkripsi XOR dengan Kombinasi Mode Block Cipher CBC - ECB 512-Bits dan Algoritma RSA. *Teknik dan Informatika*, 1-7.

Sukamto, R. A. (2010). *Algoritma dan Pemograman* . Bogor: Program Ilmu Komputer Universitas Pendidikan Indonesia.

Sulaiman, O. K. (2019). Hybrid Cryptosystem Menggunakan XOR Cipher dan Merkle-Hellman Knapsack untuk Menjaga Kerahasiaan Pesan Digital. *Teknologi Informasi*, 169-173.

Wildan Mahmud, E. M. (2020). Pengamanan Data Kombinasi Metode Cipher Block Chaining dan Modifikasi LSB. *Techno.COM*, 97-102.

LAMPIRAN

Lampiran I Tabel Kode ASCII

Desimal	Biner	Hexadesimal	Karakter
0	00000000	00	NUL
1	00000001	01	SOH
2	00000010	02	STX
3	00000011	03	ETX
4	00000100	04	EOT
5	00000101	05	ENQ
6	00000110	06	ACK
7	00000111	07	BEL
8	00001000	08	BES
9	00001001	09	HT
10	00001010	0A	LF
11	00001011	0B	VT
12	00001100	0C	FF
13	00001101	0D	CR
14	00001110	0E	SO
15	00001111	0F	SI
16	00010000	10	DLE
17	00010001	11	DC1
18	00010010	12	DC2
19	00010011	13	DC3
20	00010100	14	DC4
21	00010101	15	NAK
22	00010110	16	SYN
23	00010111	17	ETB
24	00011000	18	CAN
25	00011001	19	EM

26	00011010	1A	SUB
27	00011011	1B	ESC
28	00011100	1C	FS
29	00011101	1D	GS
30	00011110	1E	RS
31	00011111	1F	US
32	00100000	20	*(Space)*
33	00100001	21	!
34	00100010	22	"
35	00100011	23	#
36	00100100	24	$
37	00100101	25	%
38	00100110	26	&
39	00100111	27	'
40	00101000	28	(
41	00101001	29	)
42	00101010	2A	*
43	00101011	2B	+
44	00101100	2C	,
45	00101101	2D	-
46	00101110	2E	.
47	00101111	2F	/
48	00110000	30	0
49	00110001	31	1
50	00110010	32	2
51	00110011	33	3
52	00110100	34	4
53	00110101	35	5
54	00110110	36	6

55	00110111	37	7
56	00111000	38	8
57	00111001	39	9
58	00111010	3A	:
59	00111011	3B	;
60	00111100	3C	<
61	00111101	3D	=
62	00111110	3E	>
63	00111111	3F	?
64	01000000	40	@
65	01000001	41	A
66	01000010	42	B
67	01000011	43	C
68	01000100	44	D
69	01000101	45	E
70	01000110	46	F
71	01000111	47	G
72	01001000	48	H
73	01001001	49	I
74	01001010	4A	J
75	01001011	4B	K
76	01001100	4C	L
77	01001101	4D	M
78	01001110	4E	N
79	01001111	4F	O
80	01010000	50	P
81	01010001	51	Q
82	01010010	52	R
83	01010011	53	S

84	01010100	54	T
85	01010101	55	U
86	01010110	56	V
87	01010111	57	W
88	01011000	58	X
89	01011001	59	Y
90	01011010	5A	Z
91	01011011	5B	[
92	01011100	5C	\
93	01011101	5D	]
94	01011110	5E	^
95	01011111	5F	_
96	01100000	60	`
97	01100001	61	a
98	01100010	62	b
99	01100011	63	c
100	01100100	64	d
101	01100101	65	e
102	01100110	66	f
103	01100111	67	g
104	01101000	68	h
105	01101001	69	i
106	01101010	6A	j
107	01101011	6B	k
108	01101100	6C	l
109	01101101	6D	m
110	01101110	6E	n
111	01101111	6F	o
112	01110000	70	p

113	01110001	71	q
114	01110010	72	r
115	01110011	73	s
116	01110100	74	t
117	01110101	75	u
118	01110110	76	v
119	01110111	77	w
120	01111000	78	x
121	01111001	79	y
122	01111010	7A	z
123	01111011	7B	{
124	01111100	7C	|
125	01111101	7D	}
126	01111110	7E	~
127	01111111	7F	DEL
128	10000000	80	Ç
129	10000001	81	ü
130	10000010	82	é
131	10000011	83	â
132	10000100	84	ä
133	10000101	85	à
134	10000110	86	å
135	10000111	87	ç
136	10001000	88	ê
137	10001001	89	ë
138	10001010	8A	è
139	10001011	8B	ï
140	10001100	8C	î
141	10001101	8D	ì

142	10001110	8E	Ä
143	10001111	8F	Å
144	10010000	90	É
145	10010001	91	æ
146	10010010	92	Æ
147	10010011	93	ô
148	10010100	94	ö
149	10010101	95	ò
150	10010110	96	û
151	10010111	97	ù
152	10011000	98	ÿ
153	10011001	99	Ö
154	10011010	9A	Ü
155	10011011	9B	ø
156	10011100	9C	£
157	10011101	9D	Ø
158	10011110	9E	×
159	10011111	9F	*ƒ*
160	10100000	A0	á
161	10100001	A1	í
162	10100010	A2	ó
163	10100011	A3	ú
164	10100100	A4	ñ
165	10100101	A5	Ñ
166	10100110	A6	ª
167	10100111	A7	º
168	10101000	A8	¿
169	10101001	A9	®
170	10101010	AA	¬

171	10101011	AB	½
172	10101100	AC	¼
173	10101101	AD	¡
174	10101110	AE	«
175	10101111	AF	»
176	10110000	B0	░
177	10110001	B1	▒
178	10110010	B2	▓
179	10110011	B3	│
180	10110100	B4	┤
181	10110101	B5	Á
182	10110110	B6	Â
183	10110111	B7	À
184	10111000	B8	©
185	10111001	B9	╣
186	10111010	BA	║
187	10111011	BB	╗
188	10111100	BC	╝
189	10111101	BD	¢
190	10111110	BE	¥
191	10111111	BF	┐
192	11000000	C0	└
193	11000001	C1	┴
194	11000010	C2	┬
195	11000011	C3	├
196	11000100	C4	─
197	11000101	C5	┼
198	11000110	C6	ã
199	11000111	C7	Ã

200	11001000	C8	╚
201	11001001	C9	╔
202	11001010	CA	╩
203	11001011	CB	╦
204	11001100	CC	╠
205	11001101	CD	═
206	11001110	CE	╬
207	11001111	CF	¤
208	11010000	D0	ð
209	11010001	D1	Ð
210	11010010	D2	Ê
211	11010011	D3	Ë
212	11010100	D4	È
213	11010101	D5	ı
214	11010110	D6	Í
215	11010111	D7	Î
216	11011000	D8	Ï
217	11011001	D9	┘
218	11011010	DA	┌
219	11011011	DB	█
220	11011100	DC	▄
221	11011101	DD	¦
222	11011110	DE	Ì
223	11011111	DF	▀
224	11100000	E0	Ó
225	11100001	E1	ß
226	11100010	E2	Ô
227	11100011	E3	Ò
228	11100100	E4	õ

229	11100101	E5	Õ
230	11100110	E6	µ
231	11100111	E7	þ
232	11101000	E8	Þ
233	11101001	E9	Ú
234	11101010	EA	Û
235	11101011	EB	Ù
236	11101100	EC	ý
237	11101101	ED	Ý
238	11101110	EE	¯
239	11101111	EF	´
240	11110000	F0	≡
241	11110001	F1	±
242	11110010	F2	‗
243	11110011	F3	¾
244	11110100	F4	¶
245	11110101	F5	§
246	11110110	F6	÷
247	11110111	F7	¸
248	11111000	F8	°
249	11111001	F9	¨
250	11111010	FA	·
251	11111011	FB	¹
252	11111100	FC	³
253	11111101	FD	²
254	11111110	FE	■
255	11111111	FF	nbsp

RIWAYAT HIDUP

Chofifah Alfin Novianti, dilahirkan di Kabupaten Banyuwangi pada tanggal 01 November 1999, biasa dipanggil Novi. Penulis tinggal di Perum. Asrikaton Indah, Kecamatan Pakis, Kabupaten Malang. Merupakan putri kedua dari pasangan Bapak Imam Kambali dan Ibu Jamiah Rehani, serta memiliki satu kakak perempuan dan adik laki-laki.

Pendidikan dasar ditempuh di SDN 03 Rejoagung (2006-2012), kemudian melanjutkan pendidikan menengah pertama di SMP Bustanul Makmur (2012-2015), kemudian pendidikan menengah atas di SMAN Taruna Nala Jawa Timur dan lulus pada tahun 2018. Pada tahun yang sama penulis menempuh kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil program studi matematika.

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 : Chofifah Alfin Novianti
NIM : 18610057
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Pengamanan Pesan Teks Menggunakan Kriptografi Hibrida *Cipher Block Chaining* (CBC) dan *Merkle-Hellman Knapsack*
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Muhammad Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1.	21 Maret 2022	Konsultasi BAB 1	1.
2.	28 April 2022	Konsultasi Kajian Agama	2.
3.	14 Juni 2022	Konsultasi BAB 2 dan 3	3.
4.	22 Juni 2022	Revisi Kajian Agama	4.
5.	8 September 2022	Revisi BAB 2 dan 3	5.
6.	20 Desember 2022	ACC BAB 1,2 dan 3	6.
7.	07 Februari 2023	Revisi Seminar Proposal	7.
8.	07 April 2023	Konsultasi BAB 4 dan 5	8.
9.	18 April 2023	Konsultasi Kajian Agama	9.
10.	23 Mei 2023	ACC BAB 4 dan 5	10.
11.	05 Juni 2023	Revisi Seminar Hasil	11.
12.	19 Juni 2023	Konsultasi Keseluruhan	12.
13.	23 Juni 2023	ACC Keseluruhan	13.

Malang, 26 Juni 2023
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP.19741129200012200 5