IMPLEMENTASI AFFINE CIPHER DAN ALGORITMA GOLDBACH CODE DALAM MENGAMANKAN PESAN TEKS

SKRIPSI

OLEH:
RAFIKA ZAHROTUL FAUZIAH
NIM. 19610014

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

IMPLEMENTASI AFFINE CIPHER DAN ALGORITMA GOLDBACH CODE DALAM MENGAMANKAN PESAN TEKS

SKRIPSI

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

Oleh
Rafika Zahrotul Fauziah
NIM. 19610014

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

IMPLEMENTASI AFFINE CIPHER DAN ALGORITMA GOLDBACH CODE DALAM MENGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Rafika Zahrotul Fauziah
NIM. 19610014

Telah Disetujui Untuk Diuji

Malang, 21 Desember 2023

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si	Erna Herawati, M.Pd
NIP. 19900511 202321 1 029	NIDT. 19760723 20180201 2 222

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 197411292000122005

IMPLEMENTASI AFFINE CIPHER DAN ALGORITMA GOLDBACH CODE DALAM MENGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Rafika Zahrotul Fauziah
NIM. 19610014

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat.)

Tanggal, 26 Desember 2023

Ketua Penguji	: Evawati Alisah, M.Pd.	.....
Anggota Penguji 1	: Hisyam Fahmi, M.Kom	.....
Anggota Penguji 2	: Muhammad Khudzaifah, M.Si.	.....
Anggota Penguji 3	: Erna Herawati, M.Pd.	.....

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	: Rafika Zahrotul Fauziah
NIM	: 19610014
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Implementasi Affine Cipher dan Algoritma Goldbach Code dalam Mengamankan Pesan Teks

Menyatakan dengan sebenar-benarnya 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 dan 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, 26 Desember 2023
Yang membuat pernyataan,

Rafika Zahrotul Fauziah
NIM. 19610014

MOTO

"Hidup adalah permainan. Jadi jangan kalah dengan permainan yang telah diciptakan."

(Valerie Patkar- Game Over)

PERSEMBAHAN

Skripsi ini, penulis persembahkan untuk yang tersayang Ayahanda Amin dan Ibunda Nur Kholidah, Kakak Afin Baihaqi Asror dan Windy Dwi Yulitha, serta Adik penulis Cahaya Fatiha Mughnia yang senantiasa memberikan do'a, semangat, motivasi, juga dukungan moril maupun materiil serta kasih sayang yang sangat tidak terhingga kepada penulis.

Saudara dan sahabat penulis, Putri Aprilia, Galuh Farahita Al-Zunaidi, Ni Luh Ayu Linda Diana Sari, Setya Dandy Lesmana, dan juga Bayu Satrio Wibowo yang telah senantiasa menemani penulis hingga penulis dapat menyelesaikan skripsi ini.

Kepada Gulf Kanawut Traipipattanapong yang telah membuat penulis termotivasi untuk segera menyelesaikan penulisan dan penyusunan skripsi.

Dan yang terakhir untuk diri penulis sendiri, Rafika Zahrotul Fauziah yang telah berjuang melawan segala overthinking dan kemalasan untuk segera menuntaskan apa yang telah dimulai dengan semaksimal mungkin.

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas rahmat, hidayah, dan taufiq-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi dengan judul "Implementasi Affine Cipher dan Algoritma Goldbach Code dalam Mengamankan Pesan Teks" yang merupakan salah satu syarat untuk memperoleh gelar sarjana matematika di Fakultas Sains da Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Penulis mendapat banyak nasihat dan instruksi dari beberapa orang selama proses berlangsung.

Sehingga ucapan terima kasih penulis sampaikan kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Prof. Dr. H. Sri Harini, M.Si., selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc., selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Kudzaifah, M.Si., selaku dosen pembimbing I yang telah memberikan penulis motivasi serta dukungan.
5. Erna Herawati, M.Pd., selaku dosen pembimbing II yang senantiasa memberikan penulis arahan.
6. Evawati Alisah, M.Pd., selaku ketua penguji yang senantiasa memberikan arahan dan juga kritik dan saran yang membangun kepada penulis.
7. Hisyam Fahmi, M. Kom., selaku dosen penguji yang senantiasa memberikan arahan dan juga kritik dan saran yang membangun kepada penulis.
8. Prof. Dr. H. Sri Harini, M.Si., selaku dosen wali yang telah memberikan arahan dan motivasi kepada penulis.
9. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim.
10. Ayahanda Amin, Ibunda Nur Kholidah dan seluruh keluarga besar yang selalu memberikan do'a, semangat, dan motivasi kepada penulis hingga saat ini.
11. Putri Aprilia, Galuh, Dandy, Bayu, Novi, Kania, Maulida, Dila, Aza, Riris, Hilda, Izzah, Puan, yang senantiasa memberikan dukungan moril bagi penulis.

12. Rafika Zahrotul Fauziah, yang telah bekerja secara keras agar dapat menyelesaikan penulisan dan penyusunan skripsi ini.
13. Seluruh mahasiswa Matematika angkatan 2019 yang telah berjuang bersama.

Malang, 26 Desember 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SIMBOL

C	=	Cipherteks
P	=	Plainteks
m	=	Kunci Multiplikatif
m^{-1}	=	Balikan Kunci Multiplikatif
b	=	Pergeseran
n	=	Ukuran Alfabet

DAFTAR LAMPIRAN

ABSTRAK

Fauziah, Rafika Zahrotul. 2023. **Implementasi Affine Cipher dan Algoritma Goldbach Code dalam Mengamankan Pesan Teks**. Skripsi. Program Studi Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M. Si. (II) Erna Herawati, M. Pd.

Kata kunci: Affine Cipher, Goldbach Code, Algoritma Kompresi.

Perkembangan informasi saat ini memiliki dampak negatif juga positif. Untuk menanggulangi adanya dampak negatif, diperlukan adanya kriptografi. Hal ini bertujuan agar keamanan pesan teks terjaga. Affine Cipher merupakan salah satu algoritma kriptografi simetris yang menggunakan (m) sebagai kunci multiplikatif dan (b) sebagai jumlah pergeseran pada saat proses enkripsi. Pada saat proses dekripsi menggunakan balikan dari kunci multiplikatif (m-1). Goldbach Code diasumsikan bahwa setiap bilangan bulat genap yang lebih besar dari empat merupakan penjumlahan dari dua bilangan prima. Penelitian ini memiliki dua tahapan, yaitu: proses enkripsi dan dekripsi. Pada penelitian ini, proses yang akan dilakukan bertujuan untuk mengamankan pesan teks yang diawali dengan mengenkripsikannya menggunakan Affine Cipher dan setelahnya akan dikompresi dengan menggunakan Algoritma Goldbach Code untuk menghasilkan cipherteks. Kemudian untuk mengembalikan pesan akan didekompresi dengan menggunakan Algoritma Goldbach Code dan dekripsi dengan menggunakan Affine Cipher. Dengan menggabungkan Affine Cipher dan Algoritma Goldbach code hasil dari proses pengamanan pesan teks akan lebih aman dikarenakan cipherteks yang dihasilkan memiliki panjang bit yang berbeda.

ABSTRACT

Fauziah, Rafika Zahrotul. 2023. Implementation of Affine Cipher and Goldbach Code Algorithms in Securing Text Messages. Thesis. Department of Mathematics, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisors: (I) Muhammad Khudzaifah, M. Si. (II) Erna Herawati, M. Pd.

Keywords: Affine Cipher, Goldbach Code, Compression Algorithm.

The development of information today has both negative and positive impacts. To overcome the negative impact, cryptography is needed. This aims to maintain the security of text messages. Affine Cipher is a symmetric cryptography algorithm that uses (m) as the multiplicative key and (b) as the number of shifts during the encryption process. The decryption process uses the reciprocal of the multiplicative key (m-1). Goldbach Code assumes that every even integer greater than four is the sum of two prime numbers. This research has two stages, namely: encryption and decryption process. In this research, the process that will be carried out aims to secure text messages that begin by encrypting them using Affine Cipher and afterwards will be compressed using the Goldbach Code Algorithm to produce ciphertext. Then to restore the message, it will be decompressed using the Goldbach Code Algorithm and decrypted using Affine Cipher. By combining Affine Cipher and Goldbach Code Algorithm, the result of the text message security process will be more secure because the resulting ciphertext has a different bit length.

مستخلص البحث

فوزية، رفيقة زهرول. 2023. تنفيذ خوارزميات Affine Cipher و Goldbach Code في تأمين الرسائل النصية. بحث جامعي. قسم الرياضيات، كلية العلوم والتكنولوجيا ، جامعة مولانا مالك إبراهيم الإسلامية الحكومية، مالانج. المشرف: (I) محمد خذيفة، الماجستير. (II) إرنا هيراواتي، الماجستير.

الكلمات المفتاحية: التشفير الأفيني، كود جولدباخ، خوارزمية الضغط.

تطوير المعلومات الحالية له تأثير سلبي وكذلك إيجابي. للتغلب على التأثير السلبي ، هناك حاجة إلى التشفير. وذلك حتى يتم الحفاظ على أمان الرسائل النصية. أفين سيفر هي خوارزمية تشفير متماثلة تستخدم $(\mathbf{m})$ كمفتاح مضاعف و $(\mathbf{b})$ كعدد من التحولات خلال عملية التشفير. في وقت عملية فك التشفير استخدام التبادلية للمفتاح المضاعف $(\mathbf{m^{-1}})$. يفترض كود غولدباخ أن أي عدد صحيح زوجي أكبر من أربعة هو مجموع عددين أوليين. لهذا البحث مرحلتان: عملية التشفير وفك التشفير. في هذه الدراسة، تهدف العملية التي سيتم تنفيذها إلى تأمين الرسائل النصية التي تبدأ من خلال تشفيرها باستخدام أفين شيفير وبعد ذلك سيتم ضغطها باستخدام خوارزمية كود غولدباخ لإنتاج النص المشفر. ثم لإعادة الرسالة سيتم فك ضغطها باستخدام خوارزمية كود غولدباخ وفك تشفيرها باستخدام أفين شيفرة. من خلال الجمع بين شيفرة أفين ورمز خوارزمية غولدباخ، ستكون نتائج عملية أمان الرسالة النصية أكثر أمانًا لأن النص المشفر الناتج له طول بت مختلف.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini berdampak besar pada semua aspek kehidupan masyarakat, termasuk komunikasi. Dengan adanya teknologi internet dapat membantu manusia dalam berkomunikasi dengan cepat dan mudah. Dengan kemudahan ini, kebutuhan terhadap teknologi informasi dan komunikasi merupakan hal yang sangatlah penting. Pertukaran informasi dapat menimbulkan dampak positif maupun negatif. Kemajuan teknologi dalam pertukaran informasi atau pesan, dapat menyebar ke berbagai daerah dengan sangat cepat. Tetapi dibalik banyaknya dampak positif yang diterima, tidak dipungkiri bahwa dampak negatif tetap ada. Dampak negatif yang dapat ditimbulkan dikarenakan kurangnya keamanan dalam penggunaan dan juga pencegahannya. Banyak kejahatan-kejahatan yang berawal dari internet yang mengakibatkan pengguna internet merasa tidak aman dalam mengirimkan pesan. Sehingga diperlukan adanya pengamanan terhadap pesan yang kita kiriman. Pengamanan merupakan sebuah tindakan yang ditujukan untuk melindungi sesuatu dari segala acam gangguan dan keamanan.

Sehingga solusi yang dapat diambil untuk mengatasi permasalahan tersebut adalah dengan kriptografi. Kriptografi sendiri bertujuan untuk menyembunyikan suatu informasi dari individu yang tidak berwenang dengan pengubahan pesan asli menjadi pesan yang tidak bermakna. Enkripsi dan dekripsi adalah dua proses dari kriptografi. Enkripsi adalah proses memodifikasi informasi yang sebelumnya dapat dibaca dengan mudah kemudian diubah dengan menggunakan suatu algoritma sehingga tidak dapat dibaca oleh siapapun. Sementara dekripsi adalah teknik

membuat data yang tidak dapat dibaca menjadi bentuk yang dapat dibaca, dekripsi adalah kebalikan dari enkripsi (Kester, 2021). Dengan pemahaman terhadap ilmu kriptografi, dampak yang ditimbulkan dapat diminimalisir. Terdapat 3 jenis kriptografi: kriptografi simetris, kriptografi asimetris, dan *hybrid*.

Algoritma yang dikenal sebagai kriptografi simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi. Dalam kriptografi simetris, pengirim dan penerima harus berbagi kunci yang sama sebelum mengirim dan menerima pesan agar penerima dapat mendekripsi pesan yang diterimanya. Caesar Cipher, Vigenere Cipher, Affine Cipher merupakan contoh dari kriptografi simetris. Sedangkan dalam kriptografi asimetris, kunci yang berbeda digunakan untuk enkripsi dan dekripsi. Teknik kriptografi ini antara lain RSA, Elgamal, Diffie-Hellman, dan lain-lain. Penggabungan dari kriptografi simetris dan asimetris dikenal sebagai kriptografi *hybrid*.

Penelitian yang dilakukan oleh Ahmad Suhendri, dkk (2018) yang membahas tentang Affine Cipher dan one-time pad adalah algoritma kriptografi lama. Sebagai kriptografi kunci simetris, metode Affine Cipher sendiri harus memiliki kunci yang sama yang digunakan untuk ekripsi dan dekripsi. Sebaliknya, algoritma one-time pad menggunakan sekumpulan karakter kunci yang dibuat secara acak. Menggabungkan dua metode ini membutuhkan banyak waktu, tetapi tujuan dari kombinasi ini adalah untuk membuat keamanan yang diperoleh sulit diretas oleh kriptanalis. Kombinasi ini dibagi menjadi beberapa tahap, affne cipher berperan mengenkripsi plainteks pada tahap pertama, dan one-time pad berperan sebagai enkripsi tahap kedua. Selain digunakan dalam proses enkripsi, metode one-

time pad juga digunakan untuk mendekripsi cipherteks yang dihasilkan oleh one-time pad, yang kemudian didekripsi kembali dengan menggunakan Affine Cipher.

Penelitian yang dilakukan oleh Muhammad Rio Irliansyah, dkk (2017) pada penelitian ini membahas mengenai metode deflate dari kompresi file teks. Teknik LZ77 dan algoritma Huffman yang digabungkan dalam metode Deflate. Cara kerjanya dengan menghilangkan string kembar (implementasi algoritma LZ77) dan membaca hasil dari setiap blok yang akan diproses. Output yang dihasilkan kemudian dikompresi kembali menggunakan Algoritma Golbach Code. Algoritma Goldbach Code sendiri mempunyai konsep kerja yaitu menghitung jumlah frekuensi yang terbesar sampai terkecil, kemudian mencari *codeword* dengan menyandikan bilangan bulat positif n, yang diubah menjadi biangan bulat positif genap dengan rumus $(2n + 3)$. Sehingga menghasilkan ukuran file lebih kecil dari sebelum proses kompresi.

Keamanan dan penggunaannya memiliki banyak aspek, mulai dari perdagangan dan pembayaran yang aman hingga informasi pribadi dan perlindungan kata sandi (Nasution et al., 2017). Bahkan keamanan data privasi telah ditegaskan dalam Al-Qur'an sebagaimana firman Allah SWT dalam QS. An-Nuur ayat 27 yang artinya:

> *"Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat."*

Berdasarkan terjemahan ayat tersebut meskipun tidak dijelaskan secara detail mengenai keamanan data, namun ayat tersebut memiliki arti penting bagi orang yang diperintahkan untuk memberi salam dan meminta izin sebelum memasuki rumah seseorang. Dengan demikian Allah SWT berfirman dalam surat

An-Nuur tentang perlindungan terhadap pergaulan. Hal ini sama halnya dengan perlindungan data pribadi yang hanya dapat diakses dengan izin dari yang bersangkutan.

Pada penelitian ini, metode kriptografi yang digunakan yaitu kriptografi simetris Affine Cipher dan Algoritma Goldach Code. Penggunaan Affine Cipher ini dikarenakan hasil dari proses enkripsi dan dekripsinya lebih cepat dibandingkan dengan menggunakan kriptografi simetris lainnya. Affine Cipher sendiri mempunyai dua kunci yang berbeda yang digunakan dalam prosesnya. Tetapi, Affine Cipher memiliki kelemahan yaitu kunci yang digunakan. Sedangkan dengan menambahkan Algoritma Goldbach Code diharapkan dapat meminimalisir adanya kebocoran yang terjadi saat proses pengiriman pesan teks.

Berdasarkan pada uraian di atas, penulis tertarik untuk membuat judul penelitian "Implementasi Affine Cipher dan Algoritma Goldbach Code dalam Mengamankan Pesan Teks."

1.2 Rumusan Masalah

Dari latar belakang di atas, didapatkan rumusan masalah seperti berikut:

1. Bagaimana cara kerja Affine Cipher dalam mengenkripsi pesan teks dan Algoritma Goldbach Code dalam mengompresi pesan teks?
2. Bagaimana cara kerja Affine Cipher dalam mendekripsi pesan teks dan Algoritma Goldbach Code dalam dekompresi pesan teks?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka ditetapkan tujuan penelitian sebagai berikut:

1. Mengetahui penggunaan Affine Cipher untuk mengenkripsi pesan teks dan Algoritma Goldbach Code untuk mengompresi pesan teks.
2. Mengetahui penggunaan Algoritma Goldbach Code untuk dekompresi pesan teks dan Affine Cipher untuk dekripsi pesan teks.

1.4 Manfaat Penelitian

Berdasarkan pada tujuan penelitian di atas, manfaat yang didapatkan bagi siapapun khususnya bagi pembaca dan penulis sebagai berikut:

1. Bagi penulis

   Dapat mengetahui cara pengamanan pesan dengan menggunakan Affine Cipher dan Algoritma Goldbach Code.

2. Bagi pembaca dan peeliti selanjutnya
   a. Bertambahnya wawasan akan ilmu kriptografi terkhusus pada penggunaan Affine Cipher dan Algoritma Goldbach Code.
   b. Mengetahui keamanan pesan teks dengan menggunakan Affine Cipher dan Algoritma Goldbach Code.
   c. Dapat digunakan sebagai referensi dalam penelitian berikutnya.
3. Bagi Institusi

   Dapat digunakan sebagai media pembelajaran bagi para mahasiswa terkhusus pada mata kuliah Kritografi.

1.5 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Enkripsi dan dekripsi semua karakter ASCII, termasuk huruf, angka, dan tanda baca.

2. Hasil enkripsi dan dekripsi ditampilkan sebagai huruf, angka, dan masing-masing karakter pada tabel ASCII.

1.6 Definisi Istilah

Beberapa istilah yang digunakan sebagai berikut:

1. Pesan merupakan perintah, nasihat, amanat yang disampaikan melalui orang lain.
2. Plainteks merupakan pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca.
3. Cipherteks merupakan informasi yang telah diubah menjadi pesan yang tidak dimengerti dengan mudah.
4. Pengirim (*sender*) merpuakan orang yang menyampaikan sebuah pesan.
5. Penerima (*receiver*) merupakan orang yang mendapat pesan dari pengirim.
6. Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan menjadi pesan tersembunyi.
7. Dekripsi adalah kebalikan dari enkripsi, yaitu proses mengubah cipherteks menjadi plainteks.
8. Cipher adalah sebuah algoritma untuk menampilkan enkripsi dan dekripsi.
9. Kunci adalah cipher yang memiliki parameter dari sebagian informasi utama.

BAB II
KAJIAN TEORI

2.1 Kongruensi

Definisi 2.1:

Jika bilangan bulat m bukan nol membagi selisih $a - b$, dapat dikatakan a kongruen dengan $b\ modulo\ m$ dan dapat ditulis dengan $a \equiv b\ (mod\ m)$. Jika $a - b$ tidak habis membagi m, dapat dikatakan bahwa a tidak kongruen dengan $b\ modulo\ m$. Sehingga dapat ditulis dengan $a \not\equiv b\ (mod\ m)$ (Niven et al., 2000).

Contoh 2.1:

1. $15 \equiv 5(mod\ 2)$, karena $(15 - 5)$ habis terbagi oleh 2.
2. $55 \not\equiv 2(mod\ 2)$, karena $(55 - 2)$ tidak habis terbagi oleh 2.

2.2 Invers Modulo

Untuk menghitung invers bilangan bulat positif a modulo n, dengan $a < n$ dan pembagi persekutuan terbesar $\text{GCD}(a, n) = 1$. Kita harus mengalikan a dengan semua elemen dari $\mathbb{N}_n^* = \{1,2, \dots, n - 1\}$ dan elemen pertama yang menghasilkan hasil kali sama dengan 1(modulo n) merupakan invers dari a (Bufalo et al., 2021).

Contoh 2.2:

Untuk mencari invers dari $1 = 6\ modulo\ n = 7$, harus mengalikan a dengan setiap elemen $\mathbb{N}_7^* = \{1,2, \dots,6\}$, sehingga

$1 \cdot 6 \equiv 6(mod\ 7)$, $2 \cdot 6 = 12 \equiv 5(mod\ 7)$, $3 \cdot 6 = 18 \equiv 4\ (mod\ 7)$,

$4 \cdot 6 = 24 \equiv 3\ (mod\ 7)$, $5 \cdot 6 = 30 \equiv 2\ (mod\ 7)$, $6 \cdot 6 = 36 \equiv 1\ (mod\ 7)$.

Maka, $a^{-1} \equiv 6 \, mod \, 7$.

2.3 Bilangan Prima

Definisi 2.2:

Bilangan bulat $p > 1$ disebut sebagai bilangan prima, atau prima, jika tidak ada pembagi d dari p yang memenuhi $1 < d < p$. Jika bilangan bulat $a > 1$ bukan bilangan prima, maka disebut sebagai bilangan komposit (Niven et al., 2000).

Lemma 2.1

Setiap bilangan bulat yang lebih besar dari 1 memiliki pembagi prima (Strayer, 2002).

Pembuktian:

Asumsikan dengan menggunakan kontradiksi, bhawa suatu bilangan bulat yang lebih besar darii 1. Katakanlah n tidak memiliki bilangan prima. Maka kita dapat berasumsi bahwa n adalah bilangan bulat terkecil. Sekarang $n|n$. Karena n tidak memiliki pembagi prima, maka n bukan merupakan bilangan prima. Jadi n adalah bilangan komposit dan akibatnya terdapat $a, b \in \mathrm{Z}$ sehingga $n = ab$, $1 < a < n$ dan $1 < b < n$. Karena $1 < a < n$, kita mendapatkan bahwa a memiliki pembagi prima, katakanlah p sehingga $p|a$. Tetapi $a|n$ sehingga kita memiliki $p|n$ dimana n memiliki pembagi prima, adalah sebuah kontradiksi. Jadi setiap bilangan bulat yang lebih besar dari 1 memiliki pembagi prima.

Contoh 2.3:

Buktikan bahwa 19 merupakan bilangan prima!

Pembuktian:

Dengan menggunakan teorema fermat maka dapat dibuktikan sebagai berikut:

Ambil $a = 2$ dan $p = 19$ maka,

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

$$2^{19-1} \equiv 1(mod\ 19)$$

$$2^{18} \equiv 1\ (mod\ 19)$$

Karena $2^{19-1} \equiv 1(mod\ 19)$, maka 19 adalah bilangan prima.

2.4 Bilangan Biner

Sistem bilangan biner merupakan sebuah sistem penulisan angka dengan menggunakan dua simbol yaitu 0 dan 1. Sistem bilangan biner modern ditemukan oleh Gottfried Wilhelm Libniz di abad ke-17. Sistem ini adalah dasar dari semua sistem bilangan yang berbasis digital. Sistem ini dapat dikonversikankan ke dalam sistem bilangan Oktal atau Heksadesimal. Bilangan biner dapat disebut juga dengan bit, atau *Binary Digit*. Dalam pengelompokkannya bilangan biner pada komputer selalu berjumlah 8 atau dapat dikenal dengan istilah 1 Byte/bita (Maulana, 2019).

Sistem bilangan ini digunakan oleh perangkat digital seperti yang ada dalam komputer dan pemutar cd. Pada perangkat digital 0 dapat diartikan sebagai low atau tidak berhasil dan 1 diartikan high atau berhasil. Dalam perhitungnannya bilangan biner tidak sama dengan perhitungan basis 10 (bilangan desimal) (Fadilah & Insannudin, n.d.).

Desimal	Biner 8 Bit
0	00000000
1	00000001
2	00000010
3	00000011
4	00000100
5	00000101
6	00000110
7	00000111
8	00001000
9	00001001
10	00001010

Gambar 2.1 Konversi Desimal ke Bentuk Biner 8 Bit

2.5 ASCII

ASCII (*American Standard Code for Information Interchange)* adalah tabel kriptografi yang biasa digunakan dalam memaksimalkan pengamanan suatu informasi yang berupa pesan teks. ASCII merupakan sebuah kode standar yang digunakan dalam pertukaran informasi pada komputer. Jumlah dari kode ASCII yaitu 255 kode. Kode ASCII yang dimulai dari $0 \ldots 127$ merupakan kode ASCII yang digunakan untuk memanipulasi teks dan kode ASCII dari $128 \ldots 255$ merupakan kode yang digunakan untuk memanipulasi grafik. ASCII sendiri mempunyai karakter kontrol yang dibedakan dalam 5 kelompok yang sesuai dengan penggunaan berturut-turut yang meliputi *Logical Communication, Device Control, Information Separator, Code Extention,* dan *Physical Communication*. Di dalam file ASCII, masing-masing alphabetic, numeric, atau karakter khusus direpresentasikan dalam 7-bit bilangan biner (Yusman, 2015).

2.6 Algoritma Kriptografi

Algoritma kriptografi digunakan untuk membuat suatu pesan rahasia dengan menggunakan struktur khusus. Ketika komuikasi dibuka lagi, metode ini membuat pesa mudah untuk diekripsi dengan cepat dan mudah. Tiga operasi dasar dari algoritma kriptografi adalah:

1. Enkripsi, merupakan hal yang sangat penting untuk keamanan data yang dikirim dan jaminan kerahasiaan. Chiper atau kode adalah nama lain dari enkripsi.
2. Dekripsi, kebalikan dari enkripsi. Algoritma yang digunakan untuk enkripsi dan dekripsi berbeda satu sama lain.
3. Kunci, digunakan untuk enkripsi dan dekripsi. Kunci ini dibagi menjadi dua, kunci rahasia (private key) dan kunci umum (public key).

Seberapa aman suatu algoritma tergantung pada bagaimana algoritma menjalankan fungsinya. Akibatnya, teknik ini dikenal sebagai algoritma yang terbatas. Yang mana algoritma ini digunakan untuk melindung pesan yang mereka komunikasikan.

Berdasarkan kunci yang digunakan, teknik kriptografi dibagi menjadi tiga bagian:

1. Algoritma Simetri.

   Metode ini sering disebut sebagai “algoritma klasik’ karena menggunakan kunci yang sama untuk operasi ekripsi da dekripsi. Saat menggunakan algoritma ini untuk mengirim pesan, penerima harus mengetahui kunci pesan utuk memahami apa yang disampaikan. Keamaan algoritma ini tergantung pada kunci yang diberikan (Ariyus, 2008).

Algoritma yang memakai kunci ini yaitu:

a. Substitusi.

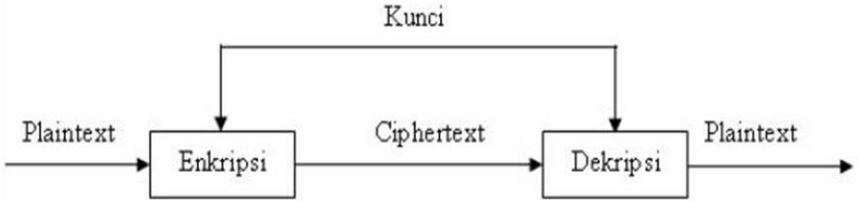
b. Transposisi (permutasi).

c. DES (Data Encryption Standard).

d. IDEA (International Data Encryption Algorithm).

e. AES (Advanced Encryption Standard).

Prosedur pengiriman pesan algoritma simetris dapat dilihat pada **Gambar 2.2**



Gambar 2.2 Skema Algoritma Simetri

2. Algoritma Asimetri

Algoritma kunci publik (public key algorithm) atau Algoritma simetri, menggunakan kunci yang berbeda untuk enkripsi dan dekripsi. Dengan menggunakan kunci, orang yang memiliki kunci dapat mengenkripsi pesan tetapi tidak dapat mendekripsikannya. Hanya pemegang kunci rahasia yang dapat membaca pesan ini. Algoritma asimetris lebih aman dalam mengirim pesan daripada algoritma simetris.

Algoritma kunci publik, yaitu:

a. DSA (Digital Signature Algorithm).

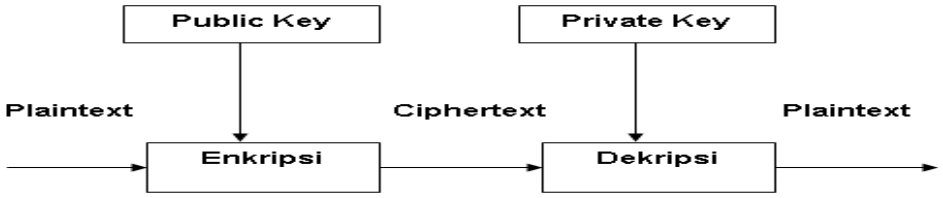
b. RSA.

c. ECC (Elliptic Curve Cryptography.

d. Kriptografi Quantum.

e. Dll.

Menggunakan algoritma asimetris, menyampaikan pesan secara sederhana didefinisikan pada **Gambar 2.3**



Gambar 2.3 Skema Algoritma Asimetri

3. Fungsi Hash.

Sebuah fungsi matematika yang disebut fungsi hash, kadang-kadang disebut sebagai fungsi satu arah (*one-way function*), *message digest*, *fingerprint*, fungsi kompresi dan *message authentication code* (MAC), dapat menerjemahkan input dengan panjang yang bervariasi menjadi urutan biner panjang yang sesuai. Fungsi ini biasanya digunakan untuk mencetak *message fingerprints* (Ariyus, 2008).

2.7 Affine Cipher

Affine Cipher merupakan sandi subtitusi yang mana setiap huruf dalam alfabet diubah menjadi numerik yang dienkripsi dengan persamaan aritmatika sederhana dan diubah kembali menjadi huruf tersebut. Affine Cipher dapat dengan mudah membuat sistem terasa aman dengan mengalikan setiap nilai teks biasa dengan angka berbeda dan kemudian menambahkan dengan nilai pergeseran (Konheim, 1986).

Metode Affine Cipher merupakan perluasan dari metode Caesar cipher, yang mana metodenya adalah dengan mengalikan plainteks (P) dengan kunci multiplikatif (m) dan menambah dengan sebuah pergeseran (b). sehingga P

menghasilkan cipherteks C yang dinyatakan dengan fungsi kongruen (Rachmawati & Candra, 2015):

$$C \equiv (mP + b)\ (mod\ n) \text{……..(1)}$$

Yang mana n merupakan ukuran dari alfabet. Persamaan 1 disebut dengan proses enkripsi. Sedangkan pada proses dekripsi dapa dilakukan dengan Persamaan 2 berikut:

$$P \equiv m^{-1}(C - b)(mod\ n) \text{……(2)}$$

Di mana m^{-1} merupakan bilangan bulat relatif prima dengan n.

Pembuktian:

$$C \equiv mP + b(mod\ n)$$

$$n|C - (mP + b)$$

$$C - (mP + b) = n \cdot x$$

$$C - mP - b = n \cdot x$$

$$mP - c + b = n(-x)$$

$$mP - (C - b) = n(-x)$$

$$n|mP - (C - b)$$

$$mP \equiv C - b\ mod\ n$$

$$P \equiv n^{-1}(C - b) mod\ n$$

Sehingga terbukti bahwa persamaan (1) menghasilkan persamaan (2).

Contoh 2.4:

Plainteks : KRIPTO (10 17 8 15 19 14)

Ambil $m = 7$ dan $b = 10$

Enkripsi $C \equiv 7P + 10(mod\ 26)$

$P_1 = 10 \rightarrow c_1 \equiv 7 \cdot 10 + 10 \equiv 80 \equiv 2\ (mod\ 26)$ (C)

$P_2 = 17 \rightarrow c_2 \equiv 7 \cdot 107 + 10 \equiv 129 \equiv 25\ (mod\ 26)$ (Z)

$P_3 = 8 \rightarrow c_3 \equiv 7 \cdot 8 + 10 \equiv 66 \equiv 14\ (mod\ 26)$ (O)

$P_4 = 15 \rightarrow c_4 \equiv 7 \cdot 15 + 10 \equiv 115 \equiv 11(mod\ 26)$ (L)

$P_5 = 19 \rightarrow c_5 \equiv 7 \cdot 19 + 10 \equiv 143 \equiv 13\ (mod\ 26)$ (N)

$P_6 = 14 \rightarrow c_6 \equiv 7 \cdot 14 + 10 \equiv 108 \equiv 4\ (mod\ 26)$ (E)

Cipherteks: CZOLNE

Dekripsi

Hitung m^{-1} yaitu $7^{-1}(mod\ 26)$ sehingga $7x \equiv 1(mod\ 26)$

Karena $7 \cdot 15 \equiv 105 \equiv 1(mod\ 26)$ sehingga solusinya: $x \equiv 15\ mod\ 26$.

Jadi, $P \equiv 15(C - 10)(mod\ 26)$

$c_1 = 2 \rightarrow p_1 \equiv 15 \cdot (2 - 10) = -120 \equiv 10(mod\ 26)$ (K)

$c_2 = 25 \rightarrow p_2 \equiv 15 \cdot (25 - 10) = 225 \equiv 17(mod\ 26)$ (R)

$c_3 = 14 \rightarrow p_3 \equiv 15 \cdot (14 - 10) = 60 \equiv 10(mod\ 26)$ (I)

$c_4 = 11 \rightarrow p_4 \equiv 15 \cdot (11 - 10) = 15 \equiv 15(mod\ 26)$ (P)

$c_5 = 13 \rightarrow p_3 \equiv 15 \cdot (13 - 10) = 45 \equiv 19(mod\ 26)$ (T)

$c_6 = 4 \rightarrow p_5 \equiv 15 \cdot (4 - 10) = -90 \equiv 14(mod\ 26)$ (O)

Sehingga plainteks yang dihasilkan yaitu KRIPTO.

2.8 Algoritma Kompresi

Kompresi data adalah proses mengenkripsi informasi menggunakan bit atau unit pembawa informasi yang lebih kecil dari representasi data ketika tidak dienkripsi dengan algoritma enkripsi tertentu (Lubis et al., 2017). Karena setiap simbol yang muncul di komputer memiliki nilai bit yang unik, kompresi data

biasanya digunakan pada perangkat keras komputer. Kompresi data ini harus mengurangi atau mempersempit jumlah data yang diambil ruang penyimpanan (Wibowo, 2012). Terdapat dua teknik kompresi data yaitu (Trivusi, 2023):

1. Kompresi Data Lossless

   Kompresi data ini digunakan untuk mengompres file tanpa kehilangan kualitas dan informasi dari file aslinya. Sederhananya dalam kompresi data lossless, ukuran file berkurang, tetapi kualitas datanya tetap sama. Kompresi ini utamanya digunakan dalam dokumen penting, informasi rahasia, dan format file PNG, RAW, GIF, dan BMP. Beberapa teknik yang digunakan dalam kompresi ini antara lain:

   a. Run Length Encoding (RLE)
   b. Lempel Ziv-Welch (LZW)
   c. Huffman Coding
   d. Arithmetic Coding

2. Kompresi Data lossy

   Kompresi data ini digunakan untuk memproses file besar menjadi file kecil. Selama proses tenik kompresinya, sejumlah kualitas data tertentu dihapus (hilang) dari file asli. Proses ini pula memfilter dan membuang data yang tidak perlu dan berlebihan demi menurunkan kualitas yang dikompresi yan kemudian dieksekusi di komputer. Kompresi data ini paling banyak digunakan dalam gambar JPEG, video MPEG, dan format audio MP3. Teknik penting dari kompresi ini yakni:

   a. Tranform codeing
   b. Discrete Cosine Transform (DCT)
   c. Discrete Wavelet Trasform (DWT)

2.9 Algoritma Goldbach Code

Kelas goldbach code dikembangkan pada tahun 2001 oleh Peter Fenwick yang berdasar pada dugaan Christian Goldbach, beliau menyatakan bahwa setiap bilangan bulat genap yang lebih besar dari empat dapat dinyatakan sebagai jumlah dari dua bilangan prima ganjil yang berbeda. Misalnya, $14 = 3 + 11$ dan $24 = 11 + 13$. Fenwick memperkenalkan kode bilangan prima sederhana yang disebut dengan G0. Sistem bilangan ini mengkodekan bilangan bulat dua kali dengan nilai offset. Setiap bilangan bulat n dapat dikodekan dengan persamaan $2(n + 3)$ untuk menghasilkan codeword yang sama (Nasution et al., 2017).

Untuk mengidentifikasi codeword Goldbach G0 yang setara untuk bilangan bulat, kedua bilangan primanya dipetakan dengan barisan bilangan prima. Misalkan $P = [3,5,7,11,13,17,19,23,29,31]$ adalah barisan dari 10 bilangan prima pertama dan misalkan $I = [0,0,0,0,0,0,0,0,0,0]$ menjadi barisan untuk indeks prima. Misalkan digit 7 akan dikodekan dalam G0. Langkah yang harus kita lakukan yaitu:

1. Pertama, tetapkan $n = 7$ dan hitung untuk $2(n + 3)$, sehingga $2(7 + 3) = 20$.
2. Selanjutnya, tentukan dari *P* dua bilangan prima pertama yang berbeda, yang dapat dijumlahkan untuk mendapat nilai 20.

Berdasarkan *P*, dua bilangan prima pertama untuk 20 adalah 7 dan 13. Kedua nilai prima ini dipetakan ke *I* meunurut indeks relatifnya yang diwakili oleh nilai 1, sehingga $I = [0,0,1,0,1,0,0,0,0,0]$. Kata sandi diidentifikasi dengan menghilangkan angka nol dari I sehingga, orde kode yang setara untuk angka 7 adalah 00101 (T. Arroyo, 2020). Contoh kode G0 untuk 15 bilangan bulat pertama dapat ditunjukkan pada **Tabel 2.1**

n	Encode $2(n+3)$	Jumlah bilangan prima	Equivalent codeword
1	8	3+5	11
2	10	3+7	101
3	12	5+7	011
4	14	3+11	1001
5	16	5+11	0101
6	18	7+11	0011
7	20	7+13	00101
8	22	5+17	010001
9	24	11+13	00011
10	26	7+19	0010001
11	28	11+17	000101
12	30	13+17	000011
13	32	13+19	0000101
14	34	11+23	00010001
15	36	5+31	100000001

Tabel 2.1 Goldbach G0 Code

Contoh 2.5:

Misalkan terdapat cipherteks CZOLNE untuk mengkompresi dengan menggunakanAlgoritma Goldbach Code dapat dilakukan seperti pada **Tabel 2.2** berikut:

Char	Frek	N	2(N+3)	Primes	Code
C	1	0	8	3+5	11
Z	1	1	10	3+7	101
O	1	2	12	5+7	011
L	1	3	14	3+11	1001
N	1	4	16	5+11	0101
E	1	5	18	7+11	0011

Tabel 2.2 Proses Kompresi Cipherteks

Berdasarkan tabel di atas, cipherteks CZOLNE dapat kita ubah menjadi “11 101 0111001 0101 0011”. Dan dari bit-bit ini akan dipecah menjadi 8 bit dan diubah menjadi karakter ASCII sehingga akan menghasilkan bentuk yang berbeda seperti pada **Tabel 2.3**:

BINARY	ASCII	CHAR
11101011	235	Ù
10010101	149	ò
0011	3	ETX

Tabel 2.3 Hasil Kompresi dengan Algoritma Goldbach Code

Sehingga cipherteks yang dihasilkan dari kompresi Algoritma Goldbach Code yaitu“ÙòETX”.

Untuk mendekrompresinya hal yang harus dilakukan yaitu mendekompresi dengan menggunakan Algoritma Goldbach Code dimana cipher akan diubah menjadi bilangan biner. Dari bilangan biner yang telah dihasilkan tersebut, akan dipecah dengan berhenti pada angka “1” yang kedua. Karena codeword hanya memiliki dua angka ”1”. Sehingga setelah bilangan biner dipecah akan dikompresi dengan melihat pada **Tabel 2.2.** Maka akan diperoleh mendapatkan hasil cipherteks awal.

2.10 Kajian Integrasi Topik dengan Al-Quran/Hadits

Komunikasi adalah sarana informasi melalui pengetahuan, warisan intelektual, dan nilai-nilai yang diubah. Oleh karena itu, kemampuan komunikasi seringkali menjadi karakteristik pendukung yang utama untuk keberhasilan misi (Ridwan & Sari, 2021). Sebagai ilmu, komunikasi islam mempunyai sumber-sumber utama yang dapat digali untuk membangun dan mengembangkan ilmu komunikasi islam. Kehadiran luas komunikasi islam dalam al-Quran dan Hadits

telah memungkinkan untuk secara sistematis memformat komunikasi islam menjadi ilmu yang tersedia untuk akademisi dan masyarakat umum. Pertukaran ajaran Islam diawali dengan perintah Allah SWT kepada Nabi Muhammad SAW peringatan umat manusia agara beriman kepada Allah SWT.

Dalam dakwahnya, Nabi melalui beberapa tahapan dakwah. Pada tahap pertama dilakukan secara tertutup di lingkungan keluarganya sendiri. Strategi ini dilakukan karena Nabi Muhammad SAW sangat memahami karakter kaum Quraisy. Kaum Quraisy rela berperang dan mati untuk demi mempertahankan keyakinanya. Karena itu, Rasulullah SAW memilih dakwah secara sembunyi-sembunyi. Pada tahapan selanjutnya, Rasulullah SAW melakukan dakwah secara terang-terangan yang dilakukan pada periode Madinah (Miftakhuddin, 2019). Nabi berhasil dalam misi dan kegiatan dakwahnya dalam hal ucapan, komunikasi verbal (lisan), maupun dalam perbuatan langsung seperti yang dicontohkan oleh beliau.

Dengan perkembangan zaman dan pesatnya perubahan teknologi informasi, teknologi informasi rentan terhadap kebocoran data. Oleh karena itu, sangat penting untuk memiliki keamanan yang dapat melindungi data agar tidak disalahgunakan oleh pihak yang tidak berhak. Keamanan basis data adalah teknik untuk mempertahankan basis data dari bahaya apapun, baik disengaja maupun tidak. Perangkat keras, perangkat lunak, manusia, bahkan data semua dapat berkontribusi pada keamanan basis data. Oleh karena itu, kontrol yang memadai diperlukan agar keamanan terjaga. Seseorang yang memiliki kewenangan untuk mengontrol dan mengelola database dapat disebut sebagai administrator. Administrator harus memiliki ketrampilan dan pengetahuan yang memadai untuk mengelola sistem.

Sehingga sangat membutuhkan administrator yang dapat dipercaya agar ketika kita memberikan hak tidak disalahgunakan.

Amanah berarti titipan, kewajiban, ketenangan, kepercayaan, kejujuran, dan kesetiaan dalam bahasa Arab. Dalam arti kata amanah berarti melakukan segala sesuatu yang dipercayakan kepada seseorang. Amanah merupakan salah satu sifat yang dimiliki oleh Rasulullah. Sehingga orang-orang yang beriman selalu memperthankan iman yang telah ditempatkan padanya. Seperti pada QS. Al-Mu'minin ayat 8:

وَٱلَّذِينَ هُمْ لِأَمَٰنَٰتِهِمْ وَعَهْدِهِمْ رَٰعُونَ ٨

"*Dan orang-orang yang memelihara amanah-amanah (yang dipikulnya) dan janjinya."*

Dalam ayat ini Allah menjelaskan bahwa salah satu sifat orang mukmin yang beruntung adalah suka memelihara amanah-amanah yang telah diberikan baik dari Allah SWT maupun dari sesama manusia yang bilamana kepada mereka dititipkannya barang atau uang sebagai amanah harus disampaikan kepada orang yang berhak menerima amanah tersebut (Abidin & Khairudin, 2017).

Dan telah dijelaskan pula dalam QS. Al-Anfal ayat 27:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُوا۟ لَا تَخُونُوا۟ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓا۟ أَمَٰنَٰتِكُمْ وَأَنتُمْ تَعْلَمُونَ ٢٧

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

Dalam tafsir QS. An-Anfal' ayat 27, menyatakan bahwa Allah SWT memerintahkan orang-orang beriman untuk menjalankan tugas yang telah

dipercayakan Allah kepada mereka, yaitu menjalankan perintah dan menjauhi larangan yang telah Allah SWT berikan kepada langit, bumi, dan gunung-gunung telah diberi perintah ini, tetapi mereka semua enggan menerimanya dan khawatir tidak akan mampu melaksanakannya. Jika seseorang memenuhi perintah tersebut, mereka berhak mendapatkan pahala yang besar dari Allah SWT tetapi jika tidak, mereka berhak mendapatkan hukuman yang berat dan dianggap penghianat Allah dan Rasul-Nya karena menghianati iman mereka.

Telah dijelaskan pula dalam hadis yang diriwayatkan oleh Abu Dawud yang membahas mengenai pentingnya menjaga rahasia:

قَالَ رَسُولُ الله صَلَّى الله عَلَيْهِ وَسَلَّمَ إِذَا حدَّثَ الرَّجُلُ بِالْحَدِيثِ ثُمَّ التَفَتَ فَهِيَ أَمَانَةٌ

(رواه ابو داود والترمذى)

"Rasulullah SAW bersabda: Apabila seseorang membicarakan sesuatu kepada orang lain (sambil) menoleh kanan kiri (karena yang dibicarakannya itu rahasia) maka itulah amanah (yang harus dijaga)." (HR. Abu Daud dan Al-Turmudzi)

Imam al-Manawi mengatakan bahwasannya jika ada orang yang memberi tahu sesuatu kemudian orang tersebut pergi atau menoleh ke kanan dan ke kiri sebagai tanda bahwa tidak ingin diketahui oleh orang, maka itu merupakan amanah yang harus dijaga kerahasiaannya. Sehingga menjaga rahasia ini wajib dilakukan hingga skala yang lebih besar.

2.11 Kajian Topik Dengan Teori Pendukung

Teknologi informasi yang berkembang secara pesat memberikan dampak yang besar terhadap kehidupan. Dengan adanya kemudahan dalam memberikan informasi, seringkali terjadi adanya kejahatan-kejahatan yang beraal dari internet sehingga mengakibatkankan pengguna internet merasa tidak aman saat melakukan

pengiriman pesan. Sehingga dengan adanya ketakutan akan kebocoran pesan, diperlukan adanya pengaman pesan. Hal ini dapat kita lakukan dengan memanfaatkan kriptografi. Sehingga dengan menggunakan kriptografi kecil kemungkinan pesan tersebut diketahui oleh pihak yang tidak memiliki wewenang.

Penerapan ilmu kriptografi ini merupakan langkah untuk dapat menentukan pesan yang telah disandikan. Dengan menentukan kunci yang akan dipakai untuk mengubah sebuah pesan. Dimana setelah melakukan pengalian kunci pada setiap bentuk dari pesan dan kunci, akan mendapatkan hasil pesan yang acak. Kemudian, dari hasil pesan acak ini dikompresi dengan menggunakan Algoritma Goldbach Code. Sehingga akan menghasilkan pesan yang sulit terbaca. Dari hasil ini, pesan yang tidak terbaca tersebut agar bisa terbaca kembali dapat melakukan hal yang sama, dengan dekompresi pesan acak tersebut kemudian mengalikan setiap pesan acak dengan menggunakan kunci yang sama saat proses penyandian. Setelah itu, pesan akan kembali menjadi teks asli yang dapat dibaca.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini menggunakan jenis penelitian studi literatur dengan tujuan untuk mengembangkan aspek-aspek teoritis dan juga manfaat praktis sehingga dapat menemukan referensi dari hasil-hasil riset yang berkaitan dengan bidang ilmu. Data yang digunakan dalam penelitian ini merupakan data yang deskriptif berupa jurnal, artikel, buku yang relevan, skripsi, dan lain-lain yang mendukung penelitian ini.

3.2 Pra Penelitian

Pada proses ini, peneliti melakukan pencarian jurnal, artikel, serta referensi lain yang berhubungan dengan Affine Cipher dan Algoritma Goldbach Code. Selanjutnya peneliti menganalisis bagaimana cara menggabungkan dua algoritma ini sehingga menghasilkan tingkat keamanan pada pesan teks.

3.3 Tahapan Penelitian

Penelitian ini memiliki 2 tahapan, yaitu:

1. Proses enkripsi:
    a. Membentuk kombinasi Algoritma enkripsi dan kompresi.
    b. Melakukan simulasi enkripsi dan kompresi.
        1) Menentukan pesan (plainteks).
        2) Mengkonversi plainteks menjadi bilangan desimal.
        3) Menentukan m dan b.
        4) Melakukan perhitungan dengan menggunakan Affine Cipher yang telah dimodifikasi.

$$C \equiv (m(P - 32) + b)(mod\ 95) + 32$$

5) Mengkonversi hasil cipherteks dari Affine dengan menggunakan Algoritma Goldbach Code.
6) Mengubah hasil dari Algoritma Goldbach Code ke bentuk ASCII.
7) Mendapatkan pesan acak (cipherteks)

2. Proses dekripsi:
   a. Membentuk algoritma dekripsi dan dekompresi.
   b. Melakukan simulasi dekripsi dan dekompresi.
      1) Dekompresi pesan acak (cipherteks) dengan menggunakan Algoritma Goldbach Code menjadi bilangan biner.
      2) Mengubah bilangan biner dengan menggunakan Algoritma Goldbach Code menjadi cipherteks biasa.
      3) Menentukan nilai dari m^{-1}.
      4) Mendekripsi dengan menggunakan Affine Cipher yang telah dimodifikasi dengan nilai b yang sama.

$$P \equiv (m^{-1}(C - 32 - b)mod\ 95) + 32$$

      5) Mendapatkan pesan asli (plainteks).

BAB IV
HASIL DAN PEMBAHASAN

4.1 Algoritma Enkripsi Affine Cipher dan Kompresi Goldbach Code

Algoritma enkripsi pesan teks dengan menggunakan Affine Cipher dan Kompresi pesan teks menggunakan Algoritma Goldbach Code sebagai berikut:

1. Proses enkripsi pertama akan dilakukan dengan menggunakan Affine Cipher. Pengirim akan menentukan sebuah pesan asli yang akan dikonversi menjadi bilangan desimal. Karena proses enkripsi ini menggunakan metode Affine Cipher sehingga akan ditentukan terlebih dahulu kunci multiplikatif (m) dan juga pergeseran (b). Kemudian proses enkripsi mengunakan Affine Cipher yang telah termodifikasi modulonya dengan ASCII Printable sehingga perhitungannya sebagai berikut:

$$C \equiv (m(P - 32) + b)(mod\ 95) + 32$$

2. Proses kompresi akan dilakukan dengan menggunakan Algoritma Goldbach Code. Pada proses ini Cipherteks yang telah dihasilkan pada saat enkripsi akan dikompresi dengan menggunakan Algoritma Goldbach Code yang selanjutnya akan diubah menjadi sebuah bentuk ASCII.

4.2 Simulasi Enkripsi Affine Cipher dan Kompresi Goldbach Code

Proses enkripsi yang akan dilakukan diawali dengan menggunakan metode Affine Cipher. Berikut langkah-langkah yang dapat dilakukan:

1. Menentukan plainteks atau pesan asli

   Plainteks yang akan digunakan dalam penelitian ini adalah “FORGIVE AND FORGET”.

2. Mengkonversi plainteks kedalam bentuk desimal.

Plainteks	Kode ASCII (desimal)
F	70
O	79
R	82
G	71
I	73
V	86
E	69
Space	32
A	65
N	78
D	68

Plainteks	Kode ASCII (desimal)
Space	32
F	70
O	79
R	82
G	71
E	69
T	84

Tabel 4.1 Konversi Karakter Alfabet Menjadi Kode ASCII (desimal)

3. Menentukan kunci multiplikatif (m) dan pergeseran (b).

   Peneliti memilih $m = 71$ dikarenakan $GCD(71,95) = 1$ dan $b = 30$.

4. Melakukan perhitungan dengan menggunakan Affine Cipher dengan rumus yang digunakan mengalami modifikasi berupa adanya penambahan dan juga pengurangan 32. Hal ini dilakukan dengan tujuan untuk membuat karakter yang akan muncul berapa pada rentang 32-126 sesuai dengan kode ASCII *printable*. Dan menggunakan modulo 95 untuk menyesuaikan dengan jumlah karakter ASCII *printable*.

$$C \equiv (m(P - 32) + b)(mod\ 95) + 32$$

Indeks Plainteks	Enkripsi Affine Cipher $(m(P-32)+b)(mod\ 95)+32$	Indek Cipherteks	Cipherteks
70	$(71(70-32)+30)(mod\ 95)$ $+32$ $=(71(38)+30)(mod\ 95)+32$ $=(2698+30)(mod\ 95)+32$ $=2728(mod 95)+32$ $=68+32$ $=100$	100	d
79	$(71(79-32)+30)(mod\ 95)$ $+32$	74	J
82	$(71(82-32)+30)(mod\ 95)$ $+32$	97	a

Indeks Plainteks	Enkripsi Affine Cipher $(m(P-32)+b)(mod\ 95)+32$	Indek Cipherteks	Cipherteks
71	$(71(71-32)+30)(mod\ 95)+32$	76	L
73	$(71(73-32)+30)(mod\ 95)+32$	123	{
86	$(71(86-32)+30)(mod\ 95)+32$	96	`
69	$(71(69-32)+30)(mod\ 95)+32$	124	|
32	$(71(32-32)+30)(mod\ 95)+32$	62	>
65	$(71(65-32)+30)(mod\ 95)+32$	125	}
78	$(71(78-32)+30)(mod\ 95)+32$	98	b
68	$(71(68-32)+30)(mod\ 95)+32$	53	S
32	$(71(32-32)+30)(mod\ 95)+32$	62	>
70	$(71(70-32)+30)(mod\ 95)+32$	100	d
79	$(71(79-32)+30)(mod\ 95)+32$	74	J
82	$(71(82-32)+30)(mod\ 95)+32$	97	a
71	$(71(71-32)+30)(mod\ 95)+32$	76	L
69	$(71(69-32)+30)(mod\ 95)+32$	124	|
84	$(71(84-32)+30)(mod\ 95)+32$	49	1

Tabel 4.2 Enkripsi dengan Menggunakan Affine Cipher

Cipherteks yang dihasilkan pada proses enkripsi menggunakan Affine Cipher yaitu "**dJaL{`|>}bS>dJaL|1**"

5. Melakukan kompresi dengan menggunakan Algoritma Goldbach Code

   Setelah hasil cipherteks telah diketahui maka akan dilakukan proses kompresi dengan menggunkan Algoritma Goldbach Code. sehingga proses yang dilakukan seperti pada **Tabel 4.3**:

Cipher teks	Frek	N	2(N+3)	Prima	Code word
d	2	1	8	$3 \cdot 1 + 5 \cdot 1$	11
J	2	2	10	$3 \cdot 1 + 5 \cdot 0 + 7 \cdot 1$	101
a	2	3	12	$3 \cdot 0 + 5 \cdot 1 + 7 \cdot 1$	011
L	2	4	14	$3 \cdot 1 + 5 \cdot 0 + 7 \cdot 0 + 11 \cdot 1$	1001
|	2	5	16	$3 \cdot 0 + 5 \cdot 1 + 7 \cdot 0 + 11 \cdot 1$	0101
>	2	6	18	$3 \cdot 0 + 5 \cdot 0 + 7 \cdot 1 + 11 \cdot 1$	0011
{	1	7	20	$3 \cdot 0 + 5 \cdot 0 + 7 \cdot 1 + 11 \cdot 0 + 13 \cdot 1$	00101
`	1	8	22	$3 \cdot 0 + 5 \cdot 1 + 7 \cdot 0 + 11 \cdot 0 + 13 \cdot 0 + 17 \cdot 1$	010001
}	1	9	24	$3 \cdot 0 + 5 \cdot 0 + 7 \cdot 0 + 11 \cdot 1 + 13 \cdot 1$	00011
b	1	10	26	$3 \cdot 0 + 5 \cdot 0 + 7 \cdot 1 + 11 \cdot 0 + 13 \cdot 0 + 17 \cdot 0 + 19 \cdot 1$	0010001
S	1	11	28	$3 \cdot 0 + 5 \cdot 0 + 7 \cdot 0 + 11 \cdot 1 + 13 \cdot 0 + 17 \cdot 1$	000101
1	1	12	30	$3 \cdot 0 + 5 \cdot 0 + 7 \cdot 0 + 11 \cdot 0 + 13 \cdot 1 + 17 \cdot 1$	000011

Tabel 4.3 Proses Kompresi Cipherteks

Berdasarkan pada tabel diatas, cipherteks "**dJaL{`|>}bS>dJaL|1**" berubah menjadi " 11 101 011 1001 00101 010001 0101 0011 00011 0010001 000101 0011 11 101 011 1001 0101 000011"

6. Mengubah hasil dari Algoritma Goldbach Code menjadi bentuk ASCII

   Dari bit-bit yang dihasilkan akan dipecah menjadi 8-bit dan akan diubah menjadi karakter ASCII sehingga akan menghasilkan bentuk yang berbeda seperti yang terdapat pada **Tabel 4.4**

Biner	Desimal	Karakter
11101011	235	Ù
10010010	146	Æ
10100010	162	ó
10100110	166	ª
00110010	50	2
00100010	34	"
10011111	159	*f*
01011100	92	\
10101000	168	¿
Biner	Desimal	Karakter
011	3	ETX

Tabel 4.4 Hasil Kompresi dengan Algoritma Goldbach Code

Sehingga cipherteks yang dihasilkan dengan menggunakan Affine Cipher yaitu "**dJaL{|>}bS>dJaL|1**" dengan panjang bit sebanyak 144 bit dan setelah dilakukan kompresi dengan menggunakan Algoritma Goldbach Code menjadi "**ÙÆóª2"*f*\¿ETX**" dengan panjang 80 bit.

4.3 Algoritma Dekripsi Affine Cipher dan Dekompresi Goldbach Code

Algoritma dekripsi pesan dengan menggunakan Affine Cipher dan Dekompresi pesan dengan Algoritma Goldbach Code sebagai berikut:

1. Proses dekripsi akan dimulai dengan menggunakan Algoritma Goldbach Code. Yang mana sebuah Cipherteks didekompresi dengan Algoritma Goldbach Code sehingga akan menghasilkan bilangan biner. Bilangan biner ini akan diubah dengan menggunakan Goldbach Code sehingga akan menghasilkan sebuah cipherteks Affine Cipher.
2. Proses dekripsi dengan menggunakan Affine Cipher. Sebelum mendekripsi cipherteks, harus menentukan terlebih dahulu nilai invers dari bilangan relatif prima (m^{-1}). Setelah nilai m^{-1} diketahui dapat dilakukan dekripsi

dengan menggunakan Affine Cipher yang telah termodifikasi, sehingga perhitungannya sebagai berikut:

$$P \equiv (m^{-1}(C - 32 - b) mod\ 95) + 32$$

4.4 Simulasi Dekripsi Affine Cipher dan Dekompresi Goldbach Code

Pada proses dekripsi akan diawali dengan mendekompresi cipherteks yang telah dihasilkan pada proses kompresi. Sehingga langkah-langkah yang dilakukan sebagai berikut:

1. Mendekompresi cipherteks dengan menggunakan Algoritma Goldbach Code menjadi sebuah bilangan biner.

   Cipherteks: **ÙÆóª2"ƒ\¿ETX** dengan menggunakan tabel ASCII maka didapatkan hasil bilangan biner seperti **Tabel 4.5**

Karakter	Desimal	Biner
Ù	235	11101011
Æ	146	10010010
ó	162	10100010
ª	166	10100110
2	50	00110010
"	34	00100010
ƒ	159	10011111
\	92	01011100
¿	168	10101000
ETX	3	011

Tabel 4.5 Mengubah Cipherteks Menjadi Bilangan Biner

   Sehingga bilangan biner yang diperoleh adalah “11101011 10010010 10100010 10100110 00110010 00100010 10011111 01011100 10101000 011”

2. Dari bilangan biner yang dihasilkan dapat kita pisah dengan berhenti untuk “1” yang kedua sehingga menghasilkan:

"11 101 011 1001 00101 010001 0101 0011 00011 0010001 000101 0011 11 101 011 1001 0101 000011" dengan melihat pada **Tabel 4.3** bilangan biner akan menjadi **"dJaL{`|>}bS>dJaL|1"**.

3. Dari hasil dekompresi tersebut cipherteks dikompresi menjadi bilangan desimal sehingga menghasilkan

Cipher teks	Desimal
d	100
J	74
a	97
L	76
{	123
`	96
|	124

Cipher teks	Desimal
>	62
}	125
b	98
S	83
>	62
d	100
J	74

Cipher teks	Desimal
a	97
L	76
|	124
1	49

Tabel 4.6 Mengubah Cipherteks menjadi Desimal

4. Sebelum melakukan dekripsi menggunakan Affine Cipher, yang harus dilakukan yaitu mencari nilai dari m^{-1} dari $m = 71$. Sehingga

$$91 \cdot 71x \equiv 91 \cdot 1(mod\ 95)$$

$$x \equiv 91\ (mod\ 95)$$

Sehingga didapatkan $71 \cdot 91 \equiv 1\ (mod\ 95)$ maka $m^{-1} = 91$.

5. Dengan menggunakan nilai $m^{-1} = 91$ dan $b = 30$ dapat didekripsi dengan menggunakan Affine Cipher. Sehingga

$$P \equiv (91(C - 32 - 30)mod\ 95) + 32$$

Indek Cipherteks	Enkripsi Affine Cipher $(91(C-32-30)mod\ 95)+32$	Indeks Plainteks	Plainteks
100	$(91(100-32-30)mod\ 95) + 32$ $= (91(38)mod\ 95) + 32$ $= (3458\ mod\ 95) + 32$ $= 38 + 32$ $= 70$	70	F

Indek Cipherteks	Enkripsi Affine Cipher $(91(C-32-30) mod\ 95)+32$	Indeks Plainteks	Plainteks
74	$(91(74-32-30) mod\ 95)+32$	79	O
97	$(91(97-32-30) mod\ 95)+32$	82	R
76	$(91(76-32-30) mod\ 95)+32$	71	G
123	$(91(123-32-30) mod\ 95)+32$	73	I
96	$(91(96-32-30) mod\ 95)+32$	86	V
124	$(91(124-32-30) mod\ 95)+32$	69	E
62	$(91(62-32-30) mod\ 95)+32$	32	Space
125	$(91(125-32-30) mod\ 95)+32$	65	A
98	$(91(98-32-30) mod\ 95)+32$	78	N
53	$(91(53-32-30) mod\ 95)+32$	68	D
62	$(91(62-32-30) mod\ 95)+32$	32	Space
100	$(91(100-32-30) mod\ 95)+32$	70	F
74	$(91(74-32-30) mod\ 95)+32$	79	O
97	$(91(97-32-30) mod\ 95)+32$	82	R
76	$(91(76-32-30) mod\ 95)+32$	71	G
124	$(91(124-32-30) mod\ 95)+32$	69	E
49	$(91(49-32-30) mod\ 95)+32$	84	T

Tabel 4.7 Dekripsi dengan Menggunkan Affine Cipher

Sehingga hasil dari dekompresi dan dekripsi pesan menggunakan Algoritma Goldbach Code dan Affine Cipher yatitu "**FORGIVE AND FORGET**".

4.5 Kajian Integrasi Agama

Pengiriman sebuah informasi rahasia harus dilakukan dengan aman hingga sebuah informasi rahasia tersebut dapat diterima dengan aman hingga pihak penerima. Sehingga penyampaian informasi rahasia sejalan dengan adanya konsep amanah. Dimana konsep amanah sendiri merupakan suatu sifat dan sikap pribadi yang setia, tulus hati dan jujur di dalam melaksanakan sesuatu yang telah dipercayakan kepadanya, berupa harta benda, rahasia maupun tugas kewajiban. Sifat amanah merupakan salah satu sifat yang melekat dalam diri Rasulullah SAW, yang mana sifat ini merupakan sifat yang dapat dipercaya oleh orang lain terhadap perilaku dan segala amanah yang telah dibebankan kepada-Nya. Selain sifat amanah, sifat tabligh merupakan sifat Rasulullah yang berarti menyampaikan. Disamping kita diberi amanah kita juga harus menyampaikan amanah tersebut. Setiap muslim diharuskan memiliki sifat amanah dikarenakan dapat memudahkan dan menyakinkan orang lain terhadap segala kepercayaan yang telah dibebankan terhadapnya (Amiruddin, 2021).

Pengiriman suatu informasi yang bersifat rahasia perlu adanya perhatian terhadap kemanannya sehingga ativitas ini tidak dapat diketahui oleh publik. Dewasa ini, informasi rahasia sering terjadi adanya kebocoran. Sehingga untuk meminimalisir terjadinya kebocoran data, dapat dilakukan dengan menggunakan kriptografi. Di dalam kriptografi ini pesan rahasia akan diubah menjadi sebuah pesan acak dengan menggunakan algoritma-algoritma dalam kriptografi. Informasi rahasia ini sama dengan amanah. Dimana orang yang mempunyai sifat ini, akan segan dalam membocorkan informasi yang telah diberikan kepadanya. Karena suatu saat akan dimintai pertanggung jawaban kelak dihadapan Allah SWT.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan di atas, dapat ditarik kesimpulan sebagai berikut:

1. Proses enkripsi dengan menggunakan Affine Cipher dan kompresi pesan menggunakan Algoritma Goldbach Code diawali dengan menentukan nilai dari kunci multiplikatif $(m) = 71$ dan pergeseran $(b) = 30$. Kemudian memasukkan indeks plainteks dan melakukan perhitungan menggunakan Affine Cipher yang telah dimodifikasi $C \equiv (m(P - 32) + b)(mod\ 95) + 32$. Setelah hasil enkripsi menggunakan Affine Cipher diketahui, cipherteks akan dikompresi dengan menggunakan Algoritma Goldbach Code. Cipherteks tersebut awalnya akan dikompresi dengan goldbach code sehingga menghasilkan bilangan biner. Selanjutnya bilangan biner akan dikelompokkan menjadi 8 bit sehingga dari bilangan biner yang berjumlah 8 bit tersebut dapat dikonversi menjadi karakter ASCII. Sehingga cipherteks yang panjang bit awalnya berjumlah 144 bit akan dikompresi menjadi 80 bit.
2. Proses dekripsi menggunakan Affine Cipher dan dekompresi menggunakan Algoritma Goldbach Code. Proses ini akan diawali dengan dekompresi cipherteks dengan menggunakan Algoritma Goldbach Code. Pada proses dekompresi ini awalnya akan mengubah cipherteks menjadi bilangan biner. Kemudian bilangan biner akan dipisah sesuai dengan jumlah bit sebelumnya. Setelah dilakukan pemisahan akan dilakukan dekompresi dengan melihat tabel kompresi goldbach code. Kemudian menentukan

balikan dari kunci multiplikatif $(m^{-1}) = 91$. Selanjutnya memasukkan indeks cipherteks dan melakukan perhitungan menggunakan Affine Cipher $P \equiv (91(C - 32 - 30) mod\ 95) + 32$ sehingga akan menghasilkan plainteks.

5.2 Saran

Penelitian ini membahas tentang implementasi Affine Cipher dan Algoritma Goldbach Code dalam mengamankan pesan teks. Untuk penelitian yang akan datang, disarankan untuk menggunakan kombinasi lain.

DAFTAR PUSTAKA

Al Qur'an dan Terjemahan. (2019). Kementrian Agama RI.

Abidin, Z., & Khairudin, F. (2017). Penafsiran ayat-ayat amanah dalam al- qur'an. *Jurnal Syahada*, *V*(2), 1–26.

Amiruddin, A. (2021). AMANAH DALAM PERSPEKTIF AL-QURAN (Studi Komparatif Tafsir Al-Misbah dan Al-Azhar). *Jurnal MUDARRISUNA: Media Kajian Pendidikan Agama Islam*, *11*(4), 833. https://doi.org/10.22373/jm.v11i4.4665

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi*.

Bufalo, M., Bufalo, D., & Orlando, G. (2021). A note on the computation of the modular inverse for cryptography. *Axioms*, *10*(2), 1–10. https://doi.org/10.3390/axioms10020116

Dwi, B. J., Joko Priono, M., Suhendri, A., & Darwis, D. (2018). Implementasi Kombinasi Affine Cipher Dan One-Time Pad Dalam. *Jurnal Informatika*, *18*(2), 124–129.

Fadilah, N., & Insannudin, E. (n.d.). *Modifikasi Affine Cipher Dan Vigènere Cipher Dengan Menggunakan N Bit*.

Irliansyah, M. R., Nastion, S. D., & Ulfa, K. (2017). Penerapan Metode Deflate Dan Algoritma Goldbach Codes Dalam Kompresi File Teks. *KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer)*, *1*(1), 186–189.

Kester, Q.-A. (2021). A cryptosystem based on Vigenère cipher with varying key (virtual) View project. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *1*(10), 15–17. https://www.researchgate.net/publication/235618077

Konheim, A. G. (1986). Computer Security and cryptography. In *IEEE Communications Magazine* (Vol. 23, Issue 7). https://doi.org/10.1109/MCOM.1985.1092611

Lubis, A. H., Nasution, S. D., & Ulfa, K. (2017). Penerapan Algoritma Goldbach Codes Dalam Pemampatan Short Message Service Berbasis Android. *KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer)*, *1*(1), 171–175.

Maulana, P. A. (2019). Proses Enkripsi & Dekripsi Pada Polinomial Dengan Menggunakan Metode Affine Cipher. *Etheses Uin*, 28.

Miftakhuddin. (2019). Pesan Komunikasi Dalam Kepemimpinan Dakwah Rasulullah Saw. *An-Nida"': Jurnal Prodi Komunikasi Penyiaran Islam*, *VIII*(2), 117–135.

Nasution, S. D., Ginting, G. L., Syahrizal, M., & Rahim, R. (2017). Data Security Using Vigenere Cipher and Goldbach Codes Algorithm. *International Journal of Engineering Research & Technology (IJERT)*, *6*(01), 360–363.

Niven, I. M., Montgomery, H. L., & Zuckerman, H. S. (2000). *Introduction to the*

theory of numbers (p. 529).

Rachmawati, D., & Candra, A. (2015). Implementasi Kombinasi Caesar dan Affine Cipher untuk Keamanan Data Teks. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *1*(2). https://doi.org/10.26418/jp.v1i2.12587

Ridwan, & Sari, H. (2021). METODE KOMUNIKASI DAKWAH RASULULLAH (KAJIAN TEMATIK DALAM KITAB SAHIH MUSLIM). *NUKHBATUL 'ULUM: Jurnal Bidang Kajian Islam*, *7*(2), 259–278. https://doi.org/10.21043/politea.v4i1.10527.2

Strayer, J. K. (2002). *Elementary Number theory*.

T. Arroyo, J. C. (2020). Caesar Cipher with Goldbach Code Compression for Efficient Cryptography. *International Journal of Emerging Trends in Engineering Research*, *8*(7), 2999–3002. https://doi.org/10.30534/ijeter/2020/19872020

Trivusi. (2023). *Kompresi Data: Pengertian, Jenis, Kelebihan, dan Kekurangannya*. Trivusi.Web.Id.

Walker, M. (2005). *Cryptography and Network Security*. https://doi.org/10.1049/ic:19960523

Wibowo, A. (2012). Kompresi Data Menggunakan Metode Huffman. *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2012*, *2*(1), 47–51. http://publikasi.dinus.ac.id/index.php/semantik/article/view/70

Yusman, M. (2015). PENGEMBANGAN APLIKASI ENKRIPSI DAN DEKRIPSI KEAMANAN DATA MENGGUNAKAN METODE ASCII. *Jurusan Ilmu Komputer FMIPA Unila*, *16.1.2015*.

LAMPIRAN-LAMPIRAN

Lampiran 1 : Karakter Kontrol ASCII (Tidak Dapat Ditampilkan):

Kode ASCII (desimal)	Kode ASCII (2-ary)	Kode ASCII (oktal)	Kode ASCII (heksadesimal)	Char (karakter)	Deskripsi (Pendahuluan)
00	0	0	0	NULL	Null character
01	1	1	1	SOH	Start of Header
02	10	2	2	STX	Start of Text
03	11	3	3	ETX	End of Text, hearts card suit
04	100	4	4	EOT	End of Transmission, diamonds card suit
05	101	5	5	ENQ	Enquiry, clubs card suit
06	110	6	6	ACK	Acknowledgement, spade card suit
07	111	7	7	BEL	Bell
08	1000	10	8	BS	Backspace
09	1001	11	9	HT	Horizontal Tab
10	1010	12	a	LF	Line feed
11	1011	13	b	VT	Vertical Tab, male symbol, symbol for Mars
12	1100	14	c	FF	Form feed, female symbol, symbol for Venus
13	1101	15	d	CR	Carriage return
14	1110	16	e	SO	Shift Out
15	1111	17	f	SI	Shift In
16	10000	20	10	DLE	Data link escape
17	10001	21	11	DC1	Device control 1
18	10010	22	12	DC2	Device control 2
19	10011	23	13	DC3	Device control 3
20	10100	24	14	DC4	Device control 4
21	10101	25	15	NAK	NAK Negative-acknowledge
22	10110	26	16	SYN	Synchronous idle
23	10111	27	17	ETB	End of trans. block
24	11000	30	18	CAN	Cancel
25	11001	31	19	EM	End of medium

26	11010	32	1a	SUB	Substitute
27	11011	33	1b	ESC	Escape
28	11100	34	1c	FS	File separator
29	11101	35	1d	GS	Group separator
30	11110	36	1e	RS	Record separator
31	11111	37	1f	US	Unit separator
127	1111111	177	7f	DEL	Delete

Lampiran 2: simbol ASCII (dapat ditampilkan):

Kode ASCII (desimal)	**Kode ASCII (2-ary)**	**Kode ASCII (oktal)**	**Kode ASCII (heksadesimal)**	**Char (karakter)**	**Deskripsi (Pendahuluan)**
32	100000	40	20	space	Space
33	100001	41	21	!	Exclamation mark
34	100010	42	22	"	Double quotes ; Quotation mark ; speech marks
35	100011	43	23	#	Number sign
36	100100	44	24	$	Dollar sign
37	100101	45	25	%	Percent sign
38	100110	46	26	&	Ampersand
39	100111	47	27	'	Single quote or Apostrophe
40	101000	50	28	(	round brackets or parentheses, opening round bracket
41	101001	51	29	)	parentheses or round brackets, closing parentheses
42	101010	52	2a	*	Asterisk
43	101011	53	2b	+	Plus sign
44	101100	54	2c	,	Comma
45	101101	55	2d	-	Hyphen, minus sign
46	101110	56	2e	.	Dot, full stop
47	101111	57	2f	/	Slash, forward slash, fraction bar, division slash
48	110000	60	30	0	number zero
49	110001	61	31	1	number one

50	110010	62	32	2	number two
51	110011	63	33	3	number three
52	110100	64	34	4	number four
53	110101	65	35	5	number five
54	110110	66	36	6	number six
55	110111	67	37	7	number seven
56	111000	70	38	8	number eight
57	111001	71	39	9	number nine
58	111010	72	3a	:	Colon
59	111011	73	3b	;	Semicolon
60	111100	74	3c	<	Less-than sign
61	111101	75	3d	=	Equals sign
62	111110	76	3e	>	Greater-than sign ; Inequality
63	111111	77	3f	?	Question mark
64	1000000	100	40	@	At sign
65	1000001	101	41	A	Capital letter A
66	1000010	102	42	B	Capital letter B
67	1000011	103	43	C	Capital letter C
68	1000100	104	44	D	Capital letter D
69	1000101	105	45	E	Capital letter E
70	1000110	106	46	F	Capital letter F
71	1000111	107	47	G	Capital letter G
72	1001000	110	48	H	Capital letter H
73	1001001	111	49	I	Capital letter I
74	1001010	112	4a	J	Capital letter J
75	1001011	113	4b	K	Capital letter K
76	1001100	114	4c	L	Capital letter L
77	1001101	115	4d	M	Capital letter M
78	1001110	116	4e	N	Capital letter N
79	1001111	117	4f	O	Capital letter O
80	1010000	120	50	P	Capital letter P
81	1010001	121	51	Q	Capital letter Q
82	1010010	122	52	R	Capital letter R
83	1010011	123	53	S	Capital letter S
84	1010100	124	54	T	Capital letter T
85	1010101	125	55	U	Capital letter U
86	1010110	126	56	V	Capital letter V
87	1010111	127	57	W	Capital letter W
88	1011000	130	58	X	Capital letter X
89	1011001	131	59	Y	Capital letter Y
90	1011010	132	5a	Z	Capital letter Z
91	1011011	133	5b	[	square brackets or box brackets,

					opening bracket
92	1011100	134	5c	\	Backslash, reverse slash
93	1011101	135	5d	]	box brackets or square brackets, closing bracket
94	1011110	136	5e	^	Circumflex accent or Caret
95	1011111	137	5f	_	underscore, understrike, underbar or low line
96	1100000	140	60	`	Grave accent
97	1100001	141	61	a	Lowercase letter a, minuscule a
98	1100010	142	62	b	Lowercase letter b, minuscule b
99	1100011	143	63	c	Lowercase letter c, minuscule c
100	1100100	144	64	d	Lowercase letter d, minuscule d
101	1100101	145	65	e	Lowercase letter e, minuscule e
102	1100110	146	66	f	Lowercase letter f, minuscule f
103	1100111	147	67	g	Lowercase letter g, minuscule g
104	1101000	150	68	h	Lowercase letter h, minuscule h
105	1101001	151	69	i	Lowercase letter i, minuscule i
106	1101010	152	6a	j	Lowercase letter j, minuscule j
107	1101011	153	6b	k	Lowercase letter k, minuscule k

108	1101100	154	6c	l	Lowercase letter l, minuscule l
109	1101101	155	6d	m	Lowercase letter m, minuscule m
110	1101110	156	6e	n	Lowercase letter n, minuscule n
111	1101111	157	6f	o	Lowercase letter o, minuscule o
112	1110000	160	70	p	Lowercase letter p, minuscule p
113	1110001	161	71	q	Lowercase letter q, minuscule q
114	1110010	162	72	r	Lowercase letter r, minuscule r
115	1110011	163	73	s	Lowercase letter s, minuscule s
116	1110100	164	74	t	Lowercase letter t, minuscule t
117	1110101	165	75	u	Lowercase letter u, minuscule u
118	1110110	166	76	v	Lowercase letter v, minuscule v
119	1110111	167	77	w	Lowercase letter w, minuscule w
120	1111000	170	78	x	Lowercase letter x, minuscule x
121	1111001	171	79	y	Lowercase letter y, minuscule y
122	1111010	172	7a	z	Lowercase letter z, minuscule z
123	1111011	173	7b	{	braces or curly brackets, opening braces

124	1111100	174	7c	|	vertical-bar, vbar, vertical line or vertical slash
125	1111101	175	7d	}	curly brackets or braces, closing curly brackets
126	1111110	176	7e	~	Tilde ; swung dash

Lampiran 3: Karakter diperluas ASCII:

Kode ASCII (desimal)	**Kode ASCII (2-ary)**	**Kode ASCII (oktal)**	**Kode ASCII (heksadesimal)**	**Char (karakter)**	**Deskripsi (Pendahuluan)**
128	10000000	200	80	Ç	Majuscule C-cedilla
129	10000001	201	81	ü	letter u with umlaut or diaeresis, u-umlaut
130	10000010	202	82	é	letter e with acute accent or e-acute
131	10000011	203	83	â	letter a with circumflex accent or a-circumflex
132	10000100	204	84	ä	letter a with umlaut or diaeresis, a-umlaut
133	10000101	205	85	à	letter a with grave accent
134	10000110	206	86	å	letter a with a ring
135	10000111	207	87	ç	Minuscule c-cedilla
136	10001000	210	88	ê	letter e with circumflex accent or e-circumflex
137	10001001	211	89	ë	letter e with umlaut or

					diaeresis ; e-umlauts
138	10001010	212	8a	è	letter e with grave accent
139	10001011	213	8b	ï	letter i with umlaut or diaeresis ; i-umlaut
140	10001100	214	8c	î	letter i with circumflex accent or i-circumflex
141	10001101	215	8d	ì	letter i with grave accent
142	10001110	216	8e	Ä	letter A with umlaut or diaeresis ; A-umlaut
143	10001111	217	8f	Å	Capital letter A with a ring
144	10010000	220	90	É	Capital letter E with acute accent or E-acute
145	10010001	221	91	æ	Latin diphthong ae in lowercase
146	10010010	222	92	Æ	Latin diphthong AE in uppercase
147	10010011	223	93	ô	letter o with circumflex accent or o-circumflex
148	10010100	224	94	ö	letter o with umlaut or diaeresis ; o-umlaut
149	10010101	225	95	ò	letter o with grave accent
150	10010110	226	96	û	letter u with circumflex accent or u-circumflex
151	10010111	227	97	ù	letter u with grave accent

152	10011000	230	98	ÿ	Lowercase letter y with diaeresis
153	10011001	231	99	Ö	Letter O with umlaut or diaeresis ; O-umlaut
154	10011010	232	9a	Ü	Letter U with umlaut or diaeresis ; U-umlaut
155	10011011	233	9b	ø	Lowercase slashed zero or empty set
156	10011100	234	9c	£	Pound sign ; symbol for the pound sterling
157	10011101	235	9d	Ø	Uppercase slashed zero or empty set
158	10011110	236	9e	×	Multiplication sign
159	10011111	237	9f	*ƒ*	Function sign ; f with hook sign ; florin sign
160	10100000	240	a0	á	Lowercase letter a with acute accent or a-acute
161	10100001	241	a1	í	Lowercase letter i with acute accent or i-acute
162	10100010	242	a2	ó	Lowercase letter o with acute accent or o-acute
163	10100011	243	a3	ú	Lowercase letter u with acute accent or u-acute
164	10100100	244	a4	ñ	eñe, enie, spanish letter enye, lowercase n with tilde

165	10100101	245	a5	Ñ	Spanish letter enye, uppercase N with tilde, EÑE, enie
166	10100110	246	a6	ª	feminine ordinal indicator
167	10100111	247	a7	º	masculine ordinal indicator
168	10101000	250	a8	¿	Inverted question marks
169	10101001	251	a9	®	Registered trademark symbol
170	10101010	252	aa	¬	Logical negation symbol
171	10101011	253	ab	½	One half
172	10101100	254	ac	¼	Quarter, one fourth
173	10101101	255	ad	¡	Inverted exclamation marks
174	10101110	256	ae	«	Angle quotes, guillemets, right-pointing quotation mark
175	10101111	257	af	»	Guillemets, angle quotes, left-pointing quotation marks
176	10110000	260	b0	▒	Graphic character, low density dotted
177	10110001	261	b1	▒	Graphic character, medium density dotted
178	10110010	262	b2	▓	Graphic character, high density dotted
179	10110011	263	b3	│	Box drawing character

					single vertical line
180	10110100	264	b4	┤	Box drawing character single vertical and left line
181	10110101	265	b5	Á	Capital letter A with acute accent or A-acute
182	10110110	266	b6	Â	Letter A with circumflex accent or A-circumflex
183	10110111	267	b7	À	Letter A with grave accent
184	10111000	270	b8	©	Copyright symbol
185	10111001	271	b9	╣	Box drawing character double line vertical and left
186	10111010	272	ba	║	Box drawing character double vertical line
187	10111011	273	bb	╗	Box drawing character double line upper right corner
188	10111100	274	bc	╝	Box drawing character double line lower right corner
189	10111101	275	bd	¢	Cent symbol
190	10111110	276	be	¥	YEN and YUAN sign
191	10111111	277	bf	┐	Box drawing character single line upper right corner
192	11000000	300	c0	└	Box drawing character

					single line lower left corner
193	11000001	301	c1	┴	Box drawing character single line horizontal and up
194	11000010	302	c2	┬	Box drawing character single line horizontal down
195	11000011	303	c3	├	Box drawing character single line vertical and right
196	11000100	304	c4	─	Box drawing character single horizontal line
197	11000101	305	c5	┼	Box drawing character single line horizontal vertical
198	11000110	306	c6	ã	Lowercase letter a with tilde or a-tilde
199	11000111	307	c7	Ã	Capital letter A with tilde or A-tilde
200	11001000	310	c8	╚	Box drawing character double line lower left corner
201	11001001	311	c9	╔	Box drawing character double line upper left corner
202	11001010	312	ca	╩	Box drawing character double line horizontal and up

203	11001011	313	cb	╦	Box drawing character double line horizontal down
204	11001100	314	cc	╠	Box drawing character double line vertical and right
205	11001101	315	cd	═	Box drawing character double horizontal line
206	11001110	316	ce	╬	Box drawing character double line horizontal vertical
207	11001111	317	cf	¤	Generic currency sign
208	11010000	320	d0	ð	Lowercase letter eth
209	11010001	321	d1	Ð	Capital letter Eth
210	11010010	322	d2	Ê	Letter E with circumflex accent or E-circumflex
211	11010011	323	d3	Ë	Letter E with umlaut or diaeresis, E-umlaut
212	11010100	324	d4	È	Capital letter E with grave accent
213	11010101	325	d5	ı	Lowercase dot less i
214	11010110	326	d6	Í	Capital letter I with acute accent or I-acute
215	11010111	327	d7	Î	Letter I with circumflex accent or I-circumflex
216	11011000	330	d8	Ï	Letter I with umlaut or

					diaeresis ; I-umlaut
217	11011001	331	d9	┘	Box drawing character single line lower right corner
218	11011010	332	da	┌	Box drawing character single line upper left corner
219	11011011	333	db	▉	Block, graphic character
220	11011100	334	dc	▄	Bottom half block
221	11011101	335	dd	¦	Vertical broken bar
222	11011110	336	de	Ì	Capital letter I with grave accent
223	11011111	337	df	▀	Top half block
224	11100000	340	e0	Ó	Capital letter O with acute accent or O-acute
225	11100001	341	e1	ß	Letter Eszett ; scharfes S or sharp S
226	11100010	342	e2	Ô	Letter O with circumflex accent or O-circumflex
227	11100011	343	e3	Ò	Capital letter O with grave accent
228	11100100	344	e4	õ	Lowercase letter o with tilde or o-tilde
229	11100101	345	e5	Õ	Capital letter O with tilde or O-tilde
230	11100110	346	e6	µ	Lowercase letter Mu ; micro sign or micron

231	11100111	347	e7	þ	Lowercase letter Thorn
232	11101000	350	e8	Þ	Capital letter Thorn
233	11101001	351	e9	Ú	Capital letter U with acute accent or U-acute
234	11101010	352	ea	Û	Letter U with circumflex accent or U-circumflex
235	11101011	353	eb	Ù	Capital letter U with grave accent
236	11101100	354	ec	ý	Lowercase letter y with acute accent
237	11101101	355	ed	Ý	Capital letter Y with acute accent
238	11101110	356	ee	¯	Macron symbol
239	11101111	357	ef	´	Acute accent
240	11110000	360	f0	≡	Congruence relation symbol
241	11110001	361	f1	±	Plus-minus sign
242	11110010	362	f2	‗	underline or underscore
243	11110011	363	f3	¾	three quarters, three-fourths
244	11110100	364	f4	¶	Paragraph sign or pilcrow ; end paragraph mark
245	11110101	365	f5	§	Section sign
246	11110110	366	f6	÷	The division sign ; Obelus
247	11110111	367	f7	¸	cedilla
248	11111000	370	f8	°	Degree symbol
249	11111001	371	f9	¨	Diaresis

250	11111010	372	fa	·	Interpunct or space dot
251	11111011	373	fb	¹	Superscript one, exponent 1, first power
252	11111100	374	fc	³	Superscript three, exponent 3, cube, third power
253	11111101	375	fd	²	Superscript two, exponent 2, square, second power
254	11111110	376	fe	■	black square
255	11111111	377	ff	nbsp	Non-breaking space or no-break space

RIWAYAT HIDUP

Rafika Zahrotul Fauziah, lahir di Kediri, 11 Juni 2000. Bertempat tinggal di Dusun Blawe Kulon, Desa Blawe, Kecamatan Purwoasri, Kabupaten Kediri. Putri dari pasangan Ayah Amin dan Ibu Nur Kholidah. Merupakan anak kedua dari 3 bersaudara dengan kakak laki-laki bernama Alfin Baihaqi Asror dan adik perempuan bernama Cahaya Fatiha Mughnia. Pendidikan dasar yang ditempuh di SD Negeri Blawe lulus pada tahun 2013, kemudian melanjutkan Pendidikan menengah pertama di SMP Negeri 1 Kunjang dan lulus pada tahun 2016. Setelah itu melanjutkan Pendidikan menengah atas di MA Negeri Purwoasri atau yang sekarang dikenal sebagai MA Negeri 2 Kediri dan lulus pada tahun 2019. Melanjutkan menempuh Pendidikan Tinggi di Universitas Islam Negeri Maulana Malik Ibrahim Malang pada tahun 2019 melalui SNMPTN pada Program Studi MAtematika di Fakultas Sains dan Teknologi.

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

BUKTI KONSULTASI SKRIPSI

Nama : Rafika Zahrotul Fauziah
NIM : 19610014
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Implementasi Affine Cipher dan Algoritma Goldbach Code dalam Mengamankan Pesan Teks
Pembimbing I : Muhammad Khudzaifah, M.Si.
Pembimbing II : Erna Herawati, M.Pd.

No	Tanggal	Hal	Tanda Tangan
1.	14 Desember 2022	Konsultasi Topik Skripsi	1.
2.	7 Maret 2023	Konsultasi Perhitungan Bab IV	2.
3.	4 April 2023	Konsultasi Bab I, II, dan III	3.
4	10 April 2023	Konsultasi Kajian Agama Bab I dan II	4.
5.	10 April 2023	ACC Bab I, II, dan III	5.
6.	11 April 2023	Konsultasi Revisi Kajian Agama Bab I dan II	6.
7.	16 Mei 2023	ACC Kajian Agama Bab I dan II	7.
8.	21 Juli 2023	ACC Seminar Proposal	8.
9.	11 September 2023	Konsultasi Revisi Seminar Proposal	9.
10.	9 Oktober 2023	Konsultasi Bab IV dan V	10.
11.	9 Oktober 2023	Konsultasi Kajian Agama Bab IV	11.
12.	12 Oktober 2023	Konsultasi Revisi Kajian Agama Bab IV	12.
13.	24 Oktober 2023	ACC Bab IV dan V	13.
14.	26 Oktober 2023	ACC Kajian Agama Bab IV	14.
15.	22 November 2023	ACC Seminar Hasil	15.

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

16.	7 Desember 2023	Konsultasi Revisi Seminar Hasil	16.
17.	21 Desember 2023	ACC Sidang Skripsi	17.
18	26 Desember 2023	ACC Keseluruhan	18.

Malang, 26 Desember 2023
Mengetahui,
Ketua Program Studi Matematika

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