PENERAPAN KOMPRESI MENGGUNAKAN KODE HUFFMAN PADA ALGORITMA RSA (*RIVEST SHAMIR ADLEMAN*) UNTUK MENYANDIKAN PESAN TEKS

SKRIPSI

OLEH
ANDINI KHAIRUNNISA
NIM. 18610048

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

PENERAPAN KOMPRESI MENGGUNAKAN KODE HUFFMAN PADA ALGORITMA RSA (*RIVEST SHAMIR ADLEMAN*) UNTUK MENYANDIKAN 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
Andini Khairunnisa
NIM. 18610048

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

PENERAPAN KOMPRESI MENGGUNAKAN KODE HUFFMAN PADA ALGORITMA RSA (*RIVEST SHAMIR ADLEMAN*) UNTUK MENYANDIKAN PESAN TEKS

SKRIPSI

Oleh
Andini Khairunnisa
NIM. 18610048

Telah Disetujui untuk Diuji
Malang, 14 Desember 2022

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah,M.Si	Erna Herawati,M.Pd
NIDT.19900511201608011057	NIDT.19760723 2018021 222

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 197411292000122005

PENERAPAN KOMPRESI MENGGUNAKAN KODE HUFFMAN PADA ALGORITMA RSA (*RIVEST SHAMIR ADLEMAN*) UNTUK MENYANDIKAN PESAN TEKS

SKRIPSI

Oleh
Andini Khairunnisa
NIM. 18610048

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

Tanggal 28 Desember 2022

Ketua Penguji	: Evawati Alisah, M.Pd	.....
Anggota Penguji I	: Hisyam Fahmi, M.Kom	.....
Anggota Penguji II	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji III	: Erna Herawati, M.Pd	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	: Andini Khairunnisa
NIM	: 18610048
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Penerapan Kompresi Menggunakan Kode Huffman pada Algoritma RSA (Rivers Shamir Adleman) untuk Menyandikan Pesan Teks.

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, 28 Desember 2022
Yang membuat pernyataan

Andini Khairunnisa
NIM. 18610048

MOTTO DAN PERSEMBAHAN

"Apapun yang menjadi takdirmu, akan mencari jalannya menemukanmu"

(Ali bin Abi Thalib**)**

Skripsi ini penulis persembahkan untuk :

Kedua orang tua penulis Bapak Setu Udoyono dan Ibu Etik Hendartik yang mendoakan dan mendukung seiring proses mengerjakan skripsi ini. Adik penulis Aninda Khairunnisa dan Ilham Abdillah yang senantiasa memberikan motivasi dan semangat.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt atas rahmat, taufik serta hidayah-nya, sehingga penulis mampu menyelesaikan penyusunan skripsi yang berjudul Penerapan Kode huffman Menggunakan Algoritma RSA (*Rivest Shamir Adleman*) Pada Pesan Teks, sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

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

1. Prof. Dr. H. M. Zainuddin, M.A, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
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 membimbing, memberikan arahan dan nasihat kepada penulis.
5. Erna Herawati, M.Pd, selaku dosen pembimbing II yang telah memberikan bimbingan, pengalaman yang berharga kepada penulis.
6. Evawati Alisah, M.Pd, selaku dosen ketua penguji dalam ujian skripsi dan telah memberikan bimbingan dan pengarahan kepada penulis.

7. Hisyam Fahmi, M.Kom, selaku dosen anggota penguji I dalam ujian skripsi dan telah memberikan bimbingan dan pengarahan kepada penulis.
8. Seluruh dosen Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim
9. Kedua orang tua tercinta, Bapak Yono dan Ibu Etik beserta adik penulis yang selalu memberikan semangat dan motivasi kepada penulis hingga saat ini.
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, 28 Desember 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Khairunnisa, Andini.2022. **Penerapan Kompresi Menggunakan Kode Huffman Pada Algoritma RSA (Rivers Shamir Adleman) untuk Menyandikan 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: Kode ASCII, Kode Huffman, RSA

Penyandian suatu pesan yang bersifat rahasia dilakukan dengan ilmu kriptografi yaitu mengubah suatu pesan kedalam bentuk yang tidak dapat dipahami lagi maknanya. Untuk menghindari hal yang tidak diinginkan dalam menyampaikan suatu pesan yang bersifat rahasia, maka penulis akan mengkaji dan membahas tentang kriptografi atau penyandian suatu pesan. Penyandian pesan teks dengan kompresi menggunakan kode Huffman dan kode ASCII akan diterapkan pada algoritma RSA, supaya dapat mengetahui kode mana yang lebih efisien dalam proses penyandian suatu pesan teks. Setelah melakukan beberapa uji coba maka dapat disimpulkan bahwa kode Huffman dapat menghasilkan ruang penyimpanan relatif kecil dalam proses penyandian daripada menggunakan kode ASCII. Rata-rata Perbedaannya ruang penyimpanan dalam kode Huffman 39,53% lebih kecil daripada kode ASCII.

ABSTRACT

Khairunnisa, Andini. 2022. **Application of Compression Using Huffman Codes in the RSA (Rivers Shamir Adleman) Algorithm for Encrypting Text Messages.** Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisor: (I) Muhammad Khudzaifah, M.Si (II) Erna Herawati, M.Pd

Keywords: ASCII Code, Huffman Code, RSA

Encryption of a message that is confidential is done with the science of cryptography, namely changing a message into a form whose meaning can no longer be understood. To avoid unwanted things in conveying a message that is confidential, the author will examine and discuss cryptography or encoding a message. Encryption of text messages with compression using Huffman codes and ASCII codes will be applied to the RSA algorithm, so that we can find out which code is more efficient in the process of encoding a text message. After conducting several trials, it can be concluded that the Huffman code can produce relatively small storage space in the encoding process than using ASCII code. The average difference is that the storage space in the Huffman code is 39.53% less than in the ASCII code.

مستخلص البحث

خير النساء، أنديني. ٢٠٢٢. **تطبيق الضغط باستخدام ترميز هوفمان باستخدام على خوارزمية ريفست وشامير** وأدلمان *(Rivers Shamir Adleman)* **لتشفير الرسائل النصية**. البحث الجامعي. قسم الرياضيات، كلية العلوم والتكنولوجيا بجامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف الأول: محمد حذيفة، الماجستير. المشرف الثاني: إيرنا هيرواتي، الماجستير

الكلمات الرئيسية: ترميز أسكي، ترميز هوفمان، ريفست وشامير وأدلمان.

يتم تشفير رسالة سرية باستخدام علم التشفير ، يمعي تغيير الرسالة إلى شكل لم يكن لفهمه معنها. لتجنب الأشياء غير المرغوب فيها في نقل رسالة سرية ، سيقوم المؤلف بفحص ومناقشة التشفير أو تشفير الرسالة. سيتم تطبيق تشفير الرسائل النصية بالضغط باستخدام أكواد *Huffman* ورموز *ASCII* على خوارزمية *RSA* ، حتى نتمكن من معرفة الرمز الأكثر كفاءة في عملية تشفير رسالة نصية. بعد إجراء العديد من التجارب ، يمكن استنتاج أن كود *Huffman* يمكن أن ينتج مساحة تخزين صغيرة نسبيًا في عملية التشفير مقارنة باستخدام كود *ASCII*الفرق المتوسط هو أن مساحة التخزين في كود هوفمان أقل بنسبة ٣٩,٥٣٪ من كود*ASCII*.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi pada zaman modern ini sangat mempengaruhi dalam berbagai aspek kehidupan. Perkembangan teknologi yang pesat dapat memberikan banyak manfaat terutama pada bidang komunikasi. Pesatnya teknologi menggunakan dasar ilmu matematika untuk memberikan kemudahan dalam menyampaikan sebuah pesan. Salah satu dasar ilmu matematika yaitu kriptografi yang menggunakan sistem aritmatika modulo sebagai peranan penting dalam aplikasi kriptografi. Banyak dokumen serta pesan yang bersifat rahasia membutuhkan keamanan yang tepat (Munir, 2019). Salah satu cara yang dapat kita lakukan dalam mengamankan sebuah pesan yaitu dengan cara menyandikan kode-kode yang tidak dapat dipahami oleh pihak yang tidak bertanggung jawab.

Kriptografi merupakan ilmu untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dipahami lagi maknanya (Munir, 2019). Kriptografi termasuk salah satu bidang matematika yang berkaitan untuk menjaga keamanan data seperti informasi pada sebuah pesan rahasia dan keaslian data. Dalam menjaga keamanan data kriptografi menyembunyikan atau menyamarkan sebuah pesan agar tidak dapat di pahami oleh pihak yang tidak bertanggung jawab dengan mengubah informasi tersebut menjadi sandi dengan menggunakan kunci. Kriptografi mempunyai berbagai macam algoritma yang dapat dipelajari, salah satunya yaitu algoritma RSA (*Rivest Shamir Adleman*).

Algoritma RSA merupakan salah satu algoritma asimetri yang dapat digunakan untuk mengamankan pesan. Penemu Algoritma RSA ini berasal dari

MIT (*Massachussets Institute of Technology*) yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976(Munir, 2009). Algoritma RSA menggunakan bilangan prima dan aritmatika modulo dalam proses enkripsi dan dekripsi. Proses enkripsi pada Algoritma RSA ini bersifat umum dan proses dekripsi Algoritma RSA bersifat rahasia. Keamanan Algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima (Munir, 2019). Kesulitan memfaktorkan bilangan tersebut dapat mengukur kekuatan Algoritma RSA menjadi lebih kuat keamanannya. Dengan kesulitan Algoritma RSA tersebut algoritma ini terdapat kelemahan yaitu kecepatannya lebih lambat dari pada algoritma kriptografi kunci yang lainnya (Munir, 2019).

Kode Huffman merupakan salah satu algoritma yang ditemukan oleh peneliti asal MIT (*Massachussets Institute of Technology*) yaitu David A. Huffman. Kode Huffman adalah salah satu algoritma dasar yang dapat digunakan untuk kompresi data dengan mengurangi jumlah bit yang diperlukan untuk merepresentasikan informasi atau pesan (Heru Nugroho, 2015). Kompresi data pada kode Huffman ini dapat dilakukan dengan mengkodekan informasi atau pesan secara singkat sehingga kecepatan pengiriman pesan relatif singkat dalam ruang penyimpanan yang relatif sedikit. Kode Huffman merupakan algoritma yang menggunakan metode statik, yaitu pemetaan kode yang sama.

Penelitian Albert Ginting (2015) menyatakan bahwa penggunaan algoritma RSA saja dalam melakukan proses enkripsi dan dekripsi memiliki kelemahan dalam kecepatan waktu pengiriman pesan karena semakin besar bilangan yang akan difaktorkan, semakin lama waktu yang dibutuhkan. Dalam penelitian Erna Zuni Astuti dan Erwin Yudi Hidayat (2013) menyatakan bahwa

kode Huffman cukup baik digunakan untuk mengompres pesan yang dikirim dengan ukuran yang terlalu besar sehingga membutuhkan tempat penyimpanan yang terlalu besar. Dengan demikian juga pesan yang terlalu besar, akan membutuhkan ruang penyimpanan yang lebih lama bila dibandingkan dengan pesan yang berukuran relatif lebih kecil. Kemudian pada penelitian Shofwan Ali Fauzi (2016) menyatakan bahwa dalam penggunaan algoritma RSA tidak cukup hanya menggunakan kode ASCII dalam proses penyandian pesan. Hal ini dikarenakan dalam menggunakan kode ASCII dapat menghasilkan ukuran yang relatif besar, sehingga dibutuhkan kode tambahan dalam proses pengiriman pesan dengan ukuran yang relatif lebih kecil.

Proses kode Huffman menggunakan kriptografi diterapkan pada algoritma RSA untuk mengamankan sebuah pesan yang dikirim oleh pengirim pesan. Pengirim pesan harus menjaga pesan yang bersifat rahasia tersebut dari pihak yang tidak seharusnya menerima pesan tersebut, sebagaimana dalam ajaran agama Islam telah mengajarkan kita tentang menjaga rahasia. Dalam menjaga pesan atau informasi yang bersifat rahasia adalah salah satu contoh dalam menjaga amanah yang telah diberikan. Dalam Al-Quran telah menjelaskan bahwa kita sebagai umat muslim untuk saling menjaga amanah yang terdapat dalam surat Al-Mu'minun ayat 8:

Artinya: "Dan orang-orang yang memelihara amanat-amanat (yang dipikulnya) dan janjinya"(Q.S Al-Mu'minun:8).

Berdasarkan ayat tersebut menjelaskan bahwa dalam memelihara sesuatu yang diamanatkan dalam berbentuk ucapan atau perbuatan yang harus dijaga dan ditepati. Apabila seseorang menyampaikan sesuatu yang penting dan rahasia

kepada orang lain, hal itu merupakan bentuk amanah sederhana yang harus dijaga oleh orang tersebut. Sabda Rasulullah SAW:

قَالَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ إِذَا حَدَّثَ الرَّجُلُ بِالْحَدِيثِ ثُمَّ الْتَفَتَ فَهِيَ أَمَانَةٌ(رواه أبو داودا)

Artinya:"Apabila seseorang membicarakan sesuatu kepada orang lain (sambil) menoleh ke kiri dan ke kanan (karena yang dibicakan itu rahasia) maka itulah amanah (yang harus dijaga)"[H.R. Abu Dawud].

Amanah pesan yang dikirimkan pengirim pesan bersifat rahasia kepada penerima pesan, sehingga berdasarkan permasalahan di atas, solusi untuk mengamankan informasi atau pesan agar lebih kuat yaitu dengan menerapkan kode Huffman pada algoritma RSA. Penerapan kompresi menggunakan kode Huffman pada algoritma RSA (*Rivest Shamir Adleman*) untuk menyandikan pesan teks pada pesan teks ini diharapkan dapat mengamankan pesan dengan kuat dan efektif.

1.2 Rumusan Masalah

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

1. Bagaimana proses enkripsi pesan menggunakan algoritma RSA dan proses kompresi menggunakan kode Huffman?
2. Bagaimana proses dekripsi pesan menggunakan algoritma RSA dan proses dekompresi menggunakan kode Huffman?
3. Bagaimana efisiensi kompresi kode Huffman menggunakan algoritma RSA untuk menyandikan pesan teks?

1.3 Tujuan Penelitian

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

1. Mengetahui proses enkripsi pesan menggunakan algoritma RSA dan proses kompresi menggunakan kode Huffman.
2. Mengetahui proses enkripsi pesan menggunakan algoritma RSA dan proses kompresi menggunakan kode Huffman.
3. Mengetahui efisiensi kompresi kode Huffman menggunakan algoritma RSA untuk menyandikan pesan teks.

1.4 Manfaat Penelitian

Penulis berharap penelitian ini dapat memberikan manfaat sebagai berikut:

1. Menambah pengetahuan tentang konsep matematis yang melandasi kode Huffman pada algoritma RSA, sehingga mengetahui metode yang dapat digunakan untuk enkripsi dan dekripsi pesan teks.
2. Memberikan informasi mengenai kriptografi dalam keamanan informasi atau pesan.
3. Memperoleh pengetahuan tentang kriptografi yang berkaitan dengan kode Huffman pada algoritma RSA (*Rivest Shamir Adleman*) sebagai media pembelajaran khususnya bagi mahasiswa.

1.5 Batasan Masalah

Batasan masalah pada penelitian ini yaitu kunci yang digunakan untuk enkripsi algoritma RSA yaitu huruf alfabet A-Z dengan panjang karakter bilangan genap 8-16 untuk membagi digit blok pesan teks menjadi 4 digit per blok.

1.6 Definisi Istilah

1. Plainteks merupakan sebuah pesan yang akan di acak kedalam bahasa yang tidak dapat dipahami.
2. Cipherteks merupakan sebuah pesan yang telah di acak kedalam bahasa yang tidak dapat dipahami.
3. Enkripsi merupakan proses menyandikan pesan asli kedalam pesan yang tidak dapat dipahami oleh pihak yang tidak dapat menerima pesan rahasia tersebut.
4. Dekripsi merupakan kebalikan dari enkripsi yaitu mengembalikan pesan yang tidak dapat dipahami tersebut kedalam pesan yang dapat terbaca.
5. Kompresi merupakan suatu teknik untuk memperkecil jumlah ukuran data dari data aslinya.

BAB II
KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Keterbagian

Definisi 1

Misalkan $a, b \in \mathbb{Z}$ dengan a $\neq 0$, maka a disebut membagi b, ditulis sebagai $a|b$ apabila $b = ak$, untuk suatu $k \in \mathbb{Z}$ (Wahyu Henky Irawan, 2014). Berdasarkan definisi keterbagian tersebut maka beberapa hal yang dapat di ambil yaitu:

1. $1|x$, untuk setiap $x \in \mathbb{Z}$, sebab terdapat $x \in \mathbb{Z}$ maka $x = 1 \cdot x$
2. $x|0$, untuk setiap $x \in \mathbb{Z}$, dengan $x \neq 0$, sebab terdapat $0 \in \mathbb{Z}$ maka
$$0 = x \cdot 0$$
3. $x|x$, untuk setiap $x \in \mathbb{Z}$, dengan $x \neq 0$, sebab terdapat $1 \in \mathbb{Z}$ maka
$$x = x \cdot 1$$
4. $x|(-x)$, untuk setiap $x \in \mathbb{Z}$, dengan $x \neq 0$, sebab terdapat $-1 \in \mathbb{Z}$ maka $-x = x \cdot -1$

Contoh

- $3|15$, sebab terdapat $5 \in \mathbb{Z}$ maka $15 = 3 \cdot 5$
- $3|18$, sebab terdapat $6 \in \mathbb{Z}$ maka $18 = 3 \cdot 6$
- $5|45$, sebab terdapat $9 \in \mathbb{Z}$ maka $45 = 5 \cdot 9$

Teorema 1

Jika $p, q \in \mathbb{Z}$ dan $p|q$, maka $p|qr$ untuk setiap $r \in \mathbb{Z}$

Bukti

Karena $p|q$, maka terdapat x $\in \mathbb{Z}$, sehingga $q = px$

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

$$q \cdot r = (p \cdot x)r = p(xr)$$

Jadi, $q \cdot r = p \cdot y$ untuk sebarang $y = x \cdot r \in \mathbb{Z}$

Dengan demikian $p|qr$, untuk setiap $r \in \mathbb{Z}$

Teorema 2

Jika p, q , r $\in \mathbb{Z}$, $p|q$ dan $q|r$, maka $p|r$

Bukti

Karena $p|q$, maka $q =$ px, terdapat $x \in \mathbb{Z}$ dan $q|r$, maka $r = qy$, terdapat

$y \in \mathbb{Z}$. Jadi , $r = q \cdot y = (px)y = p(xy)$, terdapat xy $\in \mathbb{Z}$

Dengan demikian $p|r$

Teorema 3

Jika $p, q, r \in \mathbb{Z}$, $p|q$ dan $q|r$, maka $p = \pm q$

Bukti

Karena $p|q$, maka $q = p \cdot x$, terdapat $x \in \mathbb{Z}$ dan $q|p$, maka $p = q \cdot y$ terdapat

$y \in \mathbb{Z}$. Dengan demikian $q = (qy)x = q(yx) = q(xy)$ dan

$p = (px)y = p(xy)$. Karena $q = q(xy)$ dan $p = p(xy)$, maka $xy = 1$

Oleh karena itu $x = 1$ dan $y = 1$ atau $x = -1$ dan $y = -1$

Jika $x = 1$ dan $y = 1$, maka $p = q$ dan jika $x = -1$ dan $y = -1$, maka $p = -q$

Sehingga terbukti bahwa $p = \pm q$

Teorema 4

Jika $p, q, r \in \mathbb{Z}$, $p|q$ dan $p|r$, maka $p|q + r$

Bukti

Karena $p|q$, maka $q = p \cdot x$, terdapat $x \in \mathbb{Z}$ dan $p|r$, maka $r = p \cdot y$ terdapat

$y \in \mathbb{Z}$. Jadi $q + r = (px) + (py) = p(x + y)$ dengan $x + y \in \mathbb{Z}$

Dengan demikian $p|q+r$

Teorema 5

Jika p, q , r $\in \mathbb{Z}$, $p|q$ dan $p|r$, maka $p|qx+ry$, untuk setiap $x, y \in \mathbb{Z}$ (Bentuk $qx+ry$ disebut kombinasi linier dari q dan r).

Bukti

Karena $p|q$, maka $q = p \cdot a$, terdapat $a \in \mathbb{Z}$ dan $p|r$, maka $r = p \cdot b$ terdapat $b \in \mathbb{Z}$. Jadi untuk sebarang $x, y \in \mathbb{Z}$ berlaku

$$\begin{aligned} qx+ry &= (pa)x+(pb)y \\ &= p(ax)+p(by) \\ &= p(ax+by) \end{aligned}$$

Dengan demikian $p|qx+ry$, untuk setiap $x, y \in \mathbb{Z}$

2.1.2 Aritmatika Modulo

Definisi 2

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a \, mod \, m$ (dibaca 'a modulo m') memberikan sisa jika a dibagi dengan m. Dengan kata lain $a \, mod \, m = r$ sedemikian sehingga $a = mq + r$ dengan $0 \leq r < m$ (Munir, 2009).

Beberapa contoh operator modulo sebagai berikut:

1. $27 \, mod \, 3 = 0$, sebab apabila a kelipatan dari m maka a habis dibagi dengan m sehingga hasilnya 0 atau dapat ditulis $a \, mod \, m = 0$
2. $21 \, mod \, 5 = 1$, sebab 21 dibagi 5 dengan hasil $q = 4$ dan sisa $r = 1$ sehingga dapat ditulis $21 = 5 \cdot 4 + 1$

3. $39\ mod\ 2 = 1$, sebab 39 dibagi 2 dengan hasil $q = 19$ dan sisa $r = 1$ sehingga dapat ditulis $39 = 2 \cdot 19 + 1$

2.1.3 Kongruensi

Definisi 3

Misalkan n bilangan bulat positif dan x, y adalah bilangan-bilangan bulat dengan sifat n membagi $x - y$, kita katakan bahwa x kongruen dengan y modulo n , dan ditulis $x \equiv y(mod\ n)$. Jika n tidak membagi $x - y$, kita katakan x tidak kongruen dengan y modulo n, dan ditulis $x \not\equiv y(mod\ n)$ (Taufik, 1999). Jika $n > 0$ dan $n|a - b$ maka terdapat suatu bilangan bulat t sehingga $a - b = nt$.

Contoh

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

Teorema 6

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

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

Bukti

1. Menurut definisi 3 berlaku $a \equiv a\ (mod\ n)$ yang berarti $n|a - a$. Jika $n \neq 0$ maka $n|0$ sebab $a - a = 0$
2. Berdasarkan definisi 3 Jika $a \equiv b\ (mod\ n)$berarti $n|a - b$ menurut definisi ada keterbagian bilangan bulat demikian t sehingga dapat dinyatakan

$$a - b = tn$$

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

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

Menurut definisi , ini berarti $b \equiv a \ (mod\ n)$

3. Menurut definisi 3 $a \equiv b \ (mod\ n)$ yang berarti $n|a - b$ dan $b \equiv c \ (mod\ n)$ yang berarti $n|b - c$ terdapat bilangan bulat t_1 dan t_2 sehingga:

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

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

   Kedua persamaan dijumlahkan sehingga dapat diperoleh

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

   Ini berarti menurut definisi 3 menjadi $a \equiv c \ (mod\ n)$

Teorema 7

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

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

Bukti

1. Berdasarkan definisi 3 $a \equiv b \ (mod\ n)$, maka $n|a - b$, menurut definisi 3 ada bilangan bulat t sehingga $a - b = tn$

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

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

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

   Sehingga berdasarkan definisi 3 diperoleh $a + c \equiv b + c (mod\ n)$

2. Menurut definisi 3 $a \equiv b \ (mod\ n)$ maka $n|a - b$, menurut definisi 3 ada bilangan t sehingga $a - b \ = tn$

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

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

Sehingga diperoleh $ac \equiv bc \ (mod\ n)$

2.1.4 Bilangan Prima

Bilangan prima merupakan bilangan bulat positif yang hanya habis dibagi oleh 1 dan dirinya sendiri (Munir, 2009). Bilangan prima mempunyai 2 pembagi yaitu 1 dan dirinya sendiri, sedangkan bilangan yang mempunyai lebih dari 2 pembagi disebut bilangan komposit. Bilangan prima juga merupakan bilangan bulat positif yang dapat digunakan dalam ilmu komputer salah satu ilmu tersebut yaitu kriptografi.

Definisi 4

Sebuah bilangan bulat $p > 1$ disebut bilangan prima, jika tidak ada pembagi d dari p yang memenuhi $1 < p < d$. Jika sebuah bilangan bulat $p > 1$ bukan bilangan prima, maka p dinamakan bilangan komposit (Wahyu Henky Irawan, 2014).

Cara untuk menentukan bahwa p bilangan prima atau bilangan komposit yaitu membagi p dengan bilangan prima itu sendiri contohnya pada angka 2, 3, 5 adalah bilangan prima karena mempunyai 2 pembagi yaitu 1 dan dirinya sendiri sedangkan 6, 8, 10 adalah bilangan komposit karena mempunyai lebih dari 2 pembagi seperti 6 mempunyai 4 pembagi yaitu 1, 2, 3, dan 6.

Teorema 8 (Teorema Euler)

Jika n adalah sebuah bilangan *integer* positif dan a adalah bilangan *integer* positif yang relatif prima terhadap n maka

$$a^{\phi(n)} \equiv 1(mod\ n)$$

Teorema Euler dapat juga diekspresikan dalam persamaan:

$$a^{\phi(n)+1} \equiv a(mod\ n)$$

Algoritma penyandian kunci publik RSA bersandar pada teorema Euler. Pada RSA hal pertama yang dilakukan adalah menetapkan 2 bilangan prima p dan q lalu tetapkan $n = pq$. Kemudian pilih m dengan $0 < m < n$ dan k sebarang *integer* maka berlaku:

$$m^{k\phi(n)+1} \equiv \left[\left(m^{\phi(n)}\right)^k \times m\right] mod\ n$$

$$\equiv [(1)^k \times m] mod\ n \text{ (Berdasarkan teorema Euler)}$$

$$\equiv \text{m mod n (Sadikin, 2012)}$$

Teorema 9 (Teorema Fermat)

Jika p adalah sebuah bilangan prima dan a adalah bilangan *integer* positif yang tidak habis dibagi p maka $a^{p-1} \equiv 1(mod\ p)$. (Sadikin, 2012)

Bukti

Karena p adalah suatu bilangan prima dengan $p \nmid a$, maka $(p, a) = 1$,

(jika $(p, a) \neq 1$) yaitu p dan a tidak relatif prima, maka p dan a mempunyai faktor selain 1 dan p, selanjutnya karena $(p, a) = 1$ maka untuk $a^{\phi(p)} \equiv 1(mod\ p)$ maka p merupakan bilangan prima artinya dari bilangan bulat $\{0,1,2,3, \dots, p-1\}$ hanya 0 yang tidak relatif prima, sehingga $\{1,2,3, \dots, p-1\}$. Dengan demikian

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

sehingga karena $\phi(p) = p - 1$ dan $a^{\phi(p)} \equiv 1(mod\ p)$, maka $a^{p-1} \equiv 1(mod\ p)$.

2.1.5 Pohon Biner

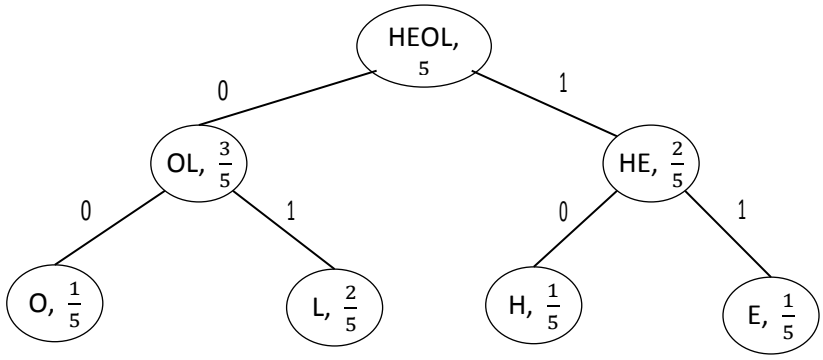
Pohon biner adalah pohon yang setiap simpul cabangnya mempunyai paling banyak 2 buah anak yaitu anak kiri ($left\ child$) dan anak kanan ($right\ child$) (Munir, 2009). Pada pohon biner terdapat akar pada masing-masing anak diantaranya pada pohon sebelah kiri disebut upapohon kiri, sedangkan pada pohon sebelah kanan disebut upapohon kanan sehingga perbedaan akar pada masing-masing anak pohon biner disebut pohon terurut.

Pohon biner juga disebut pohon condong apabila terdapat simpul yang terletak pada 1 arah yaitu kanan atau kiri saja. Pohon yang cenderung condong ke kanan disebut pohon condong-kanan, sedangkan pohon yang cenderung condong ke kiri disebut pohon condong-kiri. Pohon biner sangat berperan penting dalam ilmu komputer salah satunya yaitu kriptografi. Salah satu penerapan pohon biner pada kriptografi yaitu kode Huffman.

2.1.6 Kode Huffman

Kode Huffman merupakan kode biner yang diterapkan pada ilmu komputer salah satunya yaitu kriptografi. Kode Huffman menggunakan metode statik yaitu memetakan kode yang sama dengan menghitung peluang kemunculan tiap karakter dalam teks.Kode Huffman juga merupakan salah satu algoritma yang ditemukan oleh peneliti asal MIT (*Massachussets Institute of Technology*) yaitu David A. Huffman. Kode Huffman adalah salah satu algoritma dasar yang dapat

digunakan untuk kompresi data dengan mengurangi jumlah bit yang diperlukan untuk merepresentasikan informasi atau pesan (Heru Nugroho, 2015). Kompresi data pada kode Huffman ini dapat dilakukan dengan mengkodekan informasi atau pesan secara singkat sehingga kecepatan pengiriman pesan relatif singkat dalam ruang penyimpanan yang relatif sedikit. Cara mendapatkan kode Huffman yaitu dengan memetakan urutan simbol yang jumlahnya paling banyak sampai paling sedikit. Berikut contoh kode Huffman yang dibentuk dengan menggunakan pohon Huffman sebagai berikut:



Gambar 2.1 Pohon Huffman untuk Pesan 'HELLO'

Berdasarkan gambar pohon Huffman diatas maka hasil kode Huffman

Tabel 2. 1 Hasil Kode Huffman untuk Pesan 'HELLO'

Simbol	Kekerapan	Peluang	Kode Huffman	Kekerapan × jumlah kode Huffman
H	1	$\frac{1}{5}$	10	2
E	1	$\frac{1}{5}$	11	2
L	2	$\frac{2}{5}$	01	4

O	1	$\frac{1}{5}$	00	2
Total				10

Pada penggunaan kode Huffman ini, jumlah bit yang dihasilkan pada pesan ‘HELLO’ yaitu 10 bit, sedangkan jika menggunakan kode ASCII pada pesan ‘HELLO’ yaitu sebagai berikut:

H = 01001000 E = 01000101 L = 01001100

L = 01001100 O = 01001111

Sehingga jika menggunakan kode ASCII pada pesan ‘HELLO’yaitu $5\,x\,8 = 40$ bit. Berikut langkah-langkah pembentukkan kode Huffman sebagai berikut:

1. Pilih 2 simbol yang memiliki peluang paling kecil yaitu simbol H dan E. simbol yang sudah dipilih menjadi simpul orang tua menjadi HE dengan peluang $\frac{1}{5} + \frac{1}{5} = \frac{2}{5}$ sebagai jumlah peluang untuk anaknya yaitu simbol H dan E. simbol yang dihasilkan akan menjadi simbol baru yang akan digunakan untuk mencari simbol dengan peluang paling kecil.
2. Pilih 2 simbol berikutnya yaitu simbol O dan L. kedua simbol tersebut menjadi simbol orang tua menjadi OL yang memiliki peluang $\frac{1}{5} + \frac{2}{5} = \frac{3}{5}$
3. Pilih 2 simbol orang tua yang telah dihasilkan yaitu HE dan OL menjadi simbol baru yaitu HEOL dengan peluang $\frac{2}{5} + \frac{3}{5} = \frac{5}{5}$ yang merupakan akar dari pohon.

Berdasarkan gambar kode Huffman terdapat daun yang digunakan untuk menyatakan simbol pada pesan. Kode setiap simbol dengan memberi label 0 pada

setiap cabang sisi kiri dan label 1 untuk cabang sisi kanan (Munir, 2009). Berikut ini proses kompresi (*encoding)* dan dekompresi (*decoding*) pada kode Huffman sebagai berikut:

1. Kompresi

   Kompresi (*encoding*) merupakan suatu teknik untuk memperkecil jumlah ukuran data dari data aslinya. Proses kompresi dilakukan dengan membuat pohon Huffman pada setiap karakter. Dalam proses *encoding* pohon Huffman dapat menyusun string biner pada setiap karakter dari akar hingga daun.

   Berikut langkah-langkah encoding pohon Huffman sebagai berikut:

   a. Tentukan karakter yang akan dilakukan proses *encoding.*
   b. Membaca setiap bit pada cabang pohon Huffman dari akar menuju daun.
   c. Lakukan dengan cara yang sama pada langkah 2 sampai semua karakter di *encoding.*

   Tabel 2.2 Hasil Encoding pada Pesan ‘HELLO’

Simbol	Kode Huffman
H	10
E	11
L	01
O	00

   d. Menghitung rasio kompresi

$$rasio\ kompresi = \frac{ukuran\ setelah\ kompresi}{ukuran\ sebelum\ dikompresi}\ x\ 100\ \%$$

2. Dekompresi

Dekompresi *(decoding)* merupakan proses mengembalikan data yang terkompresi ke dalam bentuk yang dapat digunakan kembali seperti semula. Proses *decoding* dapat dilakukan dengan pohon Huffman atau tabel kode Huffman. Berikut langkah-langkah *decoding* string biner yang menggunakan pohon Huffman sebagai berikut:

a. Membaca setiap bit dan string biner mulai dari akar.
b. Setiap bit dari string biner dilakukan secara traversal sesuai cabang.
c. Gunakan cara yang sama dengan mengulangi langkah 1 dan 2 sampai menuju daun (Ariyus, 2008).

2.1.7 Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Cripto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan di kirim dari suatu tempat ke tempat lain.Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Munir, 2009). Keamanan pesan diperoleh dengan menyandikannya menjadi pesan yang tidak mempunyai makna karena informasi yang rahasia perlu disembunyikan agar tidak diketahui oleh orang yang tidak berhak, sehingga kriptografi dapat digunakan untuk menyamarkan informasi rahasia itu dari pihak yang tidak berhak membacanya (Munir, 2009).

2.1.8 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang sangat menarik karena kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang-orang mesir lewat hieroglyph.Sejarah kriptografi dimulai pada zaman Romawi kuno yaitu seorang pemimpin militer dan politikus yang bernama Julius Caesar. Pada saat itu di medan perang Julius Caesar ingin mengirim pesan kepada jenderal melalui kurir. Pesan yang dikirim Julius Caesar ini bersifat rahasia, sehingga harus dijaga keamanannya agar pesan tersebut tidak terbuka pada saat berada dalam berjalanan. Cara agar pesan tersebut tidak dapat dipahami dengan siapapun kecuali jenderal yaitu dengan mengacak pesan menjadi pesan yang tidak dapat terbaca. Dengan Mengacak pesan tersebut Julius Caesar mengganti semua susunan alfabet dadi a, b, c yaitu a menjadi d, b menjadi e, c menjadi f dan seterusnya (Ariyus, 2008).

Pada zaman Romawi pembuatan pesan rahasia dapat menggunakan alat yaitu scytale. Pada zaman tersebut digunakan saat medan perang oleh tentara sparta. Scytale merupakan suatu alat yang memiliki pita panjang dari daun papirus dan di tambah dengan sebatang silinder (Ariyus, 2008). Cara mengirim pesan melalui scytale dengan menuliskan pesan pada pita papirus digulung batang silinder, lalu pita papirus tersebut dilepas dan dikirim. Misalkan pada batang silinder ditulis dengan pesan yang berisi 6 huruf maka pada batang silinder hanya bisa membuat 3 huruf seperti ‘temukan anak saya’ maka pengirim akan menulis ini pada batang silinder

TEMUK

ANANA

KSAYA

Cara pengiriman pesan yaitu dengan melepaskan pita dari batang silinder sehingga pesan yang dihasilkan pada pita tersebut yaitu TAKENSMAAUNYKAA. Proses mengacak Pesan tersebut disebut enkripsi, jika jenderal ingin menyusun pesan acak tersebut agar dapat terbaca disebut dekripsi. Pesan yang akan di acak disebut plainteks, sedangkan pesan yang telah di acak disebut cipherteks.

2.1.9 Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah yang disusun secara sistematis dalam menyelesaikan masalah. Langkah-langkah dalam algoritma bertujuan untuk menyembunyikan pesan rahasia dari pihak yang tidak berhak menerima pesan rahasia tersebut. Berikut ini komponen-komponen dasar algoritma kriptografi sebagai berikut:

1. Enkripsi

   Enkripsi merupakan komponen dasar yang sangat penting pada kriptografi. Proses menyandikan pesan asli kedalam pesan yang tidak dapat dipahami oleh pihak yang tidak dapat menerima pesan rahasia tersebut.

2. Dekripsi

   Dekripsi merupakan kebalikan dari enkripsi yaitu mengembalikan pesan yang tidak dapat dipahami tersebut kedalam pesan yang dapat terbaca.

3. Kunci

Kunci berperan penting pada proses enkripsi dan dekripsi. Kunci dapat dibagi menjadi 3 yaitu:

a. Kunci rahasia *(private key)*

Kunci rahasia *(private key)* disebut algoritma simetri. Algoritma simetri merupakan proses enkripsi dan dekripsi yang menggunakan 2 kunci yang sama contohnya seperti Blowfish, DES (*Data Encryption Standart*), AES (*Advanced Encryption Standard),* dan lain sebagainya.

b. Kunci Umum (*Public key*)

Kunci umum *(Public key)* disebut algoritma asimetri.Algoritma asimetri merupakan merupakan proses enkripsi dan dekripsi yang menggunakan 2 kunci yang berbeda, artinya pada proses enkripsi menggunakan kunci umum (*Public key*), sedangkan pada proses dekripsi menggunakan kunci rahasia*(private key).* Contohnya pada algoritma RSA (*Rivest Shamir Adleman*).

2.1.10 Algoritma Klasik dan Modern

1. Kriptografi Klasik

Kriptografi klasik merupakan algoritma yang menggunakan 1 kunci untuk Mengamankan data. Kriptografi klasik biasanya menggunakan 2 teknik dasar yang sudah digunakan beberapa abad yang lalu seperti sebagai berikut:

a. Teknik Substitusi

Teknik substitusi yaitu teknik mengganti setiap karakter pada pesan asli *(plaintext)* dengan karakter lain.

b. Teknik Transposisi (Permutasi)

Teknik transposisi (permutasi) yaitu teknik yang dilakukan dengan menggunakan permutasi karakter (Ariyus, 2008).

2. Kriptografi Modern

Kriptografi modern merupakan algoritma yang dilakukan pada zaman modern hingga saat ini karena mempunyai kerumitan yang sangat kompleks sehingga mengoperasikannya menggunakan bantuan komputer (Ariyus, 2008).

2.1.11 Algoritma RSA (*Rivest Shamir Adleman*)

Algoritma RSA merupakan algoritma asimetri yang berasal dari MIT (*Massachussets Institute of Technology*) yang ditemukan oleh Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1976 (Munir, 2009). Algoritma RSA menggunakan bilangan prima dan aritmatika modulo dalam proses enkripsi dan deskripsi. Proses enkripsi pada Algoritma RSA ini bersifat umum artinya pada proses enkripsi menggunakan kunci umum sehingga kunci tersebut dapat diketahui oleh orang lain dan proses deskripsi Algoritma RSA bersifat rahasia artinya pada proses dekripsi menggunakan kunci rahasia sehingga pada proses dekripsi hanya dapat dilakukan oleh pihak yang dituju. Keamanan Algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima (Munir, 2019). Kesulitan memfaktorkan bilangan tersebut dapat mengukur kekuatan Algoritma RSA menjadi lebih kuat keamanannya. Dengan kesulitan

Algoritma RSA tersebut algoritma ini terdapat kelemahan yaitu kecepatannya lebih lambat dari pada algoritma kriptografi kunci yang lainnya.Besaran-besaran yang terdapat pada algoritma RSA sebagai berikut:

1. p dan q bilangan prima (rahasia)
2. $n = p \cdot q$ (tidak rahasia)
3. $\phi(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Langkah-langkah pembangkitan sepasang kunci pada algoritma RSA sebagai berikut:

1. Pilih sebarang 2 bilangan prima pertama (p) dan bilangan prima kedua (q)
2. Hitung $n = pq$
3. Hitung $\phi(n) = (p-1)(q-1)$
4. Pilih sebuah bilangan bulat e sebagai kunci publik,e harus relatif prima terhadap $\phi(n)$.
5. Hitung kunci dekripsi d dengan $d = \frac{\phi(n) \cdot t+1}{e}$

Berdasarkan prosedur pembangkitan sepasang kunci tersebut diperoleh pasangan kunci umum adalah (e, n), sedangkan pasangan kunci rahasia yaitu (d, n). Proses enkripsi dengan persamaan $c \equiv m^e (mod\ n)$, sedangkan pada proses dekripsi dengan persamaan $m \equiv c^d (mod\ n)$. Persamaan dekripsi RSA merupakan invers dari persamaan enkripsi RSA dengan menggunakan teorema

euler. Hubungan d di kunci privat dan e di kunci publik dapat ditulis sebagai berikut:

$$e \cdot d \equiv 1(mod\ \phi(n))$$

Oleh kerena itu, dengan aritmatika modulo dapat ditulis sebagai:

$$e \cdot d = t\phi(n) + 1$$

Persamaan dekripsi RSA dapat dihitung sebagai:

$m \equiv c^d(mod\ n)$	(Rumus Dekripsi)
$m \equiv m^{e \cdot d}(mod\ n)$	(Subtitusi $c \equiv m^e(mod\ n)$)
$m \equiv m^{t\phi(n)+1}(mod\ n)$	(Subtitusi $e \cdot d = t\phi(n) + 1$)
$m \equiv m^{t\phi(n)} \cdot m(mod\ n)$	(Sifat bilangan berpangkat)
$m \equiv 1^t \cdot m\ (mod\ n)$	(Teorema Euler)
$m \equiv m\ (mod\ n)$	(Sifat invers)

Oleh karena itu, algoritma dekripsi RSA merupakan invers enkripsi RSA.

2.2 Kajian Keislaman dalam Kriptografi

Kriptografi adalah ilmu dan seni yang bertujuan untuk menjaga keamanan pesan ketika dikirim dari suatu tempat ke tempat lain (Ariyus, 2008). Menjaga keamanan pesan pada zaman sekarang ini sangat penting untuk menghindari dari pihak yang tidak bertanggung jawab. Dalam al-Quran menjaga keamanan sebuah pesan yang bersifat rahasia kepada pihak yang dapat dipercaya dan bertanggung jawab yaitu amanah yang dijelaskan pada QS.Al-Mu'minun ayat 8:

Artinya: "Dan orang-orang yang memelihara amanat-amanat (yang dipikulnya) dan janjinya"(QS. Al-Mu'minun:8).

Berdasarkan ayat tersebut, menurut Syaikh Imam Al-Qurthubi memberi penjelasan dalam tafsirnya, mayoritas ulama membaca (firman Allah itu) dengan lafazh لِأَمَٰنَٰتِهِمْ yakni dengan bentuk jamak. Amanah dan janji itu mencangkup segala sesuatu yang dipikuli oleh manusia dalam urusan agama dan dunianya, baik berupa ucapan maupun perbuatan. Setiap janji adalah amanah tentang apa-apa yang sudah disampaikan, baik berupa ucapan, perbuatan ataupun keyakinan (Al-Qurthubi, 2009).

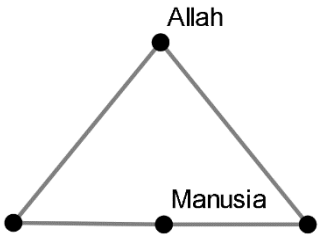
Menurut Quraish Shihab mengatakan, bahwa apabila seseorang menyampaikan suatu yang penting dan rahasia kepada orang lain, hal itu merupakan bentuk amanah sederhana yang harus dijaga oleh orang tersebut (Andika, M.Taquyuddin, & Admizal, 2020) .Apabila seseorang berkhianat kepada orang yang mempercayainya. Sebagaimana konsep amanah yang telah dijelaskan dalam Al-Qur'an surah Al-Anfal ayat 27 :

Artinya"Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul dan janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepada kamu, sedang kamu mengetahui"(QS. Al-Anfal:27).

Berdasarkan Tafsir Ibnu Katsir bahwa Ali bin Abi Thalib berkata, dari Ibnu Abbas mengenai firman Allah dan *"dan (juga) janganlah kamu mengkhianati amanat yang dipercayakan kepadamu".* Amanah merupakan segala macam bentuk perbuatan yang diamanatkan oleh Allah Swt kepada hamba-hamba-Nya. Maksud dari amanat tersebut adalah kewajiban, Dia berkata: "*janganlah kamu mengkhianati"*, yang berarti jangan melanggar amanat itu (Katsir, 2003).

Ilmu Kriptografi selain menerapkan dalam proses penyandian pesan juga dapat diterapkan dalam teori graf yaitu pohon Huffman dengan merepresentasikan

visual dari graf dengan menyatakan objek sebagai titik, sedangkan hubungan antara objek dinyatakan dengan garis seperti pada gambar berikut:



Gambar 2. 2 Hubungan antara Allah dengan Hambanya serta Sesama Hambanya

Graf dalam Al-Quran terdapat elemen-elemen yang dinyatakan titik dan sisi meliputi Pencipta (Allah SWT) dan hamba-hambanya, sedangkan garis atau sisi yang menghubungkan elemen-elemen tersebut yaitu hubungan antara Allah dengan hambanya dan hubungan sesama hamba yang terjalin, *Hablun min Allah wa Hablun min An-Nas* (Sa'adah, 2009).

2.3 Kajian Topik dengan Teori Pendukung

Dalam ilmu kriptografi memanfaatkan salah satu ilmu matematika yaitu bilangan bulat yang digunakan dalam proses menyandikan sebuah pesan. Sifat bilangan bulat melahirkan beberapa konsep salah satunya yaitu bilangan prima dan aritmatika modulo. Bilangan bulat selain digunakan dalam proses menyandikan sebuah pesan enkripsi dan dekripsi dapat digunakan dalam proses kompresi dan dekompresi pada kode Huffman. Dalam proses kode Huffman untuk membuat sebuah keputusan menggunakan pohon Huffman yang menerapkan sistem kode ASCII (*American Standart Code for Information Interchange*). Ilmu kriptografi mempunyai beberapa macam algoritma salah satunya yaitu algoritma RSA Algoritma RSA ini algoritma yang penulis gunakan dalam mengamankan

sebuah pesan dengan memanfaatkan ilmu matematika dalam pembangkitan kunci, enkripsi dan dekripsi yaitu kongruensi dan keterbagian, sehingga topik skripsi ini sangat berkaitan dengan teori pendukung yang ada dalam ilmu matematika.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Jenis penelitian ini menggunakan studi kepustakaan yaitu proses pengumpulan data maupun informasi dari beberapa sumber literatur seperti buku, jurnal, artikel, dan sebagainya yang terkait tentang algoritma kriptografi khususnya algoritma RSA dan kode Huffman.

3.2 Pra Penelitian

Pada tahap pra penelitian ini sebelum peneliti memulai penelitian terdapat beberapa hal yang perlu dilakukan sebagai berikut:

1. Mencari sumber literatur utama yang akan di jadikan sumber rujukan dalam menentukan topik penelitian.
2. Mengumpulkan berbagai jenis literatur yang berkaitan dengan teori pendukung dan pembahasan.
3. Mempelajari dan memahami literatur yang berkaitan dengan algoritma RSAdan kode Huffman.

3.3 Tahapan Penelitian

Pada tahap penelitian ini terdapat alur kerja kode Huffman pada algoritma RSA sebagai berikut:

3.3.1 Proses Enkripsi pada Algoritma RSA (*Rivest Shamir Adleman*)

Berikut ini langkah-langkah proses enkripsi algoritma RSA (*Rivest Shamir Adleman*) sebagai berikut:

1. Membangkitan kunci pada algoritma RSA yaitu sebagai berikut:
   a. Pilih sebarang 2 bilangan prima pertama (p) dan bilangan prima kedua (q).
   b. Menghitung n dari $p\ x\ q$ dapat dituliskan $n = pq$.
   c. Menentukan $\phi(n) = (p-1)(q-1)$.
   d. Pilih bilangan bulat e sebagai kunci umum, e harus relatif prima terhadap $\phi(n)$.
   e. Menghitung d dengan $d = \frac{\phi(n)\cdot t+1}{e}$
2. Menentukan plainteks dari huruf alfabet dari A-Z .
3. Melakukan enkripsi menggunakan persamaan.

$$c \equiv m^e (mod\ n)$$

4. Memperoleh cipherteks dari proses enkripsi.

3.3.2 Proses Kompresi Menggunakan Kode Huffman

Berikut ini langkah-langkah proses kompresi menggunakan kode Huffman sebagai berikut:

1. Melakukan proses kompresi dari cipherteks hasil proses enkripsi.
2. Membuat pohon Huffman.
3. Menentukan rasio kompresi.

$$rasio\ kompresi = \frac{ukuran\ setelah\ kompresi}{ukuran\ sebelum\ dikompresi}\ x\ 100\ \%$$

3.3.3 Proses Dekompresi Menggunakan Kode Huffman

Berikut ini langkah-langkah proses dekompresi menggunakan pohon Huffman sebagai berikut:

1. Membaca sebuah bit dari *string* biner mulai dari akar pohon Huffman.
2. Setiap bit dari *string* biner dilakukan secara tranversal sesuai cabang yang bersesuaian.Label 0 lihat cabang kiri pada pohon Huffman, sedangkan label 1 lihat cabang kanan pada pohon Huffman.

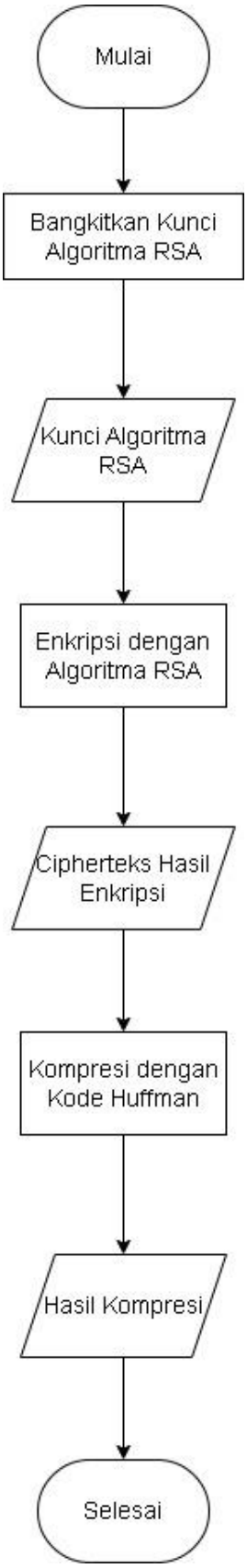
3.3.4 Proses Dekripsi pada Algoritma RSA (*Rivest Shamir Adleman*)

Berikut ini langkah-langkah proses dekripsi algoritma RSA (*Rivest Shamir Adleman*) sebagai berikut :

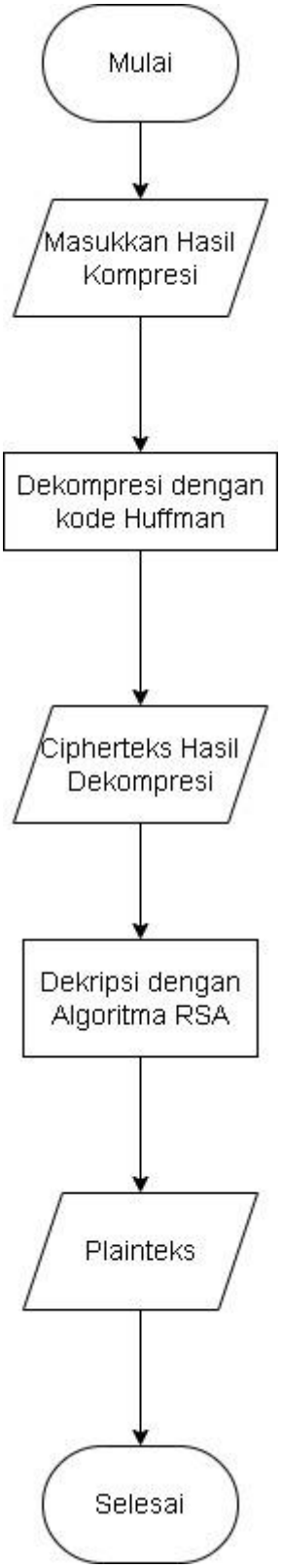
1. Masukkan cipherteks hasil dekompresi.
2. Melakukan dekripsi dengan persamaan $m \equiv c^d (mod\ n)$.
3. Mendapatkan plainteks awal.

3.3.5 Flowchart

Berikut gambaran rancangan flowchart yang akan dibuat pada gambar 3.1 dan gambar 3.2.



Gambar 3.1 Flowchart Proses Enkripsi dan Kompresi Kode Huffman Pada Algoritma RSA



Gambar 3.2 Flowchart Dekompresi dan Dekripsi Kode Huffman Pada Algoritma RSA

BAB IV
PEMBAHASAN

4.1 Proses Enkripsi Algoritma RSA dengan Kompresi pada Kode Huffman

4.1.1 Algoritma Enkripsi RSA dengan Kompresi pada Kode Huffman

Algoritma RSA menggunakan dua bilangan prima yang berbeda. Kedua bilangan prima tersebut di kalikan yang hasilnya digunakan sebagai salah satu parameter untuk proses enkripsi dan dekripsi. Beberapa parameter dalam algoritma RSA yang digunakan untuk proses enkripsi dan dekripsi adalah sebagai berikut:

1. Pengirim Membangkitan kunci pada algoritma RSA dengan memilih sebarang 2 bilangan prima pertama (p) dan bilangan prima kedua (q) dengan syarat $\neq q$, sebab jika $p = q$ maka $n = p^2$ sehingga bilangan pertama (p) dapat diperoleh dengan menarik akar pangkat dua dari (n). Jika salah satu nilai dari p dan q tidak prima maka akan menyebabkan $\phi(p) < (p-1)$ atau $\phi(q) < (q-1)$. Nilai p dan q bersifat rahasia, sehingga hanya penerima yang dapat mengetahui bilangan tersebut.
2. nilai n dari perkalian 2 sebarang bilanga prima p dan q dapat dituliskan $n = pq$, dengan n adalah salah satu parameter yang digunakan dalam proses enkripsi dan dekripsi. Nilai n bersifat tidak rahasia sehingga bilangan tersebut dapat diketahui oleh orang lain.

3. $\phi(n) = (p-1)(q-1)$, $\phi(n)$ digunakan untuk menentukan jumlah dari bilangan yang relatif prima terhadap n dan sifatnya rahasia sehingga hanya penerima pesan yang dapat mengetahui bilangan tersebut.

   Bilangan bulat e sebagai kunci umum dan e harus relatif prima terhadap $\phi(n)$, sehingga $gcd = \big(e, \phi(n)\big)$ =1 dan sifatnya tidak rahasia sehingga bilangan tersebut dapat disebarluaskan.

4. Salah satu kunci privat (d), dengan $d = \frac{\phi(n)\cdot t+1}{e}$ yang akan di kirimkan kepada penerima dan sifatmya rahasia sehingga hanya penerima yang dapat mengetahuinya.

5. Pasangan kunci publik (tidak rahasia) adalah (e, n) sedangkan pasangan kunci Privat adalah (d, n)

Dari beberapa parameter tersebut diperoleh bahwa parameter yang bersifat umum atau tidak rahasia dapat diketahui oleh orang lain dalam menerima pesan yaitu n dan e sedangkan parameter yang bersifat rahasia atau hanya dapat diketahui oleh pengirim dan penerima yaitu $\phi(n)$ dan d. Kode Huffman menggunakan bilangan biner pada graf pohon. Algoritma Huffman menggunakan prinsip pengkodean yang mirip dengan kode Morse, yaitu tiap karakter dikodekan hanya dengan rangkaian beberapa bit 0 dan 1 sesuai distribusi kemunculan karakter dalam naskah untuk proses kompresi (Amrullah, 2011).

4.1.2 Simulasi Algoritma RSA dengan Kompresi pada Kode Huffman

Berikut proses enkripsi algoritma RSA pada pesan teks sebagai berikut:

1. Pesan Teks 8 Karakter

Ambil sebarang 2 bilangan prima pertama (p) yaitu 41 ,bilangan prima kedua (q) yaitu 79

$$n = p\ x\ q = 41\ x\ 79 = 3239$$

$$\phi(n) = (p-1)\ x\ (q-1) = 40\ x\ 78 = 3120$$

Pilih sebuah bilangan bulat e, sebut $e = 29$ sebagai kunci umum,e harus relatif prima terhadap $\phi(n)$ maka, $gcd = \left(e, \phi(n)\right)$ =1 sehingga 29 relatif prima terhadap 3120 maka

$$gcd = (29, 3120) = 1$$

Hitung d dengan $d = \frac{\phi(n)\cdot k+1}{e}$ dengan nilai

$k = 1,2,3,\dots,n-1$, $d = \frac{3120\cdot 17+1}{29} = 1829$ sehingga diperoleh nilai d yang bulat adalah $d = 1829$ sebagai kunci privat.

Dimana untuk $k = 17$ karena menghasilkan d bilangan bulat yaitu d = 1829

Plainteks M = ‘apa kabar’ menggunakan tabel huruf alfabet.

Tabel 4. 1 Tabel Huruf Alfabet

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
00	01	02	03	04	05	06	07	08	09	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Maka pesan M dikodekan (spasi diabaikan) menjadi M = 0015001000010017

Pecah M menjadi 4 digit blok, maka:

m_1 = 0015

m_2 = 0010

m_3 = 0001

m_4 = 0017

Enkripsi dengan kunci (e = 29)

$c_1 \equiv 15^{29} \pmod{3239} = 2190$

$c_2 \equiv 10^{29} \pmod{3239} = 0447$

$c_3 \equiv 1^{29} \pmod{3239} = 0001$

$c_4 \equiv 17^{29} \pmod{3239} = 0015$

Sehingga menghasilkan cipherteks C = 2190 0447 0001 0015 dengan melihat tabel huruf alfabet maka di modulo 26 sehingga di dapatkan hasil cipherteks vmevabap.

2. Pesan Teks 10 Karakter

Ambil sebarang 2 bilangan prima pertama (p) yaitu 47 ,bilangan prima kedua (q) yaitu 71

$$n = p\ x\ q = 47\ x\ 71 = 3337$$

$$\phi(n) = (p-1)\ x\ (q-1) = 46\ x\ 70 = 3220$$

Pilih sebuah bilangan bulat e, sebut $e = 79$ sebagai kunci umum, e harus relatif prima terhadap $\phi(n)$ maka, $gcd = \big(e, \phi(n)\big)$ =1 sehingga 79 relatif prima terhadap 3220 maka

$$gcd = (79, 3220) = 1$$

Menghitung d dengan $d = \frac{\phi(n)\cdot k+1}{e}$ dengan nilai $k = 1,2,3, \ldots, n-1$

$$d = \frac{3220\cdot 25+1}{79} = 1019$$

Sehingga diperoleh nilai d yang bulat adalah $d = 1019$ sebagai kunci privat.

Dimana untuk $k = 25$ karena menghasilkan d bilangan bulat yaitu 1019

Plainteks M = ’HELLO TUGAS’ menggunakan tabel huruf alfabet maka pesan M dikodekan(spasi diabaikan)menjadi M = 07041111141920060018

Pecah M menjadi 4 digit blok, maka:

m_1 = 0704

m_2 = 1111

m_3 = 1419

m_4 = 2006

m_5 = 0018

Enkripsi dengan kunci (e = 79)

$c_1 \equiv 704^{79} \pmod{3337}$ = 0328

$c_2 \equiv 1111^{79} \pmod{3337}$ = 0301

$c_3 \equiv 1419^{79} \pmod{3337}$ = 1135

$c_4 \equiv 2006^{79} \pmod{3337}$ = 1426

$c_5 \equiv 18^{79} \pmod{3337}$ = 2562

Sehingga menghasilkan cipherteks C = 0328 0301 1135 1426 2562 dengan melihat tabel huruf alfabet maka di modulo 26 sehingga di dapatkan hasil cipherteks DCDBLJOAZK.

3. Pesan Teks 12 Karakter

Ambil sebarang 2 bilangan prima pertama (p) yaitu 61 ,bilangan prima kedua (q) yaitu 83

$$n = p\ x\ q = 61\ x\ 83 = 5063$$

$$\phi(n) = (p-1)\ x\ (q-1) = 60\ x\ 82 = 4920$$

Pilih sebuah bilangan bulat e, sebut $e = 187$ sebagai kunci umum, e harus relatif prima terhadap $\phi(n)$ maka, $gcd = \big(e, \phi(n)\big) = 1$, sehingga 187 relatif prima terhadap 4920 maka $gcd = (187, 4920) = 1$

Menghitung d dengan $d = \frac{\phi(n)\cdot k+1}{e}$ dengan nilai $k = 1,2,3, \ldots, n-1$

$$d = \frac{4920 \cdot 29+1}{187} = 763$$

Sehingga diperoleh nilai d yang bulat adalah $d = 763$ sebagai kunci privat.Dimana untuk $k = 29$ karena menghasilkan d bilangan bulat yaitu d = 763. Plainteks M = ‘kamu apa kabar’ menggunakan tabel huruf alfabet maka pesan M dikodekan (*spasi diabaikan*) menjadi

M = 10001220001500100010017

Pecah M menjadi 4 digit blok, maka:

m_1 = 1000

m_2 = 1220

m_3 = 0015

m_4 = 0010

m_5 = 0001

m_6 = 0017

Enkripsi dengan kunci (e = 187)

$c_1 \equiv 1000^{187}$ (mod 5063) = 1960

$c_2 \equiv 1220^{187}$ (mod 5063) = 4453

$c_3 \equiv 15^{187}$ (mod 5063) = 3255

$c_4 \equiv 10^{187}$ (mod 5063) = 4296

$c_5 \equiv 1^{187}$ (mod 5063) = 0001

$c_6 \equiv 17^{187} \pmod{5063} = 2226$

Sehingga menghasilkan cipherteks C = 1960 4453 3255 4296 0001 2226 dengan melihat tabel huruf alfabet maka di modulo 26 sehingga di dapatkan hasil cipherteks tisbgdqsabwa.

4. Pesan Teks 14 Karakter

Ambil sebarang 2 bilangan prima pertama (p) yaitu 41 ,bilangan prima kedua(q) yaitu 73

$$n = p\ x\ q = 41\ x\ 73 = 2993$$

$$\phi(n) = (p-1)\ x\ (q-1) = 40\ x\ 72 = 2880$$

Pilih sebuah bilangan bulat e, sebut sebagai kunci umum, e harus relatif prima terhadap $\phi(n)$ maka, $gcd = \big(e, \phi(n)\big)$ =1 sehingga 29 relatif prima terhadap 2880 maka

$$gcd = (29, 2880) = 1$$

Menghitung d dengan $d = \frac{\phi(n)\cdot k+1}{e}$ dengan nilai $k = 1,2,3, \ldots, n-1$

$$d = \frac{2880 \cdot 16+1}{29} = 1589$$

Sehingga diperoleh nilai d yang bulat adalah $d = 1589$ sebagai kunci privat.

Dimana untuk $k = 16$ karena menghasilkan d bilangan bulat yaitu d = 1589 Plainteks M = ‘TETAP BERSYUKUR’ menggunakan tabel huruf alfabet maka pesan M dikodekan (*spasi diabaikan*) menjadi

M =19041900150104171824201020 17

Pecah M menjadi 4 digit blok, maka:

m_1 = 1904

m_2 = 1900

m_3 = 1501

m_4 = 0417

m_5 = 1824

m_6 = 2010

m_7 = 2017

Enkripsi dengan kunci (e = 29)

$c_1 \equiv 1904^{29}$ (mod 2993) = 1410

$c_2 \equiv 1900^{29}$ (mod 2993) = 0150

$c_3 \equiv 1501^{29}$ (mod 2993) = 1458

$c_4 \equiv 417^{29}$ (mod 2993) = 1709

$c_5 \equiv 1824^{29}$ (mod 2993) = 1970

$c_6 \equiv 2010^{29}$ (mod 2993) = 1067

$c_7 \equiv 2017^{29}$ (mod 2993) = 0046

Sehingga menghasilkan cipherteks C = 1410 0150 1458 1709 1970 1067 0046 dengan melihat tabel huruf alfabet maka di modulo 26 sehingga di dapatkan hasil cipherteks OKBMOGRJTSKPAU.

5. Pesan Teks 16 Karakter

Ambil sebarang 2 bilangan prima pertama (p) yaitu 53, bilangan prima kedua (q) yaitu 73

$$n = p\ x\ q = 53\ x\ 73 = 3869$$

$$\phi(n) = (p-1)\ x\ (q-1) = 52\ x\ 72 = 3744$$

Pilih sebuah bilangan bulat e, sebut e =23 sebagai kunci umum, e harus relatif prima terhadap $\phi(n)$ maka, $gcd = \big(e, \phi(n)\big)$ =1

$$gcd = (23, 3744) = 1$$

Menghitung kunci dekripsi d dengan $d = \frac{\phi(n)\cdot k+1}{e}$

$$d = \frac{3744 \cdot 14+1}{23} = 2279$$

Dimana untuk $k = 14$ karena menghasilkan d bilangan bulat yaitu d = 2279. Plainteks M = ‘BERMAIN SEPAKBOLA' menggunakan tabel huruf alfabet maka pesan M dikodekan (*spasi diabaikan*) menjadi

M = 0104171200081318041500100114100

Pecah M menjadi 4 digit blok, maka:

m_1 = 0104

m_2 = 1712

m_3 = 0008

m_4 = 1318

m_5 = 0415

m_6 = 0010

m_7 = 0114

m_7 = 1100

Enkripsi dengan kunci (e = 23)

$c_1 \equiv 104^{23} \ (mod\ 3869)$ = 2988

$c_2 \equiv 1712^{23} \ (mod\ 3869)$ = 2219

$c_3 \equiv 9^{23} \ (mod\ 3869)$ = 3130

$c_4 \equiv 1318^{23} \ (mod\ 3869)$ = 0513

$c_5 \equiv 415^{23} \ (mod\ 3869)$ = 1904

$c_6 \equiv 10^{23} \ (mod\ 3869)$ = 3672

$c_7 \equiv 114^{23}\ (mod\ 3869)$ = 2865

$c_8 \equiv 1100^{23}\ (mod\ 3869)$ = 2396

Sehingga menghasilkan cipherteks C = 2988 2219 3130 0513 1904 3672 2865 2396 dengan melihat tabel huruf alfabet maka di modulo 26 sehingga di dapatkan hasil cipherteks DKWTFEFNTEKUCNXS.

Setelah melakukan enkripsi pada algoritma RSA yaitu proses kompresi menggunakan kode Huffman pada pesan teks sebagai berikut :

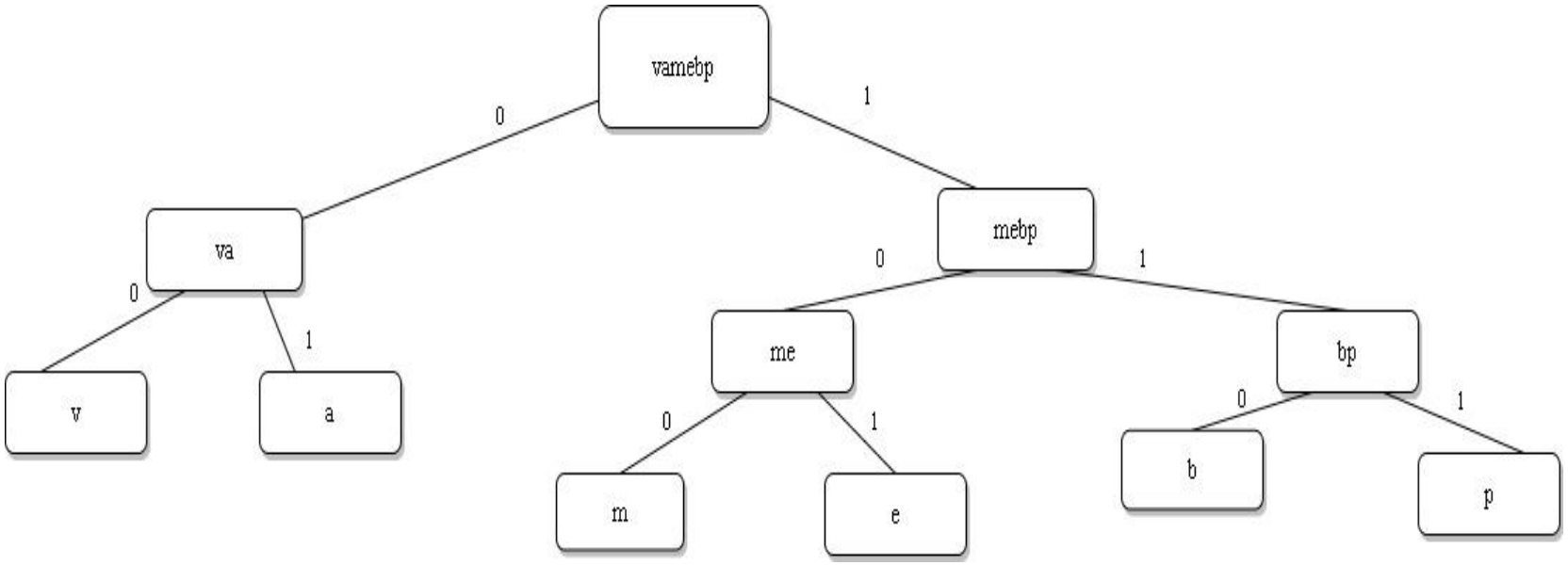
1. Pesan Teks 8 Karakter

Berikut ini tabel proses kompresi dengan cipherteks ‘vmevabap’.

Tabel 4.2 Kode ASCII pada Cipherteks ‘vmevabap’

Char	Kode ASCII (Biner)	Bit	Kekerapan	Bit x Kekerapan
v	01110110	8	2	16
m	01101101	8	1	8
e	01100101	8	1	8
a	01100001	8	2	16
b	01100010	8	1	8
p	01110000	8	1	8
Total				64 bit

Untuk mendapatkan kode Huffman, pertama menghitung kekerapan setiap karakter dengan memetakan kode atau karakter yang sama tersebut dengan membentuk pohon Huffman:



Gambar 4.1 Pohon Huffman pada Cipherteks ‘vmevabap’

Sehingga dari pohon Huffman bisa diubah menjadi kode Huffman sebagai berikut:

Tabel 4.3 Hasil Pohon Huffman pada Cipherteks ’vmevabap’

Char	Kode Huffman	Bit	Kekerapan	Bit × Kekerapan
v	00	2	2	4
m	100	3	1	3
e	101	3	1	3
a	01	2	2	4
b	110	3	1	3
p	111	3	1	3
Total				20 bit

Sehingga di dapatkan hasil kode Huffman pada Cipherteks ’vmevabap’ = 00100101000111001111

Menghitung rasio kompresi

$$rasio\ kompresi = \frac{ukuran\ setelah\ kompresi}{ukuran\ sebelum\ dikompresi}\ x\ 100\ \%$$

$$rasio\ kompresi = \frac{20}{64}\ x\ 100\% = 31{,}25\ \%$$

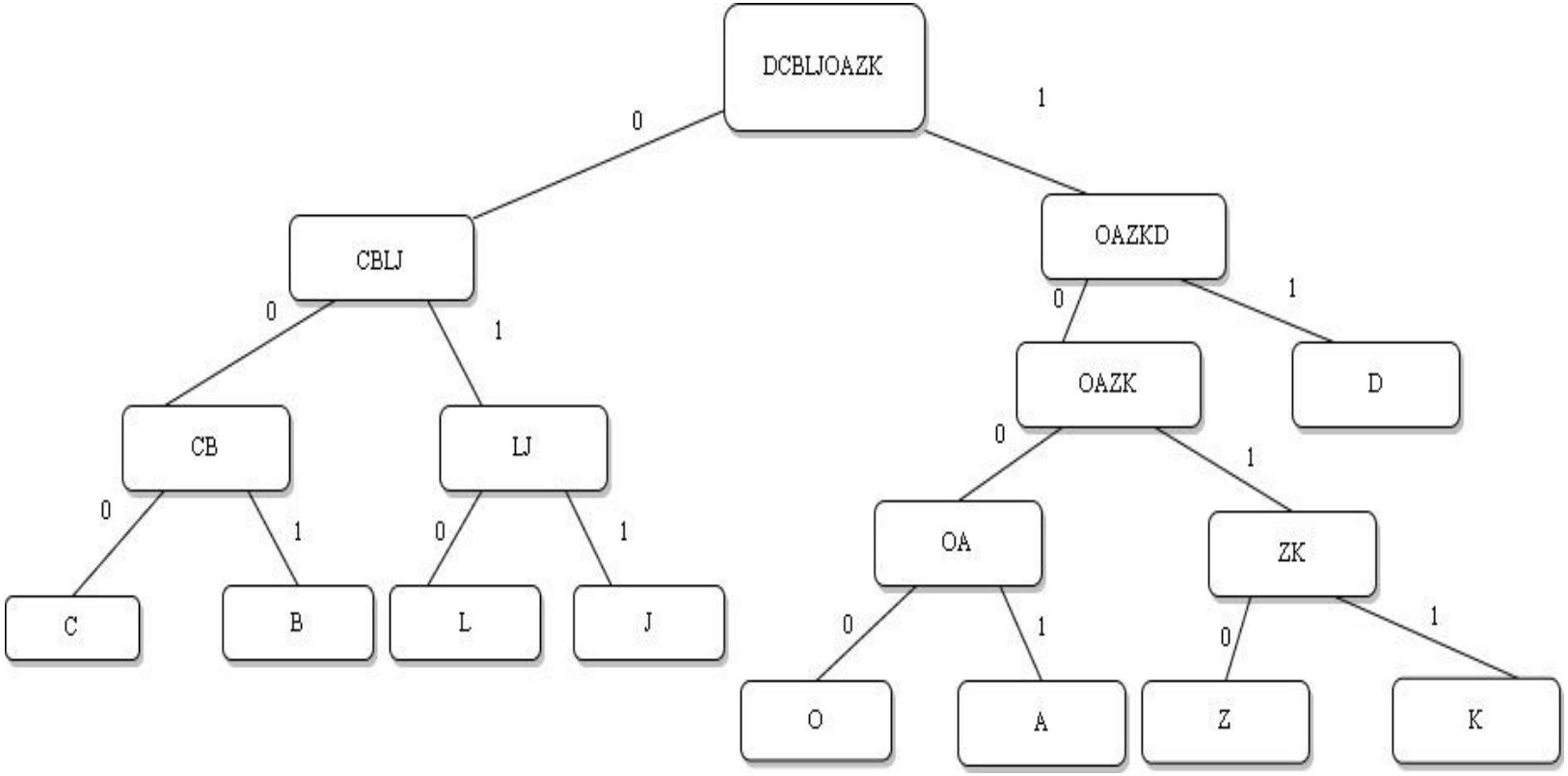
2. Pesan Teks 10 Karakter

Berikut ini tabel proses kompresi dengan cipherteks ‘DCDBLJOAZK’

Tabel 4.4 Kode ASCII pada Cipherteks ’ DCDBLJOAZK’

Char	Kode ASCII (Biner)	Bit	Kekerapan	Bit x Kekerapan
D	01000100	8	2	16
C	01000011	8	1	8
B	01000010	8	1	8
L	01001100	8	1	8
J	01001010	8	1	8
O	01001111	8	1	8
A	01000001	8	1	8
Z	01011010	8	1	8
K	01001011	8	1	8
Total				80 bit

Untuk mendapatkan kode Huffman, pertama menghitung kekerapan setiap karakter dengan memetakan kode atau karakter yang sama tersebut dengan membentuk pohon Huffman:



Gambar 4.2 Pohon Huffman pada Cipherteks ’ DCDBLJOAZK’

sehingga dari pohon Huffman bisa diubah menjadi kode Huffman sebagai berikut**:**

Tabel 4.5 Hasil Pohon Huffman pada Cipherteks ’ DCDBLJOAZK’

Char	Kode Huffman	Bit	Kekerapan	Bit x Kekerapan
D	11	2	2	4
C	000	3	1	3
B	001	3	1	3
L	010	3	1	3
J	011	3	1	3
O	1000	4	1	4
A	1001	4	1	4
Z	1010	4	1	4
K	1011	4	1	4
Total				32 bit

Sehingga didapatkan hasil kode Huffman pada Cipherteks ’DCDBLJOAZK’ = 11000110010100111000100110101011

Menghitung rasio kompresi

$$rasio\ kompresi = \frac{ukuran\ setelah\ kompresi}{ukuran\ sebelum\ dikompresi}\ x\ 100\ \%$$

$$rasio\ kompresi = \frac{32}{80}\ x\ 100\% = 40\%$$

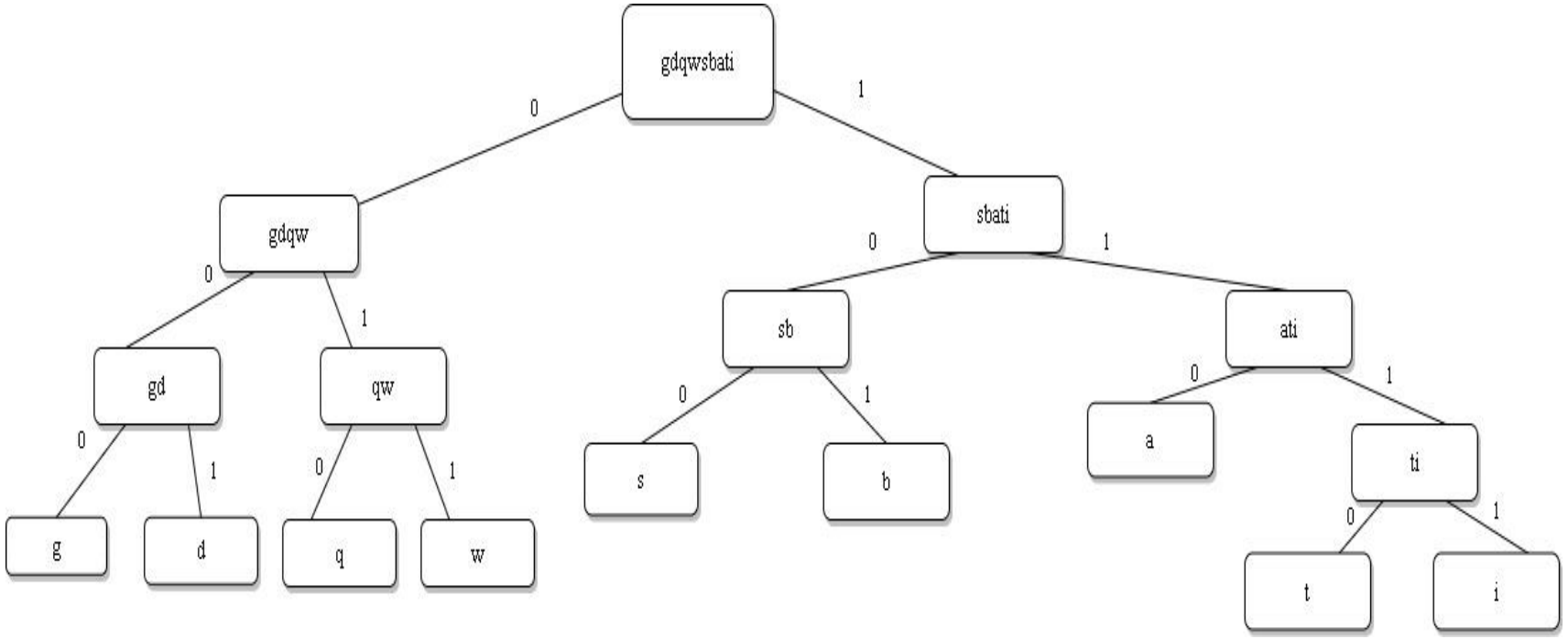
3. Pesan Teks 12 Karakter

Berikut ini tabel proses enkripsi dengan cipherteks ‘tisbgdqsabwa’

Tabel 4.6 Kode ASCII pada Cipherteks ‘tisbgdqsabwa’

Char	Kode ASCII (Biner)	Bit	Kekerapan	Bit x Kekerapan
T	01110100	8	1	8
I	01101001	8	1	8
S	01110011	8	2	16
B	01100010	8	2	16
G	01100111	8	1	8
D	01100100	8	1	8
Q	01110001	8	1	8
A	01100001	8	2	16
W	01110111	8	1	8
Total				96 bit

Untuk mendapatkan kode Huffman, pertama menghitung kekerapan setiap karakter dengan memetakan kode atau karakter yang sama tersebut dengan membentuk pohon Huffman:



Gambar 4.3 Pohon Huffman pada Cipherteks ‘tisbgdqsabwa’

sehingga dari pohon Huffman bisa diubah menjadi kode Huffman sebagai berikut**:**

Tabel 4.7 Hasil Pohon Huffman pada Cipherteks ’tisbgdqsabwa’

Char	Kekerapan	Kode Huffman	Bit	Bit x Kekerapan
t	1	1110	4	4
i	1	1111	4	4
s	2	100	3	6
b	2	101	3	6
g	1	000	3	3
d	1	001	3	3
q	1	010	3	3
a	2	110	3	6
w	1	011	3	3
Total				38 bit

Sehingga di dapatkan hasil kode Huffman pada Cipherteks ‘tisbgdqsabwa’ = 11101111100101000001010100110101011110

Menghitung rasio kompresi

$$rasio\ kompresi = \frac{ukuran\ setelah\ kompresi}{ukuran\ sebelum\ dikompresi}\ x\ 100\ \%$$

$$rasio\ kompresi = \frac{38}{96}\ x\ 100\% = 39{,}58\%$$

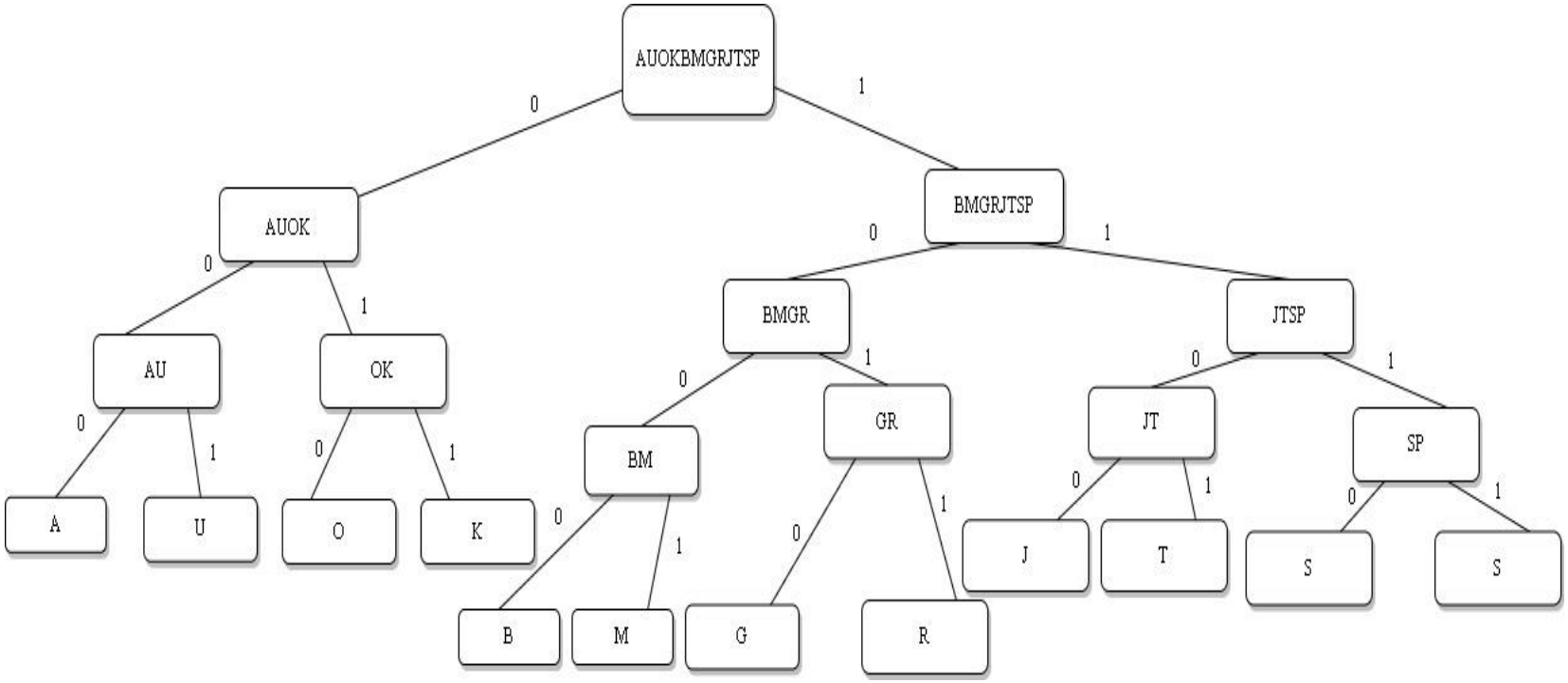
4. Pesan Teks 14 Karakter

Berikut ini tabel proses enkripsi dengan cipherteks ‘OKBMOGRJTSKPAU’

Tabel 4.8 Kode ASCII pada Cipherteks ‘OKBMOGRJTSKPAU’

Char	Kode ASCII (Biner)	Bit	Kekerapan	Bit x Kekerapan
O	01001111	8	2	16
K	01001011	8	2	16
B	01000010	8	1	8
M	01001101	8	1	8
G	01000111	8	1	8
R	01010010	8	1	8
J	01001010	8	1	8
T	01010100	8	1	8
S	01010011	8	1	8
P	01010000	8	1	8
A	01000001	8	1	8
U	01010101	8	1	8
Total				112 bit

Untuk mendapatkan kode Huffman, pertama menghitung kekerapan setiap karakter dengan memetakan kode atau karakter yang sama tersebut dengan membentuk pohon Huffman:



Gambar 4.4 Pohon Huffman pada Cipherteks ‘OKBMOGRJTSKPAU’

Sehingga dari pohon Huffman bisa diubah menjadi kode Huffman sebagai berikut**:**

Tabel 4.9 Hasil Pohon Huffman pada Cipherteks ’OKBMOGRJTSKPAU’

Char	Kekerapan	Kode Huffman	Bit	Bit x Kekerapan
O	2	010	3	6
K	2	111	3	6
B	1	1000	4	4
M	1	1001	4	4
G	1	1000	4	4
R	1	1011	4	4
J	1	1100	4	4
T	1	1101	4	4
S	1	1100	4	4
P	1	1111	4	4
A	1	000	3	3
U	1	001	3	3
Total				50 bit

Sehingga di dapatkan hasil kode Huffman pada Cipherteks ’OKBMOGRJTSKPAU’=0100111000100101010101011110011011111001111111000001

Menghitung rasio kompresi

$$rasio\ kompresi = \frac{ukuran\ setelah\ kompresi}{ukuran\ sebelum\ dikompresi}\ x\ 100\ \%$$

$$rasio\ kompresi = \frac{50}{112}\ x\ 100\% = 44{,}64\%$$

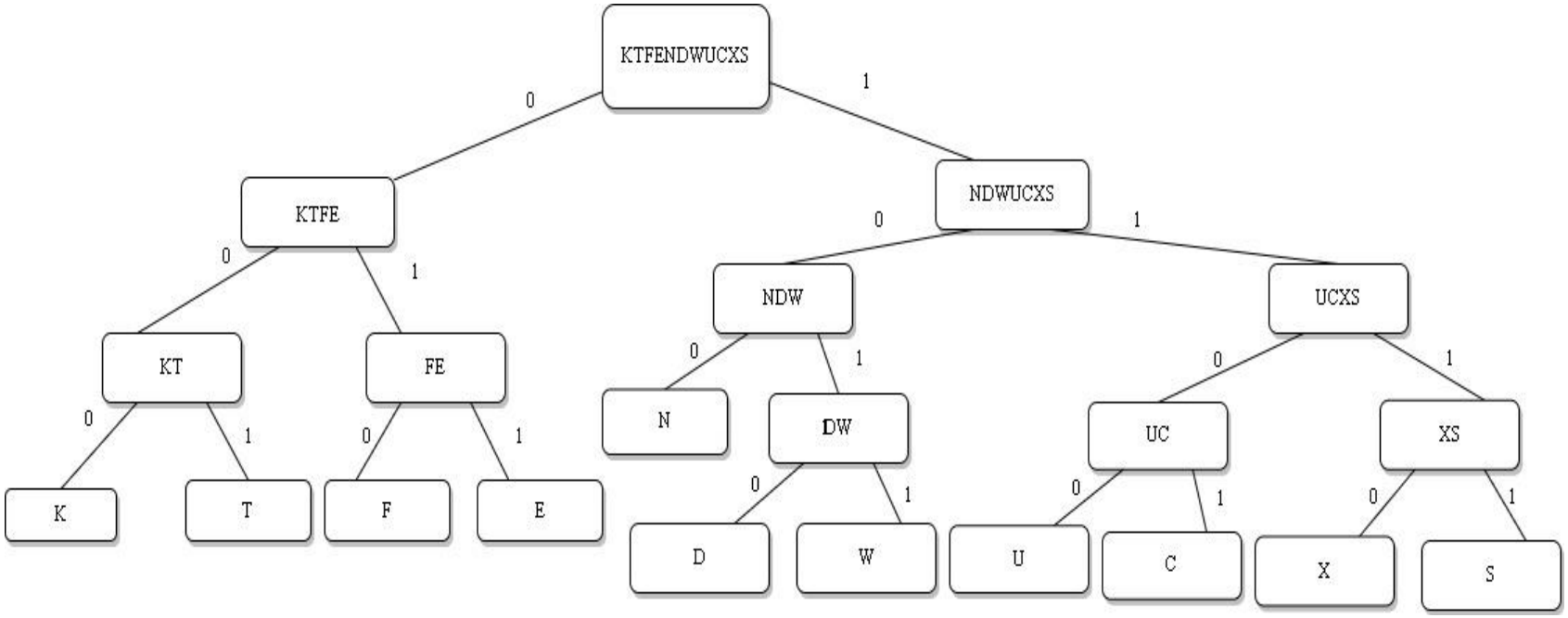
5. Pesan Teks 16 Karakter

Berikut ini tabel proses enkripsi dengan cipherteks ‘DKWTFEFNTEKUCNXS’

Tabel 4.10 Kode ASCII pada Cipherteks ‘DKWTFEFNTEKUCNXS’

Char	Kode ASCII (Biner)	Bit	Kekerapan	Bit x Kekerapan
D	01000100	8	1	8
K	01001011	8	2	16
W	01010111	8	1	8
T	01010100	8	2	16
F	01000110	8	2	16
E	01000101	8	2	16
N	01001110	8	2	16
U	01010101	8	1	8
C	01000011	8	1	8
X	01011000	8	1	8
S	01010011	8	1	8
Total				128 bit

Untuk mendapatkan kode Huffman, pertama menghitung kekerapan setiap karakter dengan memetakan kode atau karakter yang sama tersebut dengan membentuk pohon Huffman:



Gambar 4.5 Pohon Huffman pada Cipherteks ‘OKBMOGRJTSKPAU’

sehingga dari pohon Huffman bisa diubah menjadi kode Huffman sebagai berikut**:**

Tabel 4.11 Hasil Pohon Huffman pada Cipherteks ‘DKWTFEFNTEKUCNXS’

Char	Kekerapan	Kode Huffman	Bit	Bit x Kekerapan
D	1	1000	4	4
K	2	000	3	6
W	1	1011	4	4
T	2	001	3	6
F	2	010	3	6
E	2	011	3	6
N	2	100	3	6
U	1	1100	4	4
C	1	1101	4	4
X	1	1110	4	4
S	1	1111	4	4
Total				54 bit

Sehingga di dapatkan hasil kode Huffman pada Cipherteks ‘DKWTFEFNTEKUCNXS’=101000010110010100110101000010110001100110110011101111

Menghitung rasio kompresi

$$rasio\ kompresi = \frac{ukuran\ setelah\ kompresi}{ukuran\ sebelum\ dikompresi}\ x\ 100\ \%$$

$$rasio\ kompresi = \frac{54}{128}\ x\ 100\% = 42{,}19\%$$

4.2 Proses Dekompresi Kode Huffman dengan Dekripsi Algoritma RSA

4.2.1 Algoritma Dekompresi Kode Huffman dengan Dekripsi Algoritma RSA

1. Penerima melakukan proses dekompresi dengan hasil yang dikirim oleh pengirim menggunakan pohon Huffman dengan membaca sebuah bit dari *string* biner mulai dari akar pohon Huffman. Setiap bit dari *string* biner dilakukan secara tranversal sesuai cabang yang bersesuaian.Label 0 lihat cabang kiri pada pohon Huffman, sedangkan label 1 lihat cabang kanan pada pohon Huffman.
2. Penerima melakukan proses dekripsi algoritma RSA dengan memasukkan cipherteks hasil dekompresi.
3. Penerima melakukan dekripsi dengan persamaan $m \equiv c^d (mod\ n)$ sehingga penerima mendapatkan plainteks awal yang sesuai dengan pesan yang di kirim oleh pengirim.

4.2.2 Simulasi Algoritma Dekompresi Kode Huffman dengan Dekripsi Algoritma RSA

Berikut proses dekompresi menggunakan kode Huffman pada pesan teks sebagai berikut :

1. Pesan Teks 8 Karakter

   Langkah-langkah dalam proses dekompresi sebagai berikut:

   a. Membaca sebuah bit dari *string* biner yang dimulai dari akar pohon Huffman pada gambar 4.1.

b. Setiap bit dari *string* biner lakukan secara tranversal pada cabang yang bersesuaian.Label 0 lihat cabang kiri pada pohon Huffman, sedangkan label 1 lihat cabang kanan pada pohon Huffman. Maka dari kode Huffman 00100101000111001111 dihasilkan cipherteks hasil dekompresi yaitu vmevabap.

2. Pesan Teks 10 Karakter

Langkah-langkah dalam proses dekompresi sebagai berikut:

a. Membaca sebuah bit dari *string* biner yang dimulai dari akar pohon Huffman pada gambar 4.2.

b. Setiap bit dari *string* biner lakukan secara tranversal pada cabang yang bersesuaian. Label 0 lihat cabang kiri pada pohon Huffman, sedangkan label 1 lihat cabang kanan pada pohon Huffman. Maka dari kode Huffman 1100011001010011100010011010101 1 dihasilkan cipherteks hasil dekompresi yaitu DCDBLJOAZK.

3. Pesan Teks 12 Karakter

Langkah-langkah dalam proses dekompresi sebagai berikut:

a. Membaca sebuah bit dari *string* biner yang dimulai dari akar pohon Huffman pada gambar 4.3.

b. Setiap bit dari *string* biner lakukan secara tranversal pada cabang yang bersesuaian. Label 0 lihat cabang kiri pada pohon Huffman, sedangkan label 1 lihat cabang kanan pada pohon Huffman.Maka dari kode Huffman 11101111100101000001010100110101011110 dihasilkan cipherteks hasil dekompresi yaitu tisbgdqsabwa.

4. Pesan Teks 14 Karakter

Langkah-langkah dalam proses dekompresi sebagai berikut:

a. Membaca sebuah bit dari *string* biner yang dimulai dari akar pohon Huffman pada gambar 4.4.

b. Setiap bit dari *string* biner lakukan secara tranversal pada cabang yang bersesuaian.Label 0 lihat cabang kiri pada pohon Huffman, sedangkan label 1 lihat cabang kanan pada pohon Huffman.Maka dari kode Huffman 0100111000100101010101011110011011110011111100001 dihasilkan cipherteks hasil dekompresi yaitu OKBMOGRJTSKPAU.

5. Pesan Teks 16 Karakter

Langkah-langkah dalam proses dekompresi sebagai berikut:

a. Membaca sebuah bit dari *string* biner yang dimulai dari akar pohon Huffman pada gambar 4.5.

b. Setiap bit dari *string* biner lakukan secara tranversal pada cabang yang bersesuaian. Label 0 lihat cabang kiri pada pohon Huffman, sedangkan label 1 lihat cabang kanan pada pohon Huffman. Maka dari kode Huffman1010000101100101001101010000101100011001101100111 01111 dihasilkan cipherteks hasil dekompresi yaitu DKWTFEFNTEKUCNXS.

Setelah melakukan proses dekompresi yaitu proses dekripsi algoritma RSA pada pesan teks sebagai berikut :

1. Pesan Teks 8 Karakter

   Cipherteks $C =$ ‘vmevabap’ yang telah dikodekan(spasi diabaikan) dari hasil proses enkripsi menjadi $C = 2190044700010015$

   Pecah C menjadi 4 digit blok, maka:

   c_1 = 2190

   c_2= 0447

   c_3= 0001

   c_4= 0015

   Dekripsi dengan kunci rahasia d = 1829

   $m_1 \equiv 2190^{1829}$ $(mod\ 3239)$ = 0015

   $m_2 \equiv 447^{1829}$ $(mod\ 3239)$ = 0010

   $m_3 \equiv 1^{1829}$ $(mod\ 3239)$ = 0001

   $m_4 \equiv 15^{1829}$ $(mod\ 3239)$ = 0017

   Maka diperoleh plainteks M = 0015 0010 0001 0017 dengan melihat tabel huruf alfabet maka di dapatkan hasil plainteks ‘apa kabar’.

2. Pesan Teks 10 Karakter

   Cipherteks $C =$ ‘VEELVTPQLA’ yang telah dikodekan(spasi diabaikan) dari hasil proses enkripsi menjadi $C = 21040411211915161152$

   Pecah C menjadi 4 digit blok, maka:

   c_1 = 2104

   c_2= 0411

   c_3= 2119

c_4= 1516

c_5= 1152

Dekripsi dengan kunci rahasia d = 1019

$m_1 \equiv 2104^{1019}$ (mod 3337) = 0704

$m_2 \equiv 0411^{1019}$ (mod 3337) = 1111

$m_3 \equiv 2119^{1019}$ (mod 3337) = 1419

$m_4 \equiv 1516^{1019}$ (mod 3337) = 2006

$m_5 \equiv 1152^{1019}$ (mod 3337) = 0018

Maka diperoleh plainteks M = 0704 1111 1419 2006 0018 dengan melihat tabel huruf alfabet maka di dapatkan hasil plainteks ‘HELLO TUGAS’.

3. Pesan Teks 12 Karakter

Cipherteks $C =$ ‘tisbgdqsabwa’ yang telah dikodekan(spasi diabaikan) dari hasil proses enkripsi menjadi C =196044533255429600012226

Pecah C menjadi 4 digit blok, maka:

c_1 = 1960

c_2= 4453

c_3= 3255

c_4= 4296

c_5= 0001

c_6= 2226

Dekripsi dengan kunci rahasia d = 763

$m_1 \equiv 1960^{763}$ (mod 5063) =1000

$m_2 \equiv 4453^{763}$ (mod 5063) = 1220

$m_3 \equiv 3255^{763}$ (mod 5063) = 0015

$m_4 \equiv 4296^{763} (mod\ 5063) = 0010$

$m_5 \equiv 1^{763} (mod\ 5063) = 0001$

$m_6 \equiv 2226^{763} (mod\ 5063) = 0017$

Maka diperoleh plainteks M = 1000 1220 0015 0010 0001 0017 dengan melihat tabel huruf alfabet maka di dapatkan hasil plainteks ’kamu apa kabar’.

4. Pesan Teks 14 Karakter

Cipherteks C =‘OKBMOGRJTSKPAU’ yang telah dikodekan (spasi diabaikan) dari hasil proses enkripsi menjadi

C = 1410 0150 1458 1709 1970 1067 0046

Pecah C menjadi 4 digit blok, maka:

c_1 = 1410

c_2= 0150

c_3= 1458

c_4= 1709

c_5= 1970

c_6= 1067

c_7= 0046

Dekripsi dengan kunci rahasia d = 1589

$m_1 \equiv 1410^{1589} (mod\ 2993) = 1904$

$m_2 \equiv 0150^{1589} (mod\ 2993) = 1900$

$m_3 \equiv 1458^{1589} (mod\ 2993) = 1501$

$m_4 \equiv 1709^{1589} (mod\ 2993) = 0417$

$m_5 \equiv 1970^{1589} (mod\ 2993) = 1824$

$m_6 \equiv 1067^{1589} (mod\ 2993) = 2010$

$m_7 \equiv 0046^{1589} (mod\ 2993) = 2017$

Maka diperoleh plainteks: M = 1904 1900 1501 0417 1824 2010 2017 dengan melihat tabel huruf alfabet maka di dapatkan hasil plainteks ’TETAP BERSYUKUR’.

5. Pesan Teks 16 Karakter

Cipherteks $C =$ DKWTFEFNTEKUCNXS yang telah dikodekan(spasi diabaikan) dari hasil proses enkripsi menjadi

$C =$ 2988 2219 3130 0513 1904 3672 2865 2396

Pecah C menjadi 4 digit blok, maka:

c_1 = 2988

c_2= 2219

c_3= 3130

c_4= 0513

c_5= 1904

c_6= 3672

c_7= 2865

c_8= 2396

Dekripsi dengan kunci rahasia d = 2279

$m_1 \equiv 2988^{2279} (mod\ 3869) = 0104$

$m_2 \equiv 2219^{2279} (mod\ 3869) = 1712$

$m_3 \equiv 3130^{2279} (mod\ 3869) = 0008$

$m_4 \equiv 0513^{2279} (mod\ 3869) = 1318$

$m_5 \equiv 1904^{2279} (mod\ 3869) = 0415$

$m_6 \equiv 3672^{2279}\ (mod\ 3869) = 0010$

$m_7 \equiv 2865^{2279}\ (mod\ 3869) = 0114$

$m_8 \equiv 2396^{2279}\ (mod\ 3869) = 1100$

Maka diperoleh plainteks: M = 0104 1712 0008 1318 0415 0010 0114 1100 dengan melihat tabel huruf alfabet maka di dapatkan hasil plainteks 'BERMAIN SEPAKBOLA'.

Setelah melakukan 10 Kali uji coba yaitu 5 kali menggunakan ASCII dan 5 kali menggunakan kode Huffman didapatkan hasil berikut:

Perbedaan	ASCII	Kode Huffman	Rasio Kompresi (%)
8 huruf	64	20	31,25%
10 huruf	80	28	40%
12 huruf	96	38	39,58%
14 huruf	112	50	44,64%
16 huruf	122	54	42,19%
Rata-Rata			39,53 %

Tabel 4.12 Kode ASCII dan Kode Huffman

Setelah melakukan huruf yang berjumlah genap dari 8 huruf sampai 16 huruf, dapat disimpulkan kode Huffman lebih efisien 39,53 % dari pada kode ASCII. Dengan demikian, rata-rata perbedaan menggunakan kode Huffman dan kode ASCII adalah 39,53%. Kode Huffman lebih efisien dalam menyandikan pesan teks.

4.3 Kajian Keislaman dengan Hasil Penelitian

Kemajuan teknologi seiring berkembangnya zaman semakin pesat salah satunya dalam menyampaikan sebuah pesan. Pesan yang disampaikan akan dikirimkan dari suatu tempat ke tempat lain, sehingga terdapat kemungkinan bahwa pesan yang di kirim dapat diambil atau diakses oleh pihak-pihak yang tidak bertanggung jawab, oleh karena itu perlu dilakukan penyandian terhadap pesan tersebut. Tujuan dari penyandian pesan yaitu untuk melindungi suatu pesan dari orang yang tidak berhak menerimanya. Menjaga kerahasiaan suatu pesan termasuk dalam amanah yang harus dijaga dengan sebaik-baiknya, sebagaimana dalam Al-Quran surat An-Nisa' ayat 58:

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

Berdasarkan pada surat An-Nisa' ayat 58, agar pesan dapat disampaikan kepada orang yang berhak menerimanya maka dilakukan penyandian terhadap pesan tersebut. Untuk memperkuat keamanan pada pesan, dapat dilakukan penyandian dengan menggunakan teknik penyandian pesan seperti algoritma asimetri menggunakan metode algoritma RSA yang akan digunakan untuk mengamankan kunci pesan dengan mengubah kunci pesan asli kedalam bentuk pesan yang tidak dapat dipecahkan seperti isi pesan dalam surat yang dikirim oleh Nabi Sulaiman kepada Ratu Balqis sebagaimana disebutkan dalam Al-Quran surat An-Naml ayat 32:

Artinya:"Dia (Balqis) berkata,"Wahai para pembesar! Berilah aku pertimbangan dalam perkaraku (ini). Aku tidak pernah memutuskan suatu perkara sebelum kamu hadir dalam majelis(ku)"(QS. An-Naml:32).

Berdasarkan pada surat An-Naml ayat 32 bahwa setelah Ratu Balqis membacakan surat Nabi Sulaiman kepada para pembesar kerajaannya, isi pesan dalam surat tersebut sulit untuk dipecahkan sehingga Ratu Balqis meminta saran dari para pembesar tentang apa yang harus Ratu Balqis lakukan dengan bermusyawarah.

Begitupula dengan algoritma RSA mengimplementasikan enkripsi dan dekripsi pesan yang bertujuan untuk mengamankan dengan menyepakati suatu kunci rahasia yang sama antara pengirim pesan dengan penerima pesan. Sehingga menyandikan pesan dengan menggunakan kode Huffman pada algoritma RSA diharapkan dapat menjaga keamanan pesan dengan lebih baik, sehingga tetap terjaga keamanannya dari orang yang tidak berhak menerimanya.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil Pembahasan dapat ditarik kesimpulan sebagai berikut:

1. Pada proses enkripsi pesan yang dilakukan menggunakan metode Algoritma RSA dengan indeks 26 karakter yang kemudian di kompresi menggunakan kode Huffman. Dalam proses enkripsi tersebut menetapkan indeks karakter dari plainteks dan melakukan perhitungan untuk proses enkripsi dengan rumus $c \equiv m^e (mod\ n)$ menghasilkan cipherteks dengan menggunakan kunci publik. Setelah itu dilanjutkan proses kompresi yang dilakukan oleh kode Huffman.
2. Pada proses dekompresi untuk mengembalikan cipherteks ke bentuk pesan aslinya (plainteks) dengan melakukan proses dekompresi menggunakan metode kode Huffman yang kemudian dilanjutkan dengan metode proses dekripsi algoritma RSA dengan rumus $m \equiv c^d (mod\ n)$ dengan menggunakan kunci privat.
3. Proses enkripsi dengan beberapa karakter menggunakan kompresi kode Huffman berhasil diterapkan pada algoritma RSA. Perbandingan rasio kompresi menggunakan kode Huffman pada algoritma RSA adalah 39,53%, sehingga dapat diketahui bahwa kode Huffman lebih efisien dalam menyandikan pesan teks.

5.2 Saran

Dalam penelitian selanjutnya untuk metode algoritma RSA dan kode Huffman disarankan untuk menggunakan kunci dan karakter yang lebih bervariasi dan lebih banyak agar lebih aman dan sulit di pecahkan atau dapat dikombinasikan dengan kriptografi klasik lainnya.

DAFTAR PUSTAKA

Abdussakir. (2009). *Kajian Integratif Matematika dan Al-Qur'an.* Malang: UIN-Maliki Press.

Al-Qurthubi, S. I. (2009). *Tafsir Al Qurthubi.* Jakarta: Pustaka Azzam.

Andika, T., M.Taquyuddin, & Admizal, I. (2020). Amanah dan Khianat Dalam Al-Quran Menurut Quraish Shihab. *Ilmu Al-Quran dan Tafsir*, 188.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi.* Yogyakarta: C.V Andi Offset.

Astuti, E. Z., & Hidayat, E. Y. (2013). Kode Huffman Untuk Kompresi Pesan. *Techno.COM*, 117-126.

Fauji, S. A., Pradana, M. S., & Azhari, N. A. (2016). Penerapan Kode Huffman pada Algoritma RSA (Rivest-Shamir-Adleman)Untuk Menyandikan Password Email. *Jurnal UJMC*, 42.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untuk enkripsi dan dekripsi email. *Teknologi dan sistem komputer*, 254.

Heru Nugroho, S. (2015). *Matematika Diskrit dan Implementasinya Dalam Dunia Teknologi Informasi.* Yogyakarta: Deepublish.

Muhsetyo, G. (2014). *Teori Bilangan.* Tangerang Selatan: Universitas Terbuka.

Munir, R. (2009). *Matematika Diskrit.* Bandung: Informatika.

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

Sa'adah, N. (2009). *Penerapan Teori Biner Pada Kode Huffman.* Malang: Undergraduate thesis,Universitas Islam Negeri Maulana Malik Ibrahim.

Sadikin, R. (2012). *Kriptografi.* Yogyakarta: C.V Andi Offset.

Sadikin, R. (2012). *Kriptografi untuk keamanan jaringan.* Yogyakarta: Andi Offset.

Taufik, M. (1999). *Pengantar Ilmu Bilangan.* Malang: UMM Press.

Timothy John Pattiasina, S. M. (t.thn.). Analisa Kode Huffman Untuk Kompresi Data Teks. *Teknika*, 2.

Wahyu Henky Irawan, M. (2014). *Pengantar Teori Bilangan.* Malang: UIN-Maliki Press.

LAMPIRAN

Lampiran 1 Tabel Alfabet

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
00	01	02	03	04	05	06	07	08	09	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Lampiran 2 Tabel ASCII

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

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

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

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

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

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

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

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

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

RIWAYAT HIDUP

Andini Khairunnisa, lahir di kabupaten Malang pada tanggal 05 Oktober 1999, biasa dipanggil Andin. Penulis tinggal di desa Baturetno, kecamatan Singosari, Kabupaten Malang. Anak pertama dari tiga bersaudara dari pasangan bapak Setu Udoyono dan ibu Etik Hendartik.

Pendidikan dasar ditempuh di SD Islam Al-Ma'arif 01 (2006-2012), kemudian melanjutkan pendidikan menengah pertama di SMPN 2 Singosari (2012-2015), kemudian pendidikan menengah atas di SMAN 1 Singosari (2015-2018) dan tahun 2018 penulis mulai menempuh kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil program studi matematika.

Selama menjadi mahasiswa, penulis berperan cukup aktif dalam bidang komunitas dan pelatihan di luar kampus. Pada tahun 2019 penulis tergabung dalam komunitas bahasa inggris UIN Malang (MEC). Pada tahun 2020 penulis mengikuti pelatihan bersertifikat training of Fundamental Hypnosis sehingga penulis mendapatkan gelar C.FH.

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 : Andini Khairunnisa
NIM : 18610048
Fakultas / Program Studi : Sains dan Teknologi / Matematika
Judul Skripsi : Penerapan Kompresi Menggunakan Kode Huffman Pada Algoritma RSA(Rivest Shamir Adleman) untuk Menyandikan Pesan Teks
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Erna Herawati, M.Pd

No	Tanggal	Hal	Tanda Tangan
1.	10-Maret 2022	Konsultasi Bab I dan II	1.
2.	17- Maret 2022	Revisi Bab I dan II	2.
3.	19-Maret 2022	Konsultasi Kajian Agama	3.
4.	6- April 2022	Konsultasi Bab III	4.
5.	11- April 2022	Revisi Bab III	5.
6.	13- April 2022	ACC Bab I,II,III	6.
7.	11- Oktober 2022	Konsultasi Bab IV dan V	7.
8.	19- Oktober 2022	Revisi Bab IV dan V	8.
9.	25-Oktober 2022	Konsultasi Kajian Agama	9.
10.	01- November 2022	Revisi Kajian Agama	10.
11.	07- November 2022	Konsultasi Kajian Agama	11.
12.	15-November 2022	Revisi Kajian Agama	12.
13.	18-November 2022	ACC Kajian Agama	13.
14.	21-November 2022	Konsultasi Bab IV dan V	14.
15.	28-November 2022	ACC Bab IV dan V	15.
16.	2 Desember 2022	ACC Keseluruhan	16.

Malang, 28 Desember 2022
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP.197411292000122005