KAJIAN MATEMATIS DAN PENGGUNAAN BILANGAN PRIMA PADA ALGORITMA KRIPTOGRAFI RSA (RIVEST, SHAMIR, DAN ADLEMAN) DAN ALGORITMA KRIPTOGRAFI ELGAMAL

SKRIPSI

OLEH
FAURIZAL FAHMI FIRMANSYAH
NIM. 09610106

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2015

KAJIAN MATEMATIS DAN PENGGUNAAN BILANGAN PRIMA PADA ALGORITMA KRIPTOGRAFI RSA (RIVEST, SHAMIR, DAN ADLEMAN) DAN ALGORITMA KRIPTOGRAFI ELGAMAL

SKRIPSI

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

Oleh
Faurizal Fahmi Firmansyah
NIM. 09610106

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2015

KAJIAN MATEMATIS DAN PENGGUNAAN BILANGAN PRIMA PADA ALGORITMA KRIPTOGRAFI RSA (RIVEST, SHAMIR, DAN ADLEMAN) DAN ALGORITMA KRIPTOGRAFI ELGAMAL

SKRIPSI

Oleh
Faurizal Fahmi Firmansyah
NIM. 09610106

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 12 November 2014

Pembimbing I,	Pembimbing II,
H. Wahyu H. Irawan, M.Pd	Abdul Aziz, M.Si
NIP. 19710420 200003 1 003	NIP. 19760318 200604 1 002

Mengetahui,
Ketua Jurusan Matematika

Dr. Abdussakir, M.Pd
NIP. 19751006 200312 1 001

KAJIAN MATEMATIS DAN PENGGUNAAN BILANGAN PRIMA PADA ALGORITMA KRIPTOGRAFI RSA (RIVEST, SHAMIR, DAN ADLEMAN) DAN ALGORITMA KRIPTOGRAFI ELGAMAL

SKRIPSI

Oleh
Faurizal Fahmi Firmansyah
NIM. 09610106

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Sains (S.Si)
Tanggal 07 Januari 2015

Penguji Utama	:	Dr. Abdussakir, M.Pd	.....
Ketua Penguji	:	Drs. H. Turmudi, M.Si	.....
Sekretaris Penguji	:	H. Wahyu H. Irawan, M.Pd	.....
Anggota Penguji	:	Abdul Aziz, M.Si	.....

Mengetahui,
Ketua Jurusan Matematika

Dr. Abdussakir, M.Pd
NIP. 19751006 200312 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Faurizal Fahmi Firmansyah

NIM : 09610106

Jurusan : Matematika

Fakultas/Jurusan : Sains danTeknologi

Judul Penelitian : Kajian Matematis dan Penggunaan Bilangan Prima Pada Algoritma Kriptografi RSA (Rivest, Shamir, dan Adleman) dan Algoritma Kriptografi Elgamal

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

Malang, 20 Januari 2015
Yang Membuat Pernyataan,

Faurizal Fahmi Firmansyah
NIM. 09610106

MOTO

"Tidak ada kata terlambat untuk meraih sebuah kesuksesan,
selagi kita mau berusaha sekuat tenaga dan berdoa"

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Ayahanda Imam Sutrisno dan Ibunda Rofiqoh,

yang telah mengorbankan seluruh hidupnya untuk penulis.

Serta kepada kakak tercinta Ulfah Fitri Umayroh dan adik tercinta

Sindi Lucita Sari atas dukungan dan doanya yang selalu memberikan semangat

kepada penulis.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Sw tatas rahmat, taufik, serta hidayah-Nya sehingga penulis mampu menyelesaikan penyusunan skripsi ini sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak. Untuk itu ucapan terimakasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya penulis sampaikan terutama kepada:

1. Prof. Dr. H. Mudjia Rahardjo, M.Si, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. drh. Bayyinatul Muchtaromah, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Abdussakir, M.Pd, selaku ketua Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. H. Wahyu H. Irawan, M.Pd, selaku dosen pembimbing I yang telah memberikan saran, bantuan, dan bimbingannya selama penulisan skripsi ini dengan sabar sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
5. Abdul Aziz, M.Si, selaku dosen pembimbing II yang telah banyak memberikan arahan dan berbagi ilmunya kepada penulis.
6. Hairur Rahman, M.Si, selaku dosen wali yang telah membimbing dan memberi arahan dari semester awal hingga akhir.

7. Seluruh dosen dan staf administrasi Jurusan Matematika Fakultas Sains dan Teknologi yang telah bersabar dalam memberikan ilmu dan bimbingannya.
8. Keluarga tercinta Imam Sutrisno, Rofiqoh, selaku ayah dan ibu penulis, serta Ulfah Fitri Umayroh dan Sindi Lucita Sari selaku kakak dan adik penulis yang memberikan dukungan semangat dan doa sehingga penulisan skripsi ini dapat terselesaikan.
9. Seluruh teman-teman seperjuangan Jurusan Matematika angkatan 2009 yang telah memberikan dukungan kepada penulis dalam menyelesaikan skripsi ini.
10. Semua pihak yang telah membantu penulis, yang tidak dapat disebutkan satu persatu.

Akhirnya penulis berharap semoga skripsi ini bermanfaat bagi penulis dan bagi pembaca

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, Januari 2015

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SIMBOL

Simbol-simbol yang digunakan dalam skripsi ini mempunyai makna yaitu sebagai berikut:

$\mathbb{Z}^+$	: Bilangan bulat positif
$\mathbb{Z}^-$	: Bilangan bulat negatif
$(\mathbb{Z}, +, \cdot)$	: Himpunan bilangan bulat dilengkapi dengan dua buah operasi, yaitu operasi penjumlahan dan perkalian
$a \in \mathbb{Z}$	: a anggota bilangan bulat
$a \mid b$	: a membagi b
$a \nmid b$	: a tidak membagi b
$a \equiv b$	: a kongruen dengan b
$a \pmod{p}$	: a modulo p
$\phi(n)$	: Fungsi euler dari n
$\sum_{i=0}^{k} a_i$	: Penjumlahan $a_0 + a_1 + a_2 + \cdots + a_k$
$\prod_{i=0}^{k} a_i$	: Perkalian $a_0 a_1 a_2 \ldots a_k$
RSA	: Rivest, Shamir, dan Adleman
m	: Pesan yang bias dibaca (Plainteks)
c	: Pesan yang tidak bias dibaca (Chiperteks)

ABSTRAK

Firmansyah, Faurizal.F. 2015. **Kajian Matematis dan Penggunaan Bilangan Prima Pada Algoritma Kriptografi RSA dan Algoritma Kriptografi Elgamal**. Skripsi. Jurusan Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) H. Wahyu H. Irawan, M.Pd. (II) Abdul Aziz, M.Si

Kata kunci: algoritma RSA, algoritmaElgamal, bilangan prima, dekripsi, enkripsi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat lain. Algoritma kriptografi RSA dan algoritma kriptografi Elgamal merupakan jenis algoritma kriptografi asimetri, dengan arti kata kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi berbeda. Enkripsi sendiri adalah proses pembentukan plainteks (pesan yang bias dibaca) menjadi chiperteks (pesan yang tidak bias dibaca), sedangkan dekripsi adalah proses pembentukan chiperteks menjad plainteks.

Tujuan dari penelitian ini adalah mengetahui penggunaan bilangan prima pada algoritma kriptografi RSA dan algoritma kriptografi Elgamal. Hasil dari penelitian ini adalah:

1. Pada algoritma kriptografi RSA dengan menggunakan bilangan prima aman maupun bilangan prima tidak aman, proses pembentukan kunci, proses enkripsi, dan proses dekripsi tetap dapat berjalan dengan baik. Dan proses enkripsi algoritma kriptografi RSA diperoleh dari rumus $c_i = {m_i}^e \bmod n$, sedangkan proses dekripsi algoritma kriptografi RSA diperoleh dari rumus $m_i = {c_i}^d \bmod n$
2. Pada algoritma kriptografi Elgamal dengan menggunakan bilangan prima aman maupun bilangan prima tidak aman, proses pembentukan kunci, proses enkripsi, dan proses dekripsi juga tetap dapat berjalan dengan baik. Dan proses enkrips ialgoritma kriptografi Elgamal diperoleh dari rumus $a = g^k \pmod p$ dan $b = y^k\, m \pmod p$ sedangakan proses dekripsi algoritma Elgamal diperoleh dari rumus $a^{-x} = a^{p-1-x} \pmod p$ dan $m = b \,.\, (a^x)^{-1} \pmod p$

ABSTRACT

Firmansyah, Faurizal.F. 2015. **Mathematic Study and Use of Prime Numbers on RSA Cryptographic Algorithms and Elgamal cryptography algorithm**. Thesis. Department of Mathematics, Faculty of Science and Technology, State Islamic University Maulana Malik Ibrahim Malang: (I) H.Wahyu H. Irawan, M.Pd (II) AbdulAziz, M.Si

Keywords: RSA Algorithms, Elgamal Algorithms, prime numbers, decryption, encryption

Cryptography is a science and art to secure of the message during sending from one place to another. RSA cryptographic algorithm and Elgamal cryptographic algorithm are types of asymmetric cryptography algorithm, by mean the key used to perform encryption and decryption process is different. Encryption is the process of establishing plaintext (verbosity) into ciphertext (ureadable message), while decryption is the process of forming ciphertext into plaintext.

The purpose of this study is to determine the use of primes number on cryptographic algorithm RSA and Elgamal cryptographic algorithms. The results of this study are:

1. On the RSA cryptographic algorithm using safe and unsafe prime numbers, the process of forming a key, the encryption, and decryption processes can still run well . And the RSA encryption algorithm process is obtained from the formula $c_i = m_i^e \bmod n$, while the cryptographic algorithm RSA decryption process is obtained from $m_i = c_i^d \bmod n$
2. On the Elgamal cryptographic algorithm using safe and unsafe prime numbers, the process of forming a key, the encryption, and decryption processes can still run well. And the Elgamal encryption algorithm process is obtained from the formula $a = g^k \pmod p$and $b = y^k\ m \pmod p$while the cryptographic algorithm Elgamal decryption process is obtained from the formula$a^{-x} = a^{p-1-x} \pmod p$ and $m = b\ .\ (a^x)^{-1} \pmod p$

ملخص

فيرمان، فاوريزال ، ف ، عام ٢٠١٥. **دراسة الرياضيات واستخدام الأعداد الأولية في التشفير خوارزمية RSAوخوارزمية التشفير الجمل.** بحث جامعي. الشعبه الرياضيات كلية العلوم والتكنولوجيا، الجامعة الإسلامية الحكومية مولانا مالك إبراهيم مالانج. المشرف:(١) الحاج وحيو ه. إروان الماجستير ،(٢) عبد العزيزالماجستير

الكلمات الرئيسية : التشفيرRSA، تشفير الجمل، والتشفير، فك التشفير، الأعداد الأولية

خوارزمية التشفيرRSAو خوارزمية التشفير الجمل هي نوع من خوارزمية التشفير غير المتماثلة. وغالبا يشر خوارزميات التشفير غير المتماثلة كخوارزمية المفتاح العمومي مع معنى المفتاح المستخدمة لأداء عملية التشفير و فك التشفير هو مختلف. التشفير هو عملية ترسيخ غير مشفرة (الإسهاب) فى النص المشفر (لا يمكن قراءتها)، وكان فك التشفير هو عملية تشكي النص المشفر إلى نص غير مشفر.

وكان الغرض من هذه الدراسة لتحديد المفاهيم الرياضية واستخدام يعي على خوارزمية التشفيرRSAوالجمل خوارزميات التشفير. نتائج هذه الدراسة هي:

١يتم الحصول على خوارزمية التشفيرRSAعملية التشفير منالصيغة $c_i = m_i{}^e \bmod n$، خوارزمية التشفير الجمل المستمدة منالصيغة $a = g^k \pmod p$، $b = y^k m \pmod p$

٢.يتم الحصول على خوارزمية التشفيرRSAعملية فك التشفير من الصيغة $m_i = c_i{}^d \bmod n$ ، في حين يتم الحصول على عملية فك التشفير خوارزمية الجمل من الصيغة $a^{-x} = a^{p-1-x} \pmod p$و $m = b \cdot (a^x)^{-1} \pmod p$

BAB I

PENDAHULUAN

1.1 Latar Belakang

Matematika adalah ilmu yang mendasari algoritma kriptografi. Kriptografi dengan kunci asimetrik atau kriptografi kunci publik berbasis pada teori bilangan. Hal itu membuktikan bahwa matematika sebagai ilmu pengetahuan dasar yang memegang peranan sangat penting dalam perkembangan ilmu pengetahuan lain di dunia.

Perkembangan teknologi informasi semakin memudahkan penggunanya dalam berkomunikasi melalui bermacam-macam media. Komunikasi yang melibatkan pengiriman dan penerimaan pesan dengan memanfaatkan kemajuan teknologi informasi rentan terhadap pelaku kejahatan komputer yang memanfatkan celah keamanan untuk mendeteksi dan memanipulasi pesan. Keamanan dan kerahasiaan pesan menjadi aspek yang sangat penting bagi pengguna teknologi informasi. Untuk menghindari pesan yang dikirimkan jatuh pada pihak-pihak yang tidak berkepentingan dan terjadi penyalahgunaan terhadap pesan, diharapkan bagi pengguna teknologi informasi memiliki cara untuk melindungi pesan rahasia tersebut agar tidak jatuh kepada pihak-pihak yang tidak berhak menerima pesan rahasia tersebut, yaitu dengan cara melakukan enkripsi terhadap pesan tersebut, agar pesan tersebut tidak dapat dibaca dengan pihak lain. Pernyataan tersebut, sesuai dengan firman Allah pada Surat al-Anfal ayat60 :

وَأَعِدُّواْ لَهُم مَّا ٱسۡتَطَعۡتُم مِّن قُوَّةٖ وَمِن رِّبَاطِ ٱلۡخَيۡلِ تُرۡهِبُونَ بِهِۦ عَدُوَّ ٱللَّهِ وَعَدُوَّكُمۡ وَءَاخَرِينَ مِن دُونِهِمۡ لَا تَعۡلَمُونَهُمُ ٱللَّهُ يَعۡلَمُهُمۡۚ وَمَا تُنفِقُواْ مِن شَيۡءٖ فِي سَبِيلِ ٱللَّهِ يُوَفَّ إِلَيۡكُمۡ وَأَنتُمۡ لَا تُظۡلَمُونَ ٦٠

"Siapkanlah untuk menghadapi mereka kekuatan apa saja yang kalian sanggupi dan dari kuda-kuda yang ditambatkan untuk berperang (yang dengan persiapan itu) kalian menggentarkan musuh Allah dan musuh kalian serta orang-orang selain mereka yang tidak kalian ketahuisedangkan Allah mengetahuinya".(QS. al-Anfal/8:60)

Ayat ini menunjukkan bahwa umat Islam diperintahkan untuk memiliki perlengkapan apapun yang bisa menjadikan musuh-musuh mereka gentar. Maka dari itu untuk pengguna teknologi informasi agar pesan rahasia kita aman dan tidak bisa dibaca oleh pihak lain harus memiliki cara agar pesan rahasia tersebut aman yaitu dengan cara menggunakan kriptografi.

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan.Pada pengertian modern, kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan dan keutuhan data. Jadi pengertian kriptografi modern adalah tidak saja berurusan dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi (Sadikin, 2012:9).

Pada kriptografi modern terdapat berbagai macam algoritma yang bertujuan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma dari kriptografi modern terdiri atas dua bagian yaitu algoritma simetrik dan algoritma asimetrik. Algoritma simetrik adalah algoritma yang menggunakan satu kunci saja untuk mengenkripsi dan mendekripsi pesan. Sedangkan algoritma asimetrik adalah

algoritma yang menggunakan dua kunci untuk mengenkripsi dan mendekripsi pesan.Algoritma yang menggunakan kunci asimetrik atau kunci publik adalah algoritma RSA dan algoritma Elgamal.

Pada tahun 1977, Rivest, Shamir, dan Adleman merumuskan algoritma praktis yang mengimplementasikan sistem kriptografi kunci publik disebut dengan sistem kriptografi RSA. Meskipun pada tahun 1997 badan sandi Inggris memublikasikan bahwa Clifford Cock telah merumuskan sistem kriptografi RSA 3 tahun lebih dahulu daripada Rivest, Shamir, dan Adleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima (Sadikin, 2012:249).

Algoritma kunci publik lainnya adalah algoritma kriptografi kunci publik Elgamal. Penemu sistem kriptografi ini adalah Taher Elgamal pada tahun 1984. Sistem kriptografi Elgamal bersandar pada asumsi kesulitan persoalan logaritma diskrit (Sadikin, 2012:271).

Berdasarkan penjelasan diatas yang menjelaskan kriptografi bersandarkan pada teknik matematika.Maka peneliti mencoba mengkaji perumusan algoritma kriptografi RSA dan algoritma Kriptografi Elgamal dengan teorema-teorema yang sudah ada pada matematika.Oleh karena itu, pada skripsi ini penulis akan menganalisis permasalahan tersebut dengan judul "Kajian Matematis dan Penggunaan Bilangan Prima Pada Algoritma Kriptografi RSA (Rivest, Shamir, dan Adleman) dan Algoritma Kriptografi Elgamal".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, masalah yang dibahas dalam penulisan skripsi ini adalah:

1. Bagaimana penggunaan bilangan prima dalam perumusan algoritma kriptografi RSA?
2. Bagaimana penggunaan bilangan prima dalam perumusan algoritma kriptografi Elgamal?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan penelitian ini adalah:

1. Mengetahui hasil penggunaan bilangan prima dalam perumusan algoritma kriptografi RSA?
2. Mengetahui hasil penggunaan bilangan prima dalam perumusan algoritma kriptografi Elgamal?

1.4 Manfaat Penelitian

1. Bagi Peneliti

   Menambah wawasan penulis untuk mengetahui kajian matematis dan penggunaan bilangan prima pada algoritma kriptografi RSA (rivest, shamir, dan adleman) dan algoritma kriptografi elgamal.

2. Bagi lembaga UIN Maulana Malik Ibrahim Malang

   Sebagai tambahan informasi pembelajaran mata kuliah yang berhubungan dengan algoritma kriptografi RSA dan algoritma kriptografi Elgamal. Dan juga sebagai tambahan bahan kepustakaan.

3. Bagi Mahasiswa

   Menambah pengetahuan keilmuan mengenai algoritma kriptografi terutama algoritma kriptografi RSA dan algoritma kriptografi Elgamal.

1.5 Batasan Masalah

Untuk memfokuskan pada pembahasan tentang kajian matematis dan penggunaan bilangan prima pada algoritma kriptografi RSA dan algoritma kriptografi elgamal, skripsi ini terbatas pada konsep matematis pada pembentukan kunci menggunakan bilangan prima.

1.6 Sistematika Penulisan

Agar penelitian penelitian ini mudah dipahami, maka dalam sistematika penelitiannya dibentuk bab-bab yang di dalamnya terdapat beberapa subbab dengan rumusan sebagai berikut:

Bab I Pendahuluan

Pendahuluanmeliputi latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

Bab II Kajian Pustaka

Kajian pustaka meliputi teori-teori yang mendukung pembahasan.Teori-teori

tersebut berupa definisi dan teorema yang meliputi pengertian Bilangan bulat, keterbagian, sifat-sifat pembagian, aritmatika modulo dan kekongruenan, logaritma diskrit, dan bilangan prima.

Bab III Metode Penelitian

Metode penelitian meliputi jenis dan pendekatan penelitian, data dan sumber data, pengumpulan data, dan prosedur penelitian

Bab IV Pembahasan

Pada bab ini berisi tentang pembahasan perumusuan algoritma kriptografi RSA dan algoritma kriptografi Elgamal, kemudian diimplementasikan menggunakan bilangan prima.

Bab V Penutup

Penutup berisi tentang kesimpulan dari hasil penelitian dan saran sebagai acuan bagi peneliti selanjutnya.

BAB II

KAJIAN PUSTAKA

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Hubungan matematika dengan kriptografi sangat erat sekali, karena matematika adalah konsep dasar yang berhubungan dengan kriptografi terutama matematika diskrit. Dalam bab 2 ini, peneliti akan menjelaskan konsep matematis yang melandasi pembentukan algoritma kriptografi RSA dan kriptografi Elgamal, seperti teori bilangan bulat, keterbagian, sifat-sifat pembagian, algoritma euklid, aritmatika modulo, logaritma diskrit dan bilangan prima.

2.1 Teori Bilangan

Dalam pengertian yang ketat, kajian tentang sifat-sifat bilangan asli disebut dengan teori bilangan. Dalam pengertian yang lebih luas, teori bilangan mempelajari bilangan dan sifat-sifatnya. Sebagai salah satu cabang matematika, teori bilangan dapat disebut sebagai "aritmetika lanjut (*advanced aritmetics*)" karena terutama berkaitan dengan sifat-sifat bilangan asli (Muhsetyo, 1997:1).

Teori bilangan merupakan dasar perhitungan dan menjadi salah satu teori yang mendasari pemahaman kriptografi, khususnya sistem kriptografi kunci publik. Bilangan yang dimaksud hanyalah bilangan bulat *(integer).*

2.1.1 Bilangan Bulat

Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal.Himpunan semua bilangan bulat yang dinotasikan dengan $\mathbb{Z}$ yang diambil darikata *Zahlen* dari bahasa Jerman atau dinotasikan dengan I yang diambil dari huruf pertama kata *Integer* dari bahasa Inggris, adalah himpunan$\{\dots, -3, -2, -1,0,1,2,3 \dots\}$. Himpunan bilangan bulat dibagi tiga, yaitu bilangan bulat positif, yaitu bilangan bulat yang lebih besar dari nol yangdituliskan $\mathbb{Z}^+$, nol, dan bilangan bulat negatif, yaitu bilangan bulat yang lebih kecil dari nol yang dituliskan $\mathbb{Z}^-$(Abdussakir, 2009:102).

Himpunan bilangan bulat dilengkapi dengan dua buah operasi, yaitu operasi penjumlahan dan perkalian, dilambangkan $(\mathbb{Z}, +, \cdot)$ membentuk suatu sistem matematika yang disebut gelanggang atau ring (Abdussakir, 2009:102). Himpunan bilangan bulat berperan sangat penting dalam kriptografi karena banyak algoritma kriptografi yang menggunakan sifat-sifat himpunan bilangan bulat dalam melakukan proses penyandiannya.

2.1.1.1 Keterbagian

Sifat-sifat yang berkaitan dengan keterbagian *(divisibility)* merupakan dasar pengembangan teori bilangan. Jika suatu bilangan bulat dibagi oleh suatubilangan bulat yang lain, maka hasil pembagiannya adalah bilangan bulat atau bukan bilangan bulat (Muhsetyo, 1997:43).

Definisi 2.1

Misalnya $a, b \in \mathbb{Z}$dengan $a \neq 0$. a dikatakan membagi b, ditulis $a|b$, jika dan hanya jika $b = ax$, untuk suatu $x \in \mathbb{Z}$ (Abdussakir, 2009:114).

Ada beberapa hal yang dapat diambil dari definisi keterbagian di atas yaitu:

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

Contoh:

1. $4|12$, sebab ada $3 \in \mathbb{Z}$, sehingga $12 = 4 \cdot 3$
2. $15|60$, sebab ada $4 \in \mathbb{Z}$, sehingga $60 = 15 \cdot 4$

Teorema 2.1

Diberikan $a, b, c \in \mathbb{Z}$.

1. Jika $a|b$ maka $a|bx$ untuk setiap bilangan bulat x
2. Jika $a|b$ dan $b|c$ maka $a|c$
3. Jika $a|b$ dan $a|c$ maka $a|(bx + cy)$ untuk setiap $x, y \in \mathbb{Z}$
4. Jika $a|b$ dan $b|a$ maka $a = \pm b$
5. Jika $a|b$, $a > 0$, dan $b > 0$, maka $a \leq b$
6. Untuk setiap bilangan bulat $m \neq 0$, $a|b$ jika dan hanya jika $ma|mb$

(Abdussakir, 2009:115).

Bukti:

1. Jika $a|b$, maka ada $y \in \mathbb{Z}$, sehingga $b = ay$. Akibatnya, untuk setiap $x \in \mathbb{Z}$ diperoleh $bx = (ay)x = a(yx)$. Karena pada bilangan bulat berlaku sifat tertutup pada perkalian maka terdapat $p = yx \in \mathbb{Z}$. Sehingga berlaku $bx = ap$ jadi, $a|bx$.

2. Jika $a|b$, maka $b = ax$ untuk $x \in \mathbb{Z}$. Dan $b|c$, maka $c = by$ untuk $y \in \mathbb{Z}$. Diperoleh $c = by = a(xy)$, untuk suatu $xy \in \mathbb{Z}$. Jadi, $a|c$.
3. Jika $a|b$ maka $b = ap$ untuk $p \in \mathbb{Z}$. Dan $a|c$, maka $c = aq$ untuk $q \in \mathbb{Z}$. Akibatnya $bx = (ap)x$ untuk setiap $x \in \mathbb{Z}$dan $cy = (aq)y$ untuk setiap $q \in \mathbb{Z}$. Diperoleh $bx + cy = (ap)x + (aq)y = a(px + qy)$ untuk suatu $px + qy \in \mathbb{Z}$. Jadi, $a|(bx + cy)$.
4. Jika $a|b$, maka $b = ax$ untuk $x \in \mathbb{Z}$. Dan $b|a$, maka $a = by$ untuk $y \in \mathbb{Z}$. Diperoleh $b = ax = (by)x$ maka $b - b(yx) = b(1 - yx) = 0$ karena $b \neq 0$, maka $1 - yx = 0$ atau $xy = 1$. Diperoleh $x = y = 1$ atau $x = y = -1$ sehingga didapatkan $a = \pm b$.
5. Jika $a|b$, maka $b = ax$ untuk $x \in \mathbb{Z}$. Jika $a > 0, b > 0$ dan $b = ax$ maka $x > 0$ untuk $x = 1$ maka dipenuhi $a = b$. Sedangkan untuk $x > 1$ maka $b > a$. Jadi $a \leq b$.
6. Jika $a|b$, maka $b = ax$ untuk $x \in \mathbb{Z}$. Akibatnya untuk $m \in \mathbb{Z}$ dan $m \neq 0$ maka berlaku $mb = m(ax) = (ma)x$. Jadi $ma|mb$. Jika $ma|mb$ dan $m \neq 0$, maka $mb = (ma)x$ untuk suatu $x \in \mathbb{Z}$. $mb = (ma)x = m(ax)$ atau $mb - m(ax) = m(b - ax) = 0$. Karena $m \neq 0$, maka $b - ax = 0$ atau $b = ax$ untuk suatu $x \in \mathbb{Z}$. Jadi $a|b$

Definisi 2.2

Ditentukan $x,y \in \mathbb{Z}$, x dan y keduanya tidak bersama-sama bernilai 0. $a \in \mathbb{Z}$disebut pembagi (faktor) persekutuan (common divisor, common factor) dari x dan y jika $a|x$ (a membagi x) dan $a|y$ (a membagi y). $a \in \mathbb{Z}$disebut pembagi (faktor) persekutuan terbesar (gcd = *greatest common divisor*, gcf

= *greatest common factor*) dari *x* dan *y* jika *a* adalah bilangan bulat positif terbesar yang membagi x (yaitu $a|x$) dan membagi *y* (yaitu $a|y$)

Notasi:

d = (*x*,*y*) dibaca *d* adalah factor (pembagi) persekutuan terbesar dari *x* dan *y*d= (x_1, x_2, …., x_n) dibaca *d*adalah (pembagi) persekutuan terbesar dari x_1, x_2, …., x_n.

Perlu diperhatikan bahwa *d* = (*a*,*b*) didefinisikan untuk setiap pasang bilangan bulat *a*,*b* ∈ ℤ, kecuali *a* = 0 dan *b* = 0. Demikian pula, perlu dipahami bahwa (*a*,*b*) selalu bernilai bilangan bulat positif, yaitu *d* ∈ ℤ dan *d* > 0 (atau *d* ≥1) (Muhsetyo, 1997:60-61).

Contoh:

1. Himpunan semua faktor 16 adalah:

   A = {-16,-8,-4,-2,-1,1,2,4,8,16}

   Himpunan semua faktor 24 adalah:

   B = {-24,-12,-8,-6,-4,-3,-2,-1,1,2,3,4,6,8,12,24}

   Himpunan semua faktor persekutuan 16 dan 24 adalah:

   C = {,-8,-4,-2,-1,1,2,4,8}

   Karena unsure C yang terbesar adalah 8, maka (16,24) = 8

2.1.1.2 Bilangan Biner

Biner adalah sistem nomor yang digunakan oleh perangkat digital seperti komputer, pemutar cd, dan lain-lain. Sistem bilangan biner modern ditemukan oleh Gottfried Wilhelm Leibniz pada abad ke-17. Sistem bilangan biner atau yang disebut juga sistem bilangan basis dua adalah sebuah sistem bilangan yang

menggunakan dua simbol yaitu 0 dan 1.Dengan kata lain, biner hanya memiliki 2 angka yang berbeda (0 dan 1) untuk menunjukkan nilai, tidak seperti desimal yang memiliki 10 angka (0,1,2,3,4,5,6,7,8 dan 9).

Contoh dari bilangan biner adalah 10011100

Seperti yang dilihat pada contoh di atas hanya ada sekelompok angka 0 dan 1, keseluruhan 8 angka tersebut adalah bilangan biner 8 bit. Bit adalah singkatan dari Binary Digit, dan angka masing-masing digolongkan sebagai bit. Dalam istilah komputer, 1 byte = 8 bit.Kode-kode rancang bangun komputer seperti ASCII (*American Standart Code for Information Interchange*) juga menggunakan sistem pengkodean 1 byte (Buseng, 2013).

Untuk mengubah desimal ke biner hanya membagi nilai desimal dengan 2 dan kemudian menuliskan sisanya, ulangi proses ini sampai tidak bisa membagi dengan 2 lagi, misalnya nilai desimal 157:

157 ÷ 2 = 78 dengan sisa 1

78 ÷ 2 = 39 dengan sisa 0

39 ÷ 2 = 19 dengan sisa 1

19 ÷ 2 = 9 dengan sisa 1

9 ÷ 2 = 4 dengan sisa 1

4 ÷ 2 = 2 dengan sisa 0

2 ÷ 2 = 1 dengan sisa 0

1 ÷ 2 = 0 dengan sisa 1

2.1.1.3 Algoritma Pembagian

Definisi 2.3

Jika $a, b \in \mathbb{Z}$ dan $a > 0$, maka ada bilangan $q, r \in \mathbb{Z}$ yang masing-masing tunggal sehingga $b = qa + r$ dengan $0 \leq r < a$. Jika $a \nmid b$, maka r memenuhi ketidaksamaan $0 < r < a$ (Muhsetyo, 1997:50).

Teorema 2.2

Misalkan a dan b adalah bilangan bulat dengan $a > 0$. Maka terdapat bilangan bulat q dan r yang masing-masing tunggal sehingga $b = qa + r$, $0 \leq r < a$ (Abdussakir, 2009:117).

Bukti:

Diketahui a dan b adalah bilangan bulat $a > 0$. Dan $b - qa$ dengan $q \in \mathbb{Z}$ maka dapat dituliskan

$$S = \{b - qa | q \in \mathbb{Z}\}$$

Selanjutnya diambil himpunan P yang anggota himpunan S yang tidak negatif, yaitu:

$$P = \{b - qa | b - qa \geq 0, q \in \mathbb{Z}\}$$

Maka $P \neq \phi$, sebab:

1. Jika $b \geq 0$ dan $q = 0$, maka $b - qa = b - 0a = b \in P$
2. Jika $b < 0$ dan $q = b$, maka $b - qa = b - ba = b(1 - a)$

Karena $a > 0$ atau $a \geq 0$, maka $1 - a \leq 0$. Dan karena $b < 0$, maka $b(1 - a) \geq 0$, Jadi $b - ba \in P$.

Karena $P \neq \phi$ dan $P \subseteq \mathbb{N}$, sesuai prinsip urutan pada $\mathbb{N}$, maka P mempunyai unsur terkecil.

Misalkan r adalah unsur terkecil dari P, Karena $r \in P$, maka $r \geq 0$ dan $r = b -$

qa atau $b = qa + r$, untuk suatu $q \in \mathbb{Z}$. Selanjutnya akan dibuktikan bahwa $r \geq a$. Maka $0 \leq r - a$ dan $r - a = (b - qa) - a = b - (q + 1)a$, Jadi $r - a \in P$.

Karena $a > 0$, maka $r - a < r$. Jadi, ada elemen $(r - a)$ di P yang kurang dari r. Hal ini bertentangan dengan pernyataan bahwa r adalah unsur terkecil di P. Dengan demikian maka harus $r < a$. Dari $r \geq 0$ dan $r < a$, maka $0 \leq r < a$ sehingga $b = qa + r$, untuk $0 \leq r < a$.

Berikutnya akan ditunjukkan bahwa q dan r masing-masing tunggal. Andaikan ada q_1 dan q_2 dengan $q_1 \neq q_2$ dan $r_1$dan r_2 dengan $r_1 \neq r_2$ sehingga $b = q_1 a + r_1, 0 \leq r_1 < a$ dan $b = q_2 a + r_2, 0 \leq r_2 < a$. Maka $q_1 a + r_1 = q_2 a + r_2$ atau $r_2 - r_1 = a(q_1 - q_2)$.

Berarti $a|(r_2 - r_1)$ atau $(r_2 - r_1)$ adalah kelipatan dari a. Di sisi lain karena $0 \leq r_1 < a$ dan $0 \leq r_2 < a$.

Ambil $0 \leq r_1 < a \times (-1) = -a \leq -r_1 < 0$ dan $0 \leq r_2 < a$.

$$\begin{array}{l} 0 \leq r_2 < a \\ \underline{-a < -r_1 < 0} \; + \\ -a < (r_2 - r_1) < a \end{array}$$

Sehingga $-a < (r_2 - r_1) < a$.

Satu-satunya kelipatan a yang terdapat di antara $-a$ dan a adalah 0. Sehingga diperoleh $r_2 - r_1 = 0$ atau $r_2 = r_1$

Karena $r_2 - r_1 = a(q_1 - q_2)$ maka $a(q_1 - q_2) = 0$

Karena $a > 0$ maka $q_1 - q_2 = 0$ atau $q_1 = q_2$

Jadi q dan r masing-masing adalah tunggal. Jadi, $b = qa + r$, $0 \leq r < a$.

Dalam teorema di atas, yaitu $b = qa + r, 0 \leq r < a.b$ disebut bilangan yang dibagi *(dividend)*, $a$disebut pembagi *(divisor)*, q disebut hasil bagi *(quotient)*, dan r disebut sisa pembagi *(remainder)* jika$a|b$ maka diperoleh bahwa sisa pembaginya adalah 0. Sehingga dapat disimpulkan untuk $a > 0$ bahwa:

a) $a|b$ jika dan hanya jika $b = qa + r$ dan $r = 0$.

b) $a\nmid b$ jika dan hanya jika $b = qa + r$ dengan $0 \leq r < a$

c) Teorema 2.3

Jika $b \in \mathbb{Z}$ dan $b > 1$, maka setiap $n \in \mathbb{Z}^+$ dapat ditulis secara tunggal dalam bentuk $n = a_k b^k + a_{k-1} b^{k-1} + \cdots a_2 b^2 + a_1 b^1 + a_0 b^0$

Yang mana $k \in \mathbb{Z}$ dan $k \geq 0, a_i \in \mathbb{Z}$dan $0 \leq a_i \leq b - 1$ untuk $i = 0,1,2, \ldots, k$, dan $a_k \neq 0$ (Muhsetyo, 1997:54).

Bukti:

Karena $b \in \mathbb{Z}$ dan $b > 1$, maka $b > 0$, sehingga menurut algoritma pembagian, hubungan antara n dan b adalah:

$n = bq_0 + a_0, 0 \leq a_0 \leq b - 1$

Jika $q_0 \neq 0$, maka hubungan antara q_0 dan b menurut algoritma pembagian:

$q_0 = bq_1 + a_1, 0 \leq a_1 \leq b - 1$

Jika langkah yang sama dikerjakan, maka diperoleh:

$q_1 = bq_2 + a_2, 0 \leq a_2 \leq b - 1$

$q_2 = bq_3 + a_3, 0 \leq a_3 \leq b - 1$

... ...

$$q_{k-2} = bq_{k-1} + a_{k-1}, 0 \leq a_{k-1} \leq b - 1$$

$q_{k-1} = bq_k + a_k, 0 \leq a_k \leq b - 1$

Langkah terakhir ditandai dengan munculnya $q_k = 0$. Karena barisan $q_0, q_1, \dots, q_k$adalah barisan bilangan bulat tidak negatif yang menurun, maka paling banyak ada q_0 suku yang positif, dan 1 suku q_k yang bernilai 0. Dari persamaan-persamaan di atas dapat ditentukan bahwa:

$n = bq_0 + a_0$

… …

Karena $q_k = 0$:

$n = b^k a_k + b^{k-1} a_{k-1} + \cdots + ba_1 + a_0$

$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0 b^0$

Contoh:

Perhatikan langkah berturut-turut dalam pembagian algoritma untuk menuliskan 567 dalam basis 2 dan 567 dalam basis 3.

Jawab:

Untuk basis 2:

$567 = 2 \cdot 283 + 1$ $\qquad$ $17 = 2 \cdot 8 + 1$

$283 = 2 \cdot 141 + 1$ $\qquad$ $8 = 2 \cdot 4 + 0$

$141 = 2 \cdot 70 + 1$ $\qquad$ $4 = 2 \cdot 2 + 0$

$70 = 2 \cdot 35 + 1$ $\qquad$ $2 = 2 \cdot 1 + 0$

$35 = 2 \cdot 17 + 1$ $1 = 2 \cdot 0 + 1$ $(567)_{10}=(1000110111)_2$

Untuk basis 3:

$567 = 3 \cdot 189 + 0$

$189 = 3 \cdot 63 + 0$

$63 = 3 \cdot 21 + 0$

$21 = 3 \cdot 7 + 0$

$7 = 3 \cdot 2 + 1$

$2 = 3 \cdot 0 + 2$ $(567)_{10} = (210000)_3$

2.1.2 Fungsi Euler (ϕ)

Fungsi Euler digunakan untuk menyatakan banyaknya bilangan bulat $< n$ yang relatif prima terhadap n.

Definisi 2.4

Suatu himpunan bilangan bulat $\{r_1, r_2, \dots, r_k\}$ disebut dengan sistem residu tereduksi modulo m jika:

a) $(r_i, m) = 1 (i = 1, 2, \dots, k)$.

b) $r_i \not\equiv r_j$ (mod m) untuk semua $i \neq j$.

c) Jika $(x, m) = 1$, maka $x \equiv r_i$ mod (m) (Muhsetyo, 1997:279).

Contoh:

Himpunan {1,5} adalah sistem tereduksi modulo 6 karena:

a. $r_1 = 1, r_2 = 5, (r_1, 6) = (1,6) = 1$ dan $(r_2, 6) = (5,6) = 1$

b. $1 \not\equiv 5$ (mod 6)

c. $(7,6) = 1 \rightarrow 7 \equiv 1 (\text{mod } 6)$

d. $(11,6) = 1 \rightarrow 11 \equiv 5 (\text{mod } 6)$, dan seterusnya

Teorema 2.4

Jika *p* adalah suatu bilangan prima, maka $\phi(p) = p - 1$ (Muhsetyo, 1997:280).

Bukti:

Karena *p* adalah bilangan prima, maka setiap bilangan bulat positif kurang dari *p* relatife prima terhadap *p*. Ini berarti bahwa sistem residu tereduksi modulo *p*adalah himpunan {1, 2, 3,…,*p* - 1} yang mana seluruh anggotanya sebanyak (*p* - 1) sehingga $\phi(p) = p - 1$.

Teorema 2.5

Jika $m,n \in \mathbb{Z}^+$ dan $(m,n) = 1$, maka $\phi(mn) = \phi(m).\ \phi(n)$(Muhsetyo, 1997:282).

Bukti:

Bilangan-bilangan positif kurang dari atau sama dengan *mn* disusun menurut suatu cara sebagai berikut:

1	*m*+1	2*m*+1	…	(*n*-1)*m*+1
2	*m*+2	2*m*+2	…	(*n*-1)*m*+2
3	*m*+3	2m+3	…	(*n*-1)*m*+3
.	.	.		.
.	.	.		.
.	.	.		.
m	2*m*	3*m*	…	*mn*

Ambil suatu bilangan positif *r* yang tidak lebih dari *m*, maka:

a. Untuk $(m,r) = d > 1$, tidak ada bilangan pada baris ke *r* yang relatif prima dengan *mn*. Hal ini disebabkan oleh bentuk $(km + r)$ dari sebarang bilangan pada baris ke *r*, dimana *k* adalah bilangan bulat yang memenuhi:

   $1 \leq k \leq (n-1)$

   dengan $d \mid (km + r)$ karena $d \mid m$ dan $d \mid r$

b. Untuk $(m,r) = 1$ dengan $1 \leq k \leq m$, maka banyaknya bilangan pada baris ke *r* yang relatif prima terhadap *mn* dapat dicari sebagai berikut:

   Bilangan-bilangan pada baris ke *r* adalah $r, m+r, 2m+r, \ldots, (n-1)m+r$ karena $(m,r)=1$, maka masing-masing bilangan pada baris ke *r* adalah relatif prima terhadap *m*, sehingga *n* bilangan pada baris ke *r* ini membentuk system residu yang komplit modulo *n*, sehingga terdapat $\phi(n)$ bilangan yang relatif prima dengan. Karena bilangan-bilangan $\phi(n)$ ini relatif prima terhadap *m*, maka $\phi(n)$ ini juga relatif dengan *mn*.Selanjutnya, karena terdapat $\phi(m)$ baris yang masing-masing memuat $\phi(n)$ bilangan yang relatif prima terhadap *mn*, maka dapat disimpulkan bahwa$\phi(mn) = \phi(m).\ \phi(n)$

Definisi 2.5

Jika m adalah suatu bilangan bulat positif, maka banyaknya residu di dalam sistem residu tereduksi modulo m adalah $\phi(m)$. $\phi(m)$ disebut fungsi ϕ-Euler dari m. Dari definisi dapat diketahui bahwa $\phi(m)$ adalah sama dengan banyaknya bilangan bulat positif kurang dari m yang relatif prima dengan m (Muhsetyo, 1997:279).

Contoh:

1. Himpunan $\{1\}$ adalah sistem residu tereduksi modulo 2 sehingga $\phi(2) = 1$

2. Himpunan $\{1, 2\}$ adalah sistem residu tereduksi modulo 3 sehingga $\phi(3) = 2$
3. Himpunan $\{1, 3, 5, 7, 9, 11, 13, 15\}$ adalah sistem residu tereduksi modulo 16 sehingga $\phi(16) = 8$

4. Metode *Fast Exponentiation*

Metode *fast exponentiation* ini digunakan untuk menghitung operasi pemangkatan besar bilangan bulat modulo dengan cepat. Metode ini memanfaatkan ekspansi biner dari bilangan Z(Hamidah, 2009) yaitu:

$$Z = \sum_{i=0}^{k} a_i \cdot 2^i$$

Karena $z$ditulis dengan ekspansi biner maka $a \in \{0,1\}$, sehingga:

$$g^z = g^{\sum_{i=0}^{k} a_i \cdot 2^i} = \prod_{i=0}^{k} (g^{2^i})^{a_i} = \prod_{0 \le i \le k, a_i = 1} g2^i$$

$$g^z = g^{\left((a_0 \cdot 2^0) + (a_1 \cdot 2^1) + (a_2 \cdot 2^2) + \cdots + (a_k \cdot 2^k)\right)}$$

Metode *fast exponetiation* didasarkan pada pernyataan berikut ini:

$$g2^{i+1} = (g^{2^i})^a$$

Contoh:

Akan dihitung $6^{73} \pmod{100}$

Jawab:

Pertama tentukan expansi biner dari 73

$73 = 1 \cdot 2^6 + 1 \cdot 2^3 + 1 \cdot 2^0$ atau $73 = (1001001)_2$

Kemudian dihitung

$6^{2^0} = 6$

$6^{2^1} = 36$

$6^{2^2} = 36^2 = 96 \pmod{100}$

$6^{2^3} = 16 \pmod{100}$

$6^{2^4} = 16^2 = 56 \pmod{100}$

$6^{2^5} = 56^2 = 36 \pmod{100}$

$6^{2^6} = 56^2 = 96 \pmod{100}$

Sehingga diperoleh:

$6^{73} = 6 \cdot 6^{2^3} \cdot 6^{2^6} \pmod{100}$

$= 6 \cdot 16 \cdot 96 \pmod{100}$

$= 16 \pmod{100}$

Jadi, $6^{73} \pmod{100} = 16$

2.1.4 Aritmetika Modulo dan Kekongruenan

Definisi 2.6

Diketahui $a, b, m \in \mathbb{Z}$. a disebut kongruen dengan b modulo m, ditulis $a \equiv b \pmod{m}$, jika $(a - b)$ habis dibagi m, yaitu $m|(a - b)$. Jika $(a - b)$tidak habis dibagi m, yaitu $m\nmid(a - b)$, maka ditulis $a \not\equiv b \pmod{m}$, dibaca a tidak kongruen dengan b modulo m. Karena $(a - b)$ habis dibagi oleh m jika dan hanya jika $(a - b)$ habis dibagi oleh $-m$, maka: $a \equiv b \pmod{m}$ jika dan hanya jika $b \equiv a \pmod{m}$ (Muhsetyo, 1997:138).

Contoh:

1. $17 \equiv 2 \pmod{3}$ (3 habis dibagi $17 - 2 = 15 \rightarrow 15 \div 3 = 5$)
2. $-7 \not\equiv 15 \pmod{3}$ (3 tidak habis dibagi $-7 - 15 = -22$)

Definisi 2.7

Misalkan a dan b adalah bilangan bulat dan m adalah bilangan bulat> 0, maka $a \equiv b \pmod{m}$ jika m habis membagi $a - b$(Munir, 2012:192).

Contoh:

Bilangan 38 kongruen dengan 13 modulo 5 karena 5 membagi 38 – 13 = 25, sehingga dapat kita tulis bahwa $38 \equiv 13 (\text{mod } 5)$. Tetapi, 41 tidak kongruen dengan 30 modulo 5 karena 5 tidak habis membagi 41 – 30 = 11 sehingga dapat kita tulis $41 \not\equiv 30 (\text{mod } 5)$. Dengan cara yang sama, kita dapat menunjukkan bahwa:

$17 \equiv 2 (\text{mod } 3)$ (3 habis membagi 17 – 2 = 15 → 15÷3 = 5)

$-7 \equiv 15 (\text{mod } 11)$ (11 habis membagi -7 – 15 = -22 → -22÷11 = 2)

$12 \not\equiv 2 (\text{mod } 7)$ (7 tidak habis membagi 12 – 2 = 10)

$-7 \not\equiv 15 (\text{mod } 3)$ (3 tidak habis membagi -7 – 15 = -22)

Kekongruenan $a \equiv b (\text{mod } m)$ dapat pula dituliskan dalam hubungan $a = b + km$, yang dalam hal ini adalah sembarang k adalah bilangan bulat. Pembuktiannya adalah sebagai berikut:

Menurut definisi 2.7, $a \equiv b (\text{mod } m)$ jika $m|(a - b)$, maka terdapat bilangan bulat k sedemikian sehingga $a - b = km$ atau $a = b + km$.

2.1.5 Bilangan Prima

Bilangan bulat positif yang mempunyai aplikasi penting dalam ilmu komputer dan matematika diskrit adalah bilangan prima. Bilangan prima adalah bilangan bulat positif yang lebih dari 1 yang hanya habis dibagi oleh 1 dan dirinya

sendiri (Munir, 2012:200).

Sifat pembagian pada bilangan bulat melahirkan konsep-konsep bilangan prima dan aritmetika modulo, dan salah satu konsep bilangan bulat yang digunakan dalam penghitungan komputer adalah bilangan prima. Dengan ditemukannya bilangan prima, teori bilangan berkembang semakin jauh dan lebihmendalam. Banyak dalil dan sifat dikembangkan berdasarkan bilangan prima. Bilangan prima juga memainkan peranan yang penting pada beberapa algoritma kunci publik, seperti algoritma RSA dan algoritma Elgamal.

Definisi 2.8

Jika p suatu bilangan bulat positif lebih dari 1 yang hanya mempunyai pembagi positif 1 dan p, maka p disebut bilangan prima. Jika suatu bilangan bulat $q > 1$ bukan suatu bilangan prima, maka q disebut bilangan komposit.

Untuk menguji apakah p merupakan bilangan prima atau bilangan komposit, dapat menggunakan cara yang paling sederhana, yaitu cukup membagi p dengan sejumlah bilangan prima, yaitu $2, 3, \dots,$ bilangan prima $\leq \sqrt{p}$. Jika p habis dibagi salah satu dari bilangan prima tersebut, maka p adalah bilangan komposit tetapi jika p tidak habis di bagi oleh semua bilangan prima tersebut, maka p adalah bilangan prima.

Teorema 2.6

Jika p adalah suatu bilangan prima dan $p|a_1a_2, \dots, a_n$, maka paling sedikit membagi satu faktor $a_k(1 \leq k \leq n)$ (Muhsetyo, 1997:100).

Bukti:

$p|a_1a_2, \dots, a_n$ atau $p|a_1(a_2, a_3 \dots, a_n)| \rightarrow p|a_1$ atau $p|a_2, a_3 \dots, a_n$, jika $p \nmid a_1$ maka terbukti p paling sedikit membagi satu faktor a_k, jika $p \nmid a_1$ maka

$p|a_2, a_3 \dots, a_n$ atau $p|a_2(a_3, a_4 \dots, a_n)$, $p|a_2(a_3, a_4 \dots, a_n) \rightarrow p|a_2$ atau $p|a_3 a_4, \dots, a_n$. Demikian seterusnya diperoleh $p|a_{n-1}, a_n$, $p|a_{n-1}, a_n \rightarrow p|a_{n-1}$ atau $p|a_n$. Ini berarti bahwa p paling sedikit membagi faktor a_k.

Teorema 2.7 (Teorema Kecil Fermat)

Jika p adalah suatu bilangan prima dan$p\nmid a$, maka $a^{p-1} \equiv 1(\text{mod } p)$

(Muhsetyo, 1997:152)

Bukti:

Karena p adalah suatu bilangan prima dengan $p\nmid a$, maka $(p, a) = 1$ (jika $(p, a)|1$) yaitu p dan$a$ tidak relatif prima, maka p dan a mempunyai faktor selain 1 dan p, bertentangan dengan sifat p sebagai bilangan prima), selanjutnya karena $(p, a) = 1$ maka untuk $a^{\phi(p)} \equiv 1(\text{mod } p)$.

P adalah bilangan prima, berarti dari bilangan-bilangan bulat:

$$\{0, 1, 2, 3, \dots, p-1\}$$

yang tidak relatif prima dengan p hanyalah 0, sehingga:

$$\{1, 2, 3, \dots, p-1\}$$

Merupakan sistem residu tereduksi modulo p, dengan demikian

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

Karena $\phi(p) = p - 1$ dan $a^{\phi(p)} \equiv 1$, maka $a^{p-1} \equiv 1(\text{mod } p)$

Contoh:

Carilah nilai-nilai x yang memenuhi $2^{250} \equiv x(\text{mod } 7)$ dan $0 \leq x < 7$

Jawab:

Karena 7 adalah bilangan prima, maka $\phi(7) = 7 - 1 = 6$

Karena $7\nmid 2$ dan 7 adalah bilangan prima, maka:

$2^{\phi(7)} \equiv 1 (\text{mod } 7)$

$2^6 \equiv 1 (\text{mod } 7)$

$2^{250} \equiv (2^6)^{41} \cdot 2^4 \equiv 1 \cdot 2^4 (\text{mod } 7) \equiv 1 \cdot 16 \ (\text{mod } 7) \equiv 16 \ (\text{mod } 7) \equiv 2 \ (\text{mod } 7)$ jadi $x = 2$.

2.1.5.1 Relatif Prima

Dua buah bilangan bulat dan dikatakan relatif prima jika FPB/GCD $(x, y) = 1$ (Respatiadi, 2013).

Contoh:

20 dan 3 relatif prima sebab FPB $(20, 3) = 1$. Begitu juga 7 dan 11 relatif prima karena FPB $(7, 11) = 1$. Tetapi 20 dan 5 tidak relatif prima sebab FPB $(20, 5) = 5$ dan 1.

Jika x dan y relatif prima, maka terdapat bilangan bulat m dan n sedemikian sehingga: $mx + ny = 1$.

Contoh:

Bilangan 20 dan 3 adalah relatif prima karena FPB $(20, 3) = 1$, atau dapat ditulis: $2 \cdot 20 + (-13) \cdot 3 = 1$, dengan $m = 2$ dan $n = -13$. Tetapi 20 dan 5 tidak relatif prima karena FPB $(20, 5) = 5 \neq 1$ sehingga 20 dan 5 tidak dapat dinyatakan dalam m. $20 + n \cdot 5 = 1$.

2.1.6 Logaritma Diskrit

Keamanan kriptografi Elgamal terletak pada sulitnya menghitung logaritma diskrit. Jadi, algoritma diskrit mempunyai peranan yang sangat penting untuk menjaga keamanan suatu informasi yang menggunakan kriptografi

Elgamal. Misalkan p adalah bilangan prima, g dan y adalah sembarang bilangan bulat. Carilah x sedemikian hingga $g^x \equiv y \ (mod\ p)$, maka x inilah yang disebut dengan masalah algoritma diskrit. Salah satu metode yang dapat digunakan untuk mencari nilai logaritma diskrit adalah metode enumerasi, yaitu dengan mengecek seluruh kemungkinan, mulai dari 0, 1, 2, dan seterusnya sampai akhirnya ditemukan nilai x yang tepat. Metode enumerasi membutuhkan sebanyak $x - 1$ proses pergandaan modulo dan sebanyak x perbandingan. Apabila menggunakan nilai x yang lebih besar, maka metode ini membutuhkan proses perhitungan dan waktu yang lebih banyak lagi. Namun pada penggunaan yang sebenarnya, digunakan nilai logaritma diskrit yang besar seperti $g^x = 2^{225}$. Oleh karena itu, dengan menggunakan metode enumerasi dirasakan menjadi sia-sia karena dibutuhkan paling sedikit sebanyak $2^{225} - 1$ proses perhitungan, sehingga dibutuhkan waktu yang sangat lama untuk mencari nilai logaritma diskret tersebut. Namun, dalam skripsi ini tidak dibahas lebih lanjut mengenai logaritma diskrit karena batasan masalahnya hanya pada konsep-konsep matematika yang mendasari pembentukan kriptografi Elgamal. Konsep-konsep matematika seperti bilangan prima dan logaritma diskrit adalah konsep-konsep yang mendasari kriptografi Elgamal. Dan selain konsep tersebut, untuk memahami dan membuat kriptografi Elgamal, seseorang perlu mengetahui proses-proses perhitungan dengan matematika terutama yang berhubungan dengan faktor persekutuan terbesar, pemangkatan, aritmatika modulo, kekongruenan dan lainnya (Hamidah, 2009).

2.2 Kriptografi

Kriptografi berasal dari bahasaYunani, menurut bahasa dibagi menjadi dua

kripto dan *graphia*, kripto berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut teminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Keamanan pesan diperoleh dengan menyandikannya menjadi pesan yang tidak mempunyai makna (Munir, 2012:203). Menurut catatan sejarah, kriptografi sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja-raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir-kurinya. Berkaitan dengan pesan rahasia, Allah berfirman:

وَإِذْ أَسَرَّ ٱلنَّبِيُّ إِلَىٰ بَعْضِ أَزْوَٰجِهِۦ حَدِيثًا فَلَمَّا نَبَّأَتْ بِهِۦ وَأَظْهَرَهُ ٱللَّهُ عَلَيْهِ عَرَّفَ بَعْضَهُۥ
وَأَعْرَضَ عَنۢ بَعْضٍ ۖ فَلَمَّا نَبَّأَهَا بِهِۦ قَالَتْ مَنْ أَنۢبَأَكَ هَٰذَا ۖ قَالَ نَبَّأَنِىَ ٱلْعَلِيمُ ٱلْخَبِيرُ ﴿٣﴾

"*(Dan) ingatlah (ketika Nabi membicarakan secara rahasia kepada salah seorang dari istri-istrinya) yakni kepada Siti Hafshah (suatu pembicaraan) tentang mengharamkan Siti Mariyah atas dirinya, kemudian Nabi saw. Berkata kepada Siti Hafshah, "Jangan sekali-kali kamu membuka rahasia ini." (Maka tatkala menceritakan peristiwa itu) kepada Siti Aisyah, ia menduga bahwa hal ini tidak dosa (dan Allah memberitahukan hal itu) Dia membukanya (kepadanya) yakni kepada Nabi Muhammad tentang pembicaraan Siti Hafshah kepada Siti Aisyah itu (lalu dia memberitahukan sebagiannya) kepada Siti Hafshah (dan menyembunyikan sebagian yang lain) sebagai kemurahan dari dirinya terhadap dia. (Maka tatkala dia, Muhammad, memberitahukan pembicaraan itu, lalu Hafshah bertanya, "Siapakah yang telah memberitahukan hal ini kepadamu?" Nabi menjawab, "Telah diberitahukan kepadaku oleh Yang Maha Mengetahui lagi Maha Waspada") yakni Allah SWT (QS. al- Tahrim/66:3)*"

Selama bertahun-tahun kriptografi hanya digunakan oleh pihak militer. Agen keamanan nasional semua Negara bekerja keras untuk mempelajari kriptografi. Maka dari itu kriptografi terus berkembang karena semakin banyaknya informasi yang harus diamankan kerahasiaannya. Selama tiga puluh tahun terakhir ini bukan hanya agen militer yang berniat menggunakan kriptografi namun pribadi-pribadi yang lain yang tidak ingin diketahui kehidupan pribadinya juga menggunakan kriptografi.

2.2.1 Kriptografi RSA

Algortima RSA dijabarkan pada tahun1977 oleh Ron Rivest, Adi Shamir, dan Len Adlemandari MIT. Huruf RSA itu sendiri juga berasal dariinisial nama mereka (Rivest-Shamir-Adleman).Clifford Cocks, seorang matematikawan Inggris yang bekerja untuk GCHQ, menjabarkan tentang sistem ekivalen pada dokumen internal di tahun 1973.Penemuan Clifford Cocks tidak terungkap hinggatahun 1997 dikarenakan alasan *top secret classification*. Algoritma tersebut dipatenkan oleh Massachusetts Institute of Technology pada tahun 1983 di AmerikaSerikat sebagai U. S. Patent 4405829. Paten tersebut berlaku hingga 21September 2000. Semenjak algoritma RSA dipublikasikan sebagai aplikasi paten, regulasi disebagian besar negara-negara lain tidak memungkinkan penggunaan paten. Hal inimenyebabkan hasil temuan Clifford Cocks di kenalsecara umum, Amerika Serikat tidak dapat mematenkannya (Arifin, 2009).

2.2.2 Kriptografi Elgamal

Kriptografi Elgamal ditemukan oleh ilmuwan Mesir, yaitu Taher Elgamal pada tahun 1985, merupakan algoritma kriptografi kunci publik. Algoritma Elgamal terdiri atas tiga proses, yaitu proses pembentukan kunci, enkripsi, dan dekripsi. Algoritma ini mempunyai kerugian pada cipherteksnya yang mempunyai panjang dua kali lipat dari plainteksnya. Akan tetapi, algoritma ini mempunyai kelebihan pada enkripsi. Untuk plainteks yang sama, algoritma ini memberikan cipherteks yang berbeda (dengan kepastian yang dekat) setiap kali plainteks dienkripsi.Algoritma ini merupakan *cipher*blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok *cipherteks* yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan (Arifin, 2009).

BAB III

METODE PENELITIAN

3.1 Jenis dan Pendekatan Penelitian

Ditinjau dari jenis datanya, jenis penelitian ini merupakan jenis penelitian kualitatif. Penelitian kualitatif adalah penelitian yang bermaksud untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian secara utuh dan dengan cara deskripsi dalam bentuk kata-kata dan bahasa pada suatu konteks khusus yang alamiah, serta dengan memanfaatkan berbagai metode alamiah yang salah satunya bermanfaat untuk keperluan meneliti dari segi prosesnya. Untuk pendekatan penelitian, peneliti menggunakan metode kepustakaan. *Library research* (penelitian kepustakaan), yaitu penelitian yang dilaksanakan dengan menggunakan literatur (kepustakaan), baik berupa buku, catatan, maupun laporan hasil penelitian dari penelitian terdahulu (Hasan, 2002:11).

3.2 Data dan Sumber Data

Data yang digunakan dalam penelitian ini adalah data kualitatif. Pada penelitian ini, data tersebut berupa definisi-definisi dan teorema seperti definisi bilangan bulat, definisi bilangan prima, definisi keterbagian, definisi kriptografi RSA, definisi keriptografi Elgamal, dan beserta teorema teoremanya.

Sementara itu, sumber data yang digunakan dalam penelitian ini adalah sumber data sekunder, yakni data yang berupa dokumen-dokumen yang telah tersedia. Peneliti membaca literatur-literatur yang dapat menunjang penelitian, yaitu literatur-literatur yang berhubungan dengan penelitian ini.

3.3 Pengumpulan Data

Teknik pengumpulan data merupakan langkah yang paling strategis dalam penelitian, karena tujuan utama dari penelitian adalah mendapatkan data (Sugiyono, 2010:224).

Dalam kegiatan pengumpulan data untuk penelitian ini digunakan metode pengumpulan studi pustaka atau metode dokumentasi. Dengan cara mencari data yang berupa buku-buku seperti buku *kriptografi keamanan data dan komunikasi*, buku*teori bilangan*, berupa jurnal kriptografi RSA dan Elgamal, maupun internet yang berhubungan dengan penelitian ini. Adapun kegiatan yang dilakukan oleh peneliti untuk pengumpulan data yaitu:

1. Persiapaan

   Sebelum peneliti memperoleh data, peneliti mempersiapkan suatu permasalahan yang akan di analisa kemudian mengidentifikasi permasalahan tersebut. Maka dari permasalahan tersebut pengumpulan data dapat diperoleh.

2. Mencari Literatur

   Dalam mencari literatur, peneliti mencari literatur yang berhubungan dengan penelitian ini. Seperti buku, jurnal, arsip-arsip, artikel maupun internet dan lain-lain.

3. Hasil Mencari Literatur

   Setelah peneliti mendapatkan literatur yang berhubungan dengan penelitian ini, maka diperoleh hasilnya. Seperti definisi-definisi dan teoreme-teorema yang berhubungan dengan penelitian ini.

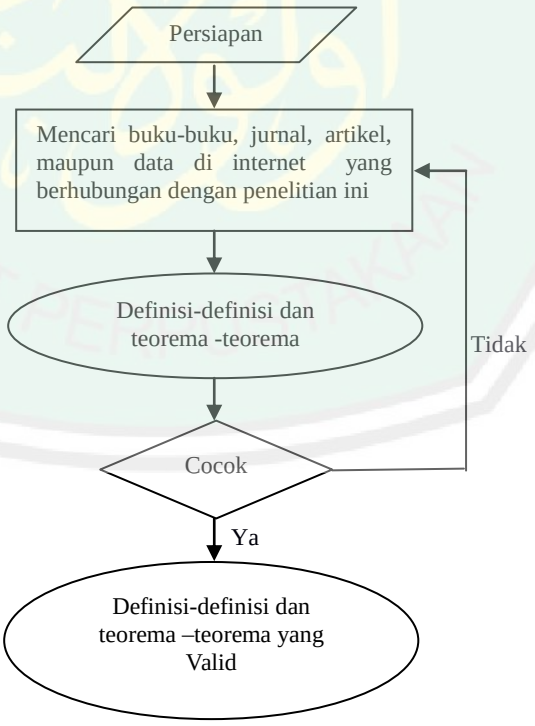
4. Menentukan Pilihan

Dalam menentukan pilihan ini, pilihan didasarkan atas hasil mencari literatur. Pilihan disini ada dua kemungkinan antara iya dan tidak. Jika pilihan tidak, maksudnya literatur yang didapatkan tidak cocok dengan penelitian ini. Maka peneliti harus mencari lagi data yang berhubungan dengan penelitian tersebut. Jika pilihan ya, maksudnya literatur sudah cocok dengan penelitian ini. Maka peneliti tidak harus mencari data lagi.

5. Hasil terakhir

Hasil akhir dari proses pengumpulan data adalah definisi yang valid, teorema yang valid, dan data pendukung lainnya yang valid dengan penelitian ini.

Flowchart Pengumpulan Data:



Gambar 3.1 *Flowchart* Pengumpulan Data

3.4 Analisa Data

Analisa data adalah kegiatan mengubah data hasil penelitian menjadi informasi yang dapat digunakan untuk mengambil kesimpulan dalam suatu penelitian.Dalam penelitian ini, analisa dilakukan dengan cara mengkaji perumusan algoritma kriptografi RSA dan algoritma kriptografi Elgamal terlebih dahulu, kemudian mengimplementasikan pada contoh dengan menggunakan bilangan prima pada pembentukan kuncinya, sehingga dapat menghasilkan rumus enkripsi dan dekripsi yang saling berkaitan. Peneliti menganalisa data dengan langkah-langkah sebagai berikut:

1. Mempersiapkan Data.

   Sebelum menganalisa data, peneliti mempersiapkan data yang telah diperoleh dari pengumpulan data. Data tersebut berupa kata-kata atau teks,seperti definisi-definisi, teorema-teorema, dan lain-lain.
2. Mengkaji Rumus algoritma kriptografi RSA dan algoritma kriptografi Elgamal dengan teorema matematika yang ada.
3. Implementasi contoh menggunakan bilangan prima.
4. Diberikan Pesan.

   Pada penelitian ini pesan disini berupa teks.
5. Pesan dirubah menjadi chiperteks.
6. Diberikan algoritma RSA.

   Langkah-langkah membangkitkan kunci dengan algoritma RSA:

   a. Pilih dua buah bilangan prima, p_1 dan p_2 yang bersifat rahasia.
   b. Setelah mendapat p_1 dan p_2, maka akan didapat nilai $n = p_1 . p_2$
   c. Selanjutnya hitung $\phi(n)$, untuk menyatakan banyaknya bilangan bulat < n yang relatif prima terhadap n.

$\phi(n)= (p_1-1)(p_2-1)$.

d. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya *e*, yang relatif prima terhadap $\phi(n)$.Bilangan yang relatif prima adalah bilangan yang memiliki *gcd* = 1.

e. Selanjutnya menghitung nilai *d*, dengan kekongruenan $ed \equiv 1 \pmod{\phi(n)}$. sehingga *d* dapat dihitung dengan cara yang sederhana dengan persamaan:

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

Dengan mencoba nilai-nilai *k*, sehingga diperoleh nilai *d* bilangan bulat.

Melalui langkah di atas maka akan didapat:

- kunci publik: (*e*,*n*).
- kunci privat: (*d*,*n*).

Langkah-langkah mengenkripsi pesan dengan algoritma RSA:

a. Plain teks terlebih dahulu dipecah menjadi blok-blok kecil.

b. Melakukan perhitungan menggunakan rumus sebagai berikut:

$c_i = m_i^e \bmod n$.

Langkah-langkah mendekripsi pesan dengan algoritma RSA:

a. Dengan menghitung rumus $m_i = c_i^d \bmod n$ dengan d adalah kunci privat.

7. Diberikan algoritma Elgamal

Langkah-langkah membangkitkan kunci dengan algoritma Elgamal:

a. Pilih sembarang bilangan prima *p*
b. Pilih dua buah bilangan acak, *g* dan *x* dengan syarat $g<p$ dan $1 \le x \le p-2$
c. Hitung $y = g^x \bmod p$.

Melalui langkah di atas maka akan didapat:

- kunci publik: triple (*y*, *g*, *p*).
- kunci privat: pasangan (*x*, *p*).

Langkah-langkah mengenkripsi pesan dengan algoritma Elgamal:

a. Pertama-tama plain teks dipecah-pecah menjadi blok yang lebih kecil dan disusun menjadi blok-blok $m_1, m_2, \ldots, m_n$.

b. Pilih bilangan acak k yang terletak pada nilai $1 \leq k \leq p-2$

c. Setiap blok m dienkripsi dengan rumus:

$a = g^k \bmod p$

$b = y^k m \bmod p$

Pasangan a dan b adalah cipher teks untuk blok pesan m. Jadi ukuran cipher teks dua kali ukuran plain teksnya.

Langkah-langkah mendekripsi pesan dengan algoritma Elgamal:

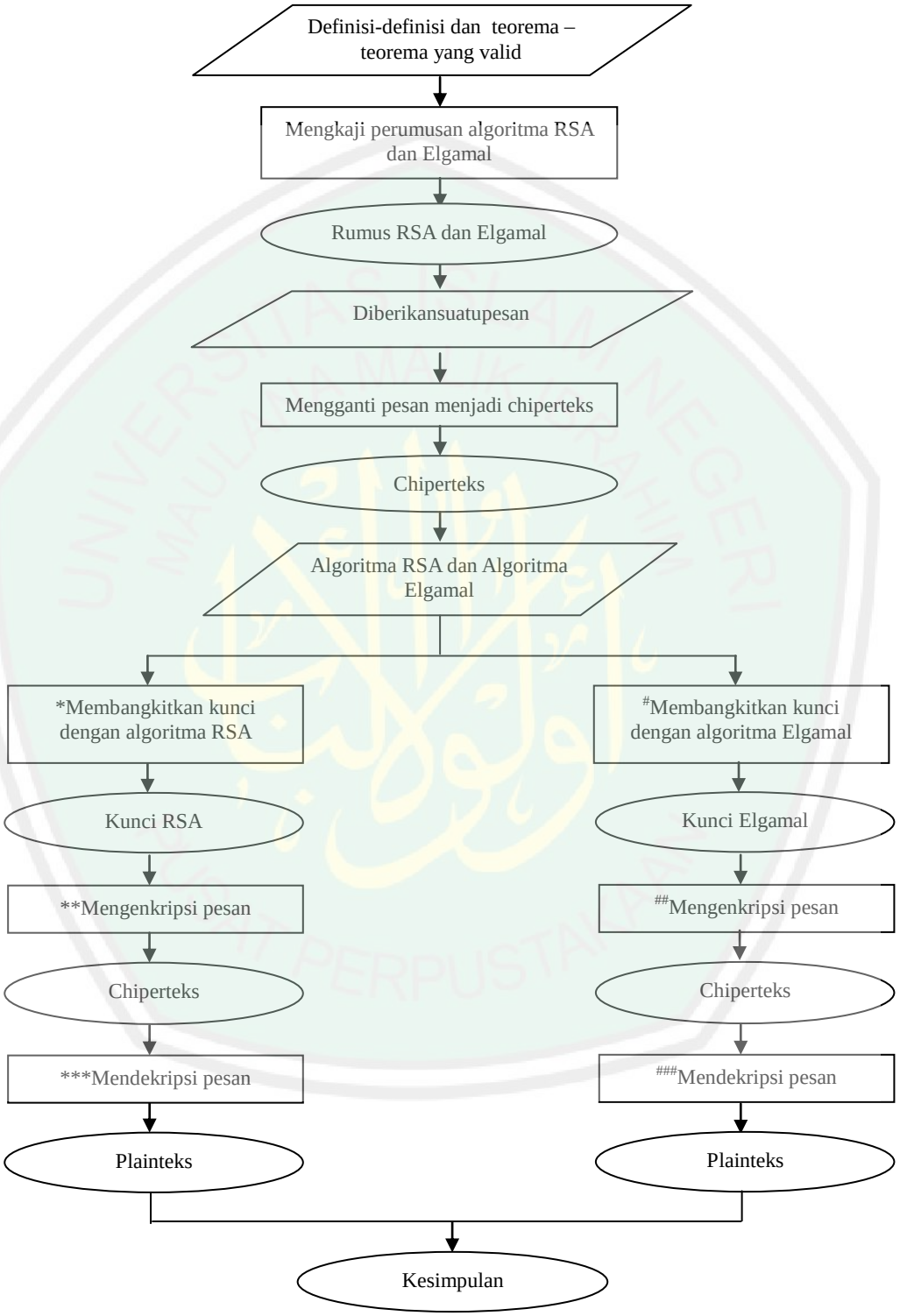
a. Gunakan kunci privat x untuk menghitung $a^{-x} = a^{p-1-x} \bmod p$

b. Hitung plain teks m dengan persamaan: $m = b/a^x \bmod p$

8. Kesimpulan

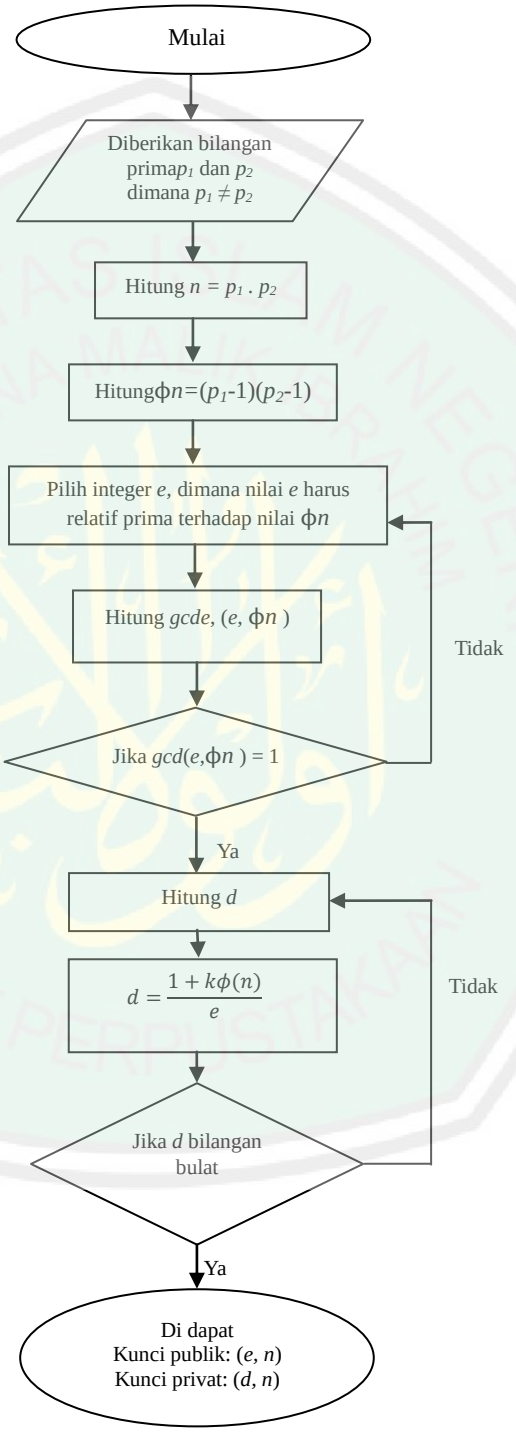
Kesimpulan dari penelitian ini adalah mengetahui penggunaan bilangan prima pada algoritma kriptografi RSA dan algoritma kriptografi Elgamal

Flowchart analisa data, terlihat seperti pada gambar di bawah ini:



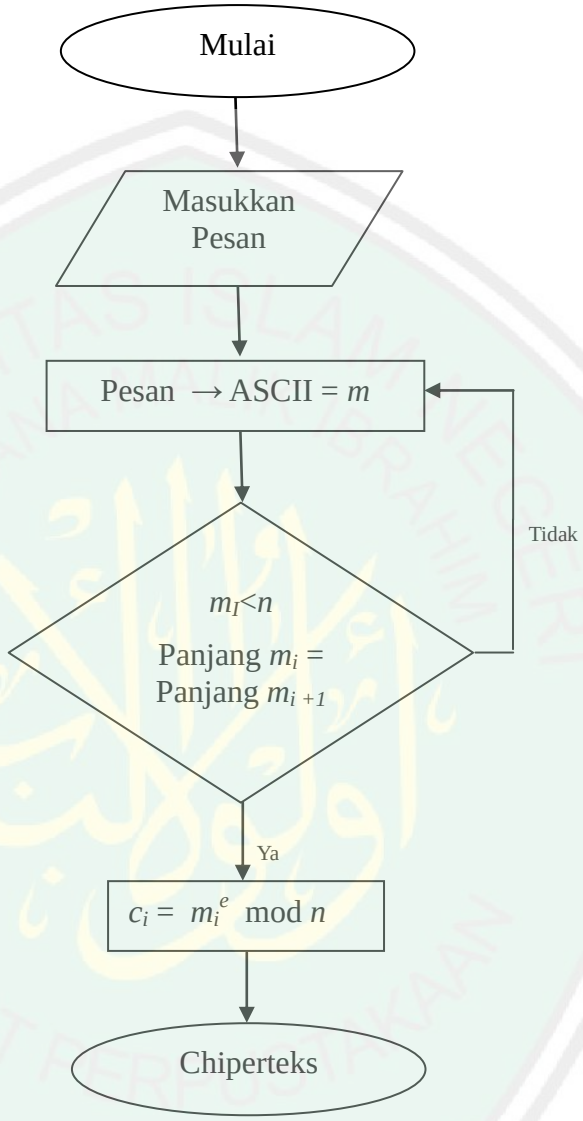
Gambar 3.2 *Flowchart* Analisa Data

**Flowchart* pembangkitan kunci pada algoritma RSA, terlihat seperti pada gambar di bawah ini:



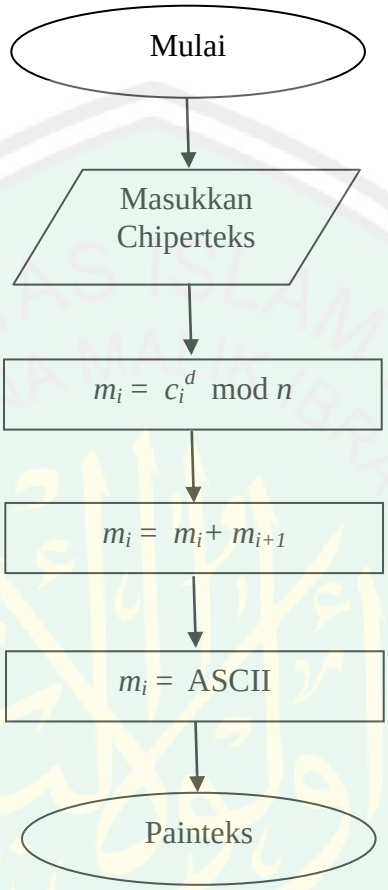
Gambar 3.3*Flowchart* Pembangkitan Kunci Pada Algoritma RSA

****Flowchart** proses enkripsi pada algoritma RSA, terlihat seperti pada gambar di bawah ini:



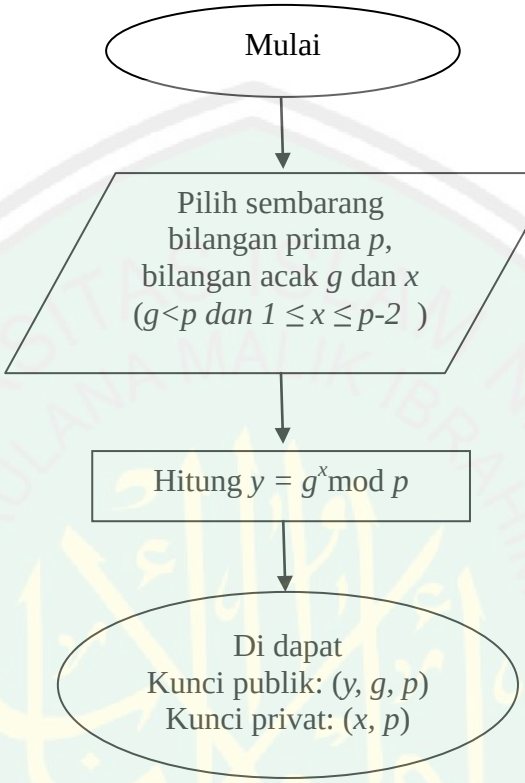
Gambar 3.4 *Flowchart* Enkripsi Pada Algoritma RSA

***Flowchartproses dekripsi pada algoritma RSA, terlihat seperti pada gambar di bawah ini:



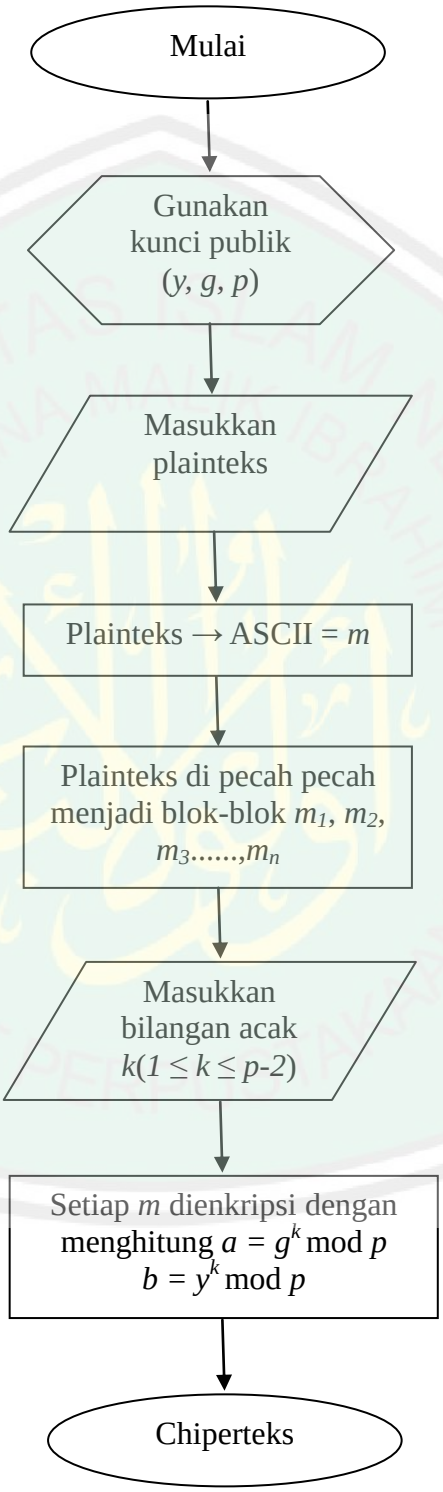
Gambar 3.5 *Flowchart* Dekripsi Pada Algoritma RSA

#*Flowchart* proses pembangkitankunci pada algoritma Elgamal, terlihat seperti pada gambar di bawah ini:



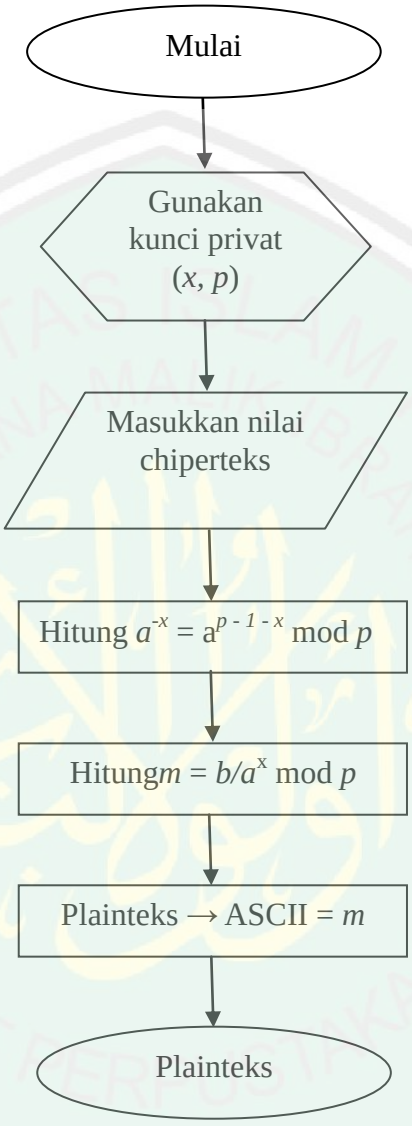
Gambar 3.6 *Flowchart* Pembangkitan Kunci Pada Algoritma Elgamal

[##]*Flowchart* proses enkripsi pada algoritma Elgamal, terlihat seperti pada gambar di bawah ini:



Gambar 3.7 *Flowchart* Enkripsi Pada Algoritma Elgamal

###*Flowchart* proses dekripsi pada algoritma Elgamal, terlihat seperti pada gambar di bawah ini:



Gambar 3.8 *Flowchart* Dekripsi Pada Algoritma Elgamal

1.5 Prosedur Penelitian

Prosedur penelitian adalah langkah-langkah atau urutan-urutan yang harus dilalui atau dikerjakan dalam suatu penelitian, sehingga mampu menjawab rumusan masalah dan tujuan penelitian.Tahapan prosedur pada penelitian ini adalah:

1. MerumuskanMasalah.

Sebelum peneliti melakukan penelitian, peneliti mempersiapkan suatu permasalahan yang akan di bahas pada penelitian ini, karena jika tidak ada masalah maka penelitian ini tidak akan berjalan. Rumusan masalah pada penelitian ini adalahBagaimana penggunaan bilangan prima pada algoritma kriptografi RSA dan bagaimana penggunaan bilangan prima pada algoritma kriptografi Elgamal.

2. MengumpulkanData.

Sebelum peneliti memperoleh data, peneliti mempersiapkan suatu permasalahan yang akan di analisa kemudian mengidentifikasi permasalahan tersebut. Maka dari permasalahan tersebut pengumpulan data dapat diperoleh dan peneliti mencari literatur yang berhubungan dengan penelitian ini. Setelah peneliti mendapatkan literatur yang berhubungan dengan penelitian ini, maka diperoleh hasilnya seperti definisi-definisi dan teoreme-teorema yang valid.

3. Menganalisis Data.

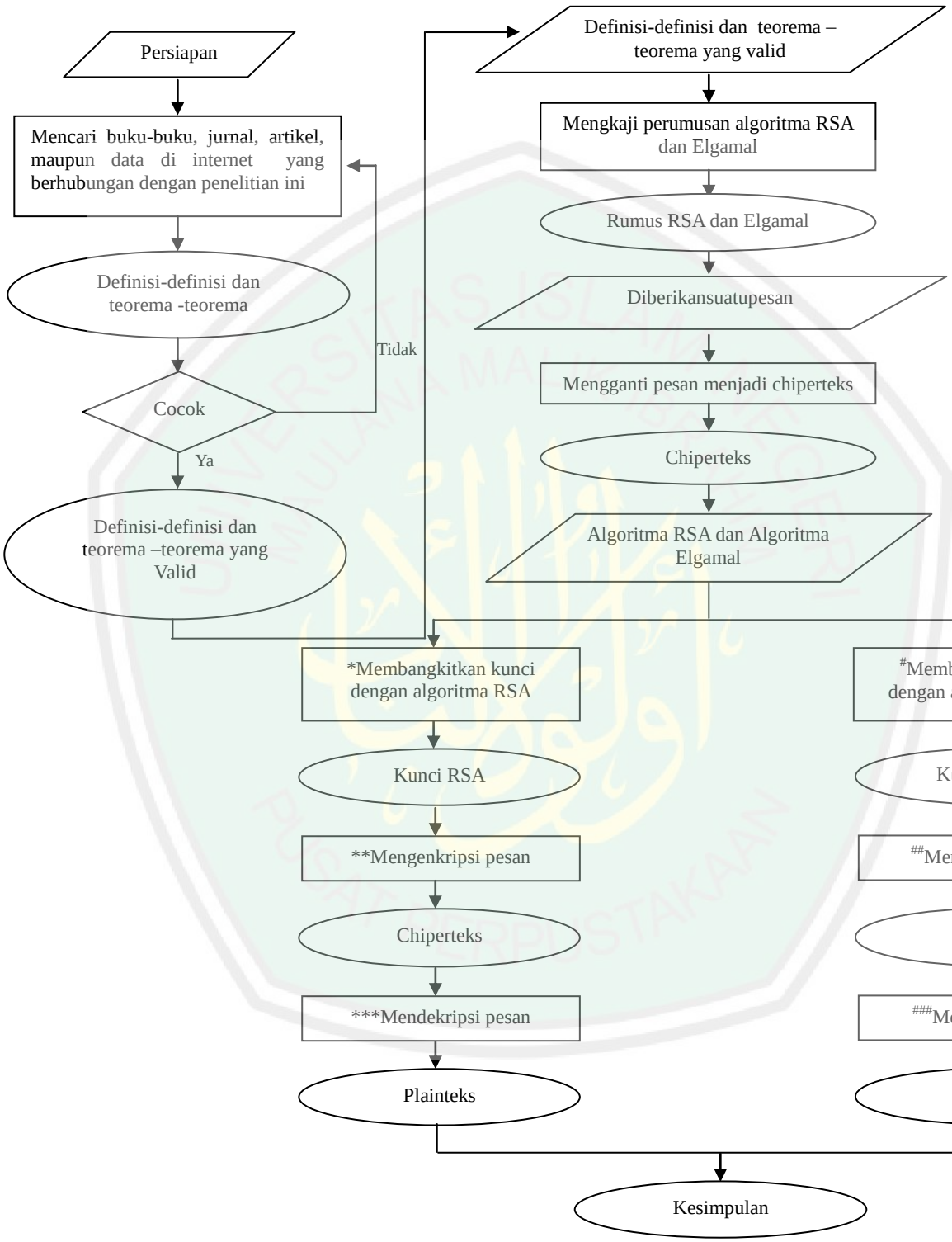
Sebelum menganalisa data, peneliti mempersiapkan data yang telah diperoleh dari pengumpulan data, data tersebut berupa kata-kata atau teks. Seperti definisi-definisi, teorema-teorema, dan lain-lain. Setelah data telah dipersiapkan,

maka tugas peneliti selanjutnya yaitu membaca, mempelajari, dan menganalisa dengan langkah-langkah yang telah dijelaskan sebelumnya. Dalam penelitian ini, Analisa dilakukan dengan cara mengkaji perumusan algoritma kriptografi RSA dan algoritma kriptografi Elgamal terlebih dahulu, kemudian mengimplementasikan pada contoh dengan menggunakan bilangan prima pada pembentukan kuncinya, sehingga dapat menghasilkan rumus enkripsi dan dekripsi yang saling berkaitan.

4. Membuat Kesimpulan.

Setelah peneliti melakukan analisa data, langkah yang terakhir adalah peneliti membuat kesimpulan.Kesimpulannya adalah mengetahui tujuan dari penelitian ini yaitu mengetahuipenggunaan bilangan prima pada algoritma kriptografi RSA dan algoritma kriptografi Elgamal.

Flowchart prosedur penelitian, terlihat seperti pada gambar di bawah ini:



Gambar 3.9 *Flowchart* ProsedurPenelitian

BAB IV

PEMBAHASAN

Kriptografi dengan kunci asimetrik atau kriptografi kunci publik berbasis pada persoalan dari teori bilangan. Contohnya sistem kriptografi RSA bersandarkan pada persoalan faktorisasi bilangan komposit dan sistem kriptografi ElGamal berdasarkan persoalan logaritma diskrit yang merupakan persoalan pada teori bilangan. Pada bab 4 ini akan membahas konsep matematis pada perumusan algoritma kriptografi RSA dan algoritma kriptografi Elgamal juga mengimplementasikan menggunakanbilangan prima aman dan bilangan prima tidak aman pada algoritma kriptografi RSA dan algoritma kriptografi Elgamal.

4.1 Perumusan Algoritma Kriptografi RSA

Algortima RSA dijabarkan pada tahun1977 oleh Ron Rivest, Adi Shamir, dan Len Adlemandari MIT. Huruf RSA itu sendiri juga berasal dari inisial nama mereka (Rivest-Shamir-Adleman) (Arifin, 2009).

Besaran–besaran yang digunakan pada algoritma kriptografi RSA antara lain:

1. p_1 dan p_2 bilangan prima.
2. $n = p_1 . p_2$.
3. $\phi(n) = (p_1-1) . (p_2-1)$.
4. e (kunci enkripsi).
5. d (kunci dekripsi).
6. m (plainteks / pesan yang bisa dibaca).
7. c (cipherteks / pesan yang tidak bisa dibaca).

Perumusan Algoritma Kriptografi RSA:

1. Membangkitkan Kunci

   Langkah-langkah membangkitkan kunci dengan algoritma RSA:

   a. Pilih dua buah bilangan prima, p_1 dan p_2.

   b. Setelah mendapat p_1 dan p_2, maka akan didapat nilai $n = p_1 . p_2$

   c. Selanjutnya hitung fungsi euler dari n yang dilambangkan dengan $\phi(n)$, fungsi euler pada algoritma kriptografi RSA adalah sebagai dasar perumusan algoritma kriptografi RSA, sehingga dapat menghasilkan rumus enkripsi dan dekripsi yang saling berkaitan. Fungsi euler dari $n\phi(n)$, untuk menyatakan banyaknya bilangan bulat $<n$ yang relatif prima terhadap n.

      $\phi(n) = \phi(p_1) . \phi(p_2)$

      $= (p_1\text{-}1) .(p_2\text{-}1).$

      Berdasarkan teorema 2.4, Jika p adalah suatu bilangan prima, maka $\phi(p_1) = p - 1$

      Bukti:

      Karena p adalah bilangan prima, maka setiap bilangan bulat positif kurang dari p relatife prima terhadap p. Ini berarti bahwa sistem residu tereduksi modulo $p$adalah himpunan $\{1, 2, 3,\ldots,p - 1\}$ yang mana seluruh anggotanya sebanyak $(p - 1)$ sehingga $\phi(p) = p - 1$ (Muhsetyo, 1997:280).

   d. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya e, yang relatif prima terhadap $\phi(n)$.Bilangan yang relatif prima adalah bilangan yang memiliki $gcd = 1$.

e. Selanjutnya menghitung nilai *d*, dengan kekongruenan $ed \equiv 1 \pmod{\phi(n)}$.

Karena $gcd\,(e,\phi(n)) = 1 \rightarrow ed + \phi(n).k = 1$

$ed = 1 - \phi(n).k$

$\phi(n).k = 1 - ed$

$\phi(n).k = -(ed - 1)$

$\phi(n).k = ed - 1$

$ed \equiv 1 \pmod{\phi(n)}$.

sehinggad dapat dihitung dengan cara yang sederhana dengan persamaan:

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

Dengan mencoba nilai-nilai *k*, sehingga diperoleh nilai *d* bilangan bulat.

Melalui langkah di atas maka diperoleh:

- kunci publik: (*e*,*n*).
- kunci privat: (*d*,*n*)

2. Mengenkripsi Pesan

Langkah-langkah mengenkripsi pesan dengan algoritma RSA:

a. Plain teks terlebih dahulu dipecah menjadi blok-blok kecil.

b. Melakukan perhitungan menggunakan rumus sebagai berikut:

$c_i = m_i^e \pmod{n}$ (Caroline, 2011).

Karena$c_i = m_i^e \pmod{n} \rightarrow n \mid c_i - m_i^e$

$n \mid c_i \rightarrow c_i = n \,.\, k, \forall k \in \mathbb{Z}$

atau

$n \mid m_i^e \rightarrow m_i^e = n \,.\, t, \quad \forall t \in \mathbb{Z}$

3. Mendekripsi Pesan

Langkah-langkah mendekripsi pesan dengan algoritma RSA:

a. Dengan menghitung rumus $m_i = {c_i}^d (\mathrm{mod}\, n)$ dengan d adalah kunci privat (Caroline, 2011)

Karena $m_i = {c_i}^d (\mathrm{mod}\, n) \rightarrow n \mid m_i - {c_i}^d$

$n \mid m_i \rightarrow m_i = n \,.\, k, \forall k \in \mathbb{Z}$

atau

$n \mid {c_i}^d \rightarrow {c_i}^d = n \,.\, t, \quad \forall t \in \mathbb{Z}$

4.2 Perumusan Algoritma Kriptografi Elgamal

Kriptografi Elgamal ditemukan oleh ilmuwan Mesir, yaitu Taher Elgamal pada tahun 1985, merupakan algoritma kriptografi kunci publik. Algoritma Elgamal terdiri atas tiga proses, yaitu proses pembentukan kunci, enkripsi, dan dekripsi. Elgamal merupakan algoritma dalam kriptografi yang termasuk dalam kategori algoritma asimetris

Besaran – besaran yang digunakan pada algoritma kriptografi Elgamal antara lain:

1. p bilangan prima.
2. g bilangan bulat.
3. x bilangan bulat.
4. y, g, p (kunci publik).
5. x, p (kunci privat).

1. Membangkitkan Kunci.

Langkah-langkah membangkitkan kunci dengan algoritma Elgamal:

a. Pilih sembarang bilangan prima $p \geq 5$.

b. Pilih dua buah bilangan acak$g,x \in \mathbb{Z}$, dengan syarat $g < p$ dan $1 \leq x \leq p - 2$.

c. Hitung $y = g^x \pmod{p}$ (Caroline, 2011).

Melalui langkah di atas maka akan didapat:

- kunci publik: triple (y, g, p).
- kunci privat: pasangan (x, p).

Contoh:

Pilih bilangan prima $p = 5$ dan bilangan bulat $g = 2$ dan $x = 3$, dimana $g < p$ dan $1 \leq x \leq p - 2$. Selanjutnya dapat dihitung:

$y = g^x \pmod{p}$

$= 2^3 \pmod{5}$

$= 8 \bmod 5$

$= 3$

Dan diperoleh:

- kunci publik: triple $(y, g, p) = (3, 2, 5)$
- kunci privat: pasangan $(x, p) = (3, 5)$

2. Mengenkripsi Pesan

Langkah-langkah mengenkripsi pesan dengan algoritma Elgamal:

a. Pertama-tama plain teks dipecah-pecah menjadi blok yang lebih kecil dan disusun menjadi blok-blok $m_1, m_2, \ldots, m_n$.

b. Pilih bilangan acak k yang terletak pada nilai $1 \leq k \leq p-2$

c. Setiap blok m dienkripsi dengan rumus:

$a = g^k \pmod{p}$ dan $b = y^k\, m \pmod{p}$ (Caroline, 2011).

Contoh:

Diberikan plainteks (m) “B”, yang jika dikonversikan ke kode ASCII bernilai m = 66. Dari proses pembentukan kunci diketahui bilangan prima$p$ = 5, bilangan bulat g = 2,y = 3. kemudian pilih bilangan acak k = 3. Selanjutnya dapat dihitung:

$a = g^k \pmod p$

$= 2^3 \pmod 5$

$= 8 \pmod 5$

$= 3$

Dan

$b = y^k\, m \pmod p$

$= 3^3 . 66 \pmod 5$

$= 1782 \pmod 5$

$=2$

3. Mendekripsi Pesan

Langkah-langkah mendekripsi pesan dengan algoritma Elgamal:

a. Gunakan kunci privat x untuk menghitung $a^{-x} = a^{p-1-x} \pmod p$ (Caroline, 2011).

Berdasarkan teorema fermat setiap $p$bilangan prima dan $p \nmid a$ maka

$a^{p-1} \equiv 1 \pmod p$.

Ada p bilangan prima dan untuk suatu $a \in \mathbb{Z}$ $p \nmid a$ jadi diperoleh:

$a^{p-1} \equiv 1 \pmod p$, jika kedua ruas dikalikan a^{-x} maka:

$a^{-x} . a^{p-1} \equiv a^{-x} . 1 \pmod p$

$a^{p-1-x} \equiv a^{-x} \pmod p$ atau dapat ditulis

$a^{-x} = a^{p-1-x} \pmod p$

Contoh :

Diketahui $a = 3$, $p = 5$, dan x = 3. Selanjutnya dapat dihitung:

$a^{-x} = a^{p-1-x} (\text{mod } p)$

$= 3^{5-1-3} (\text{mod } 5)$

$= 3$

b. Hitung plain teks m dengan persamaan: $m = b \,.\, (a^x)^{-1} (\text{mod} p)$ (Caroline, 2011).

Dari persamaan $m = b \,.\, (a^x)^{-1} (\text{mod} p)$ diketahui:

$a = g^k (\text{mod } p)$

$b = y^k \, m (\text{mod } p)$

$y = g^x (\text{mod } p)$

Teorema 4.2.1

Diberika (p, g y) sebagai kunci publik dan x sebagai kunci privat pada kriptografi Elgamal. Jika diberikan cipherteks (a, b) maka $m = b \,.(a^x)^{-1} (\text{mod } p)$ dengan m adalah plainteks (Stinson, 1995:68).

Bukti:

$b \,.\, (a^x)^{-1} \equiv y^k \, m \,.\, (a^x)^{-1} (\text{mod } p)$

$\equiv (g^x)^k m.(g^k)^{-x} (\text{mod } p)$

$\equiv g^{xk} \,.g^{k-x} \,.m (\text{mod } p)$

$\equiv g^0 .m (\text{mod } p)$

$\equiv m (\text{mod } p)$

Dengan demikian didapatkan:

$b \,.\, (a^x)^{-1} \equiv m (\text{mod } p)$ atau $m = b \,.(a^x)^{-1} (\text{mod } p)$

Contoh:

Diketahui $b = 2$, $a^{-x} = 3$, $p = 5$. Selanjutnya dapat dihitung:

$m = b \,.\, (a^{x})^{-1} \,(\text{mod } p)$
$= 2.\ 3 \,(\text{mod } 5)$
$= 6 \,(\text{mod } 5)$
$= 1$

4.3 Implementasi Algoritma

Selanjutnya peneliti membuat kasus permasalahan menyamarkan pesan pada algoritma RSA dan algoritma Elgamal dengan pesan rahasia yang sama dengan menggunakan bilangan prima aman dan bilangan prima tidak aman. Pesan tersebut berbunyi "SELAMAT PAGI" dan pesan ini merupakan pesan rahasia, maka yang harus dilakukan:

Diberikan tabel konversi pesan ke dalam ASCII seperti di bawah ini:

Tabel 4.1 Konversi Pesan ke Dalam Kode ASCII

i	**Karakter**	**Plainteks *m***	**Kode ASCII**
1	S	m_1	83
2	E	m_2	69
3	L	m_3	76
4	A	m_4	65
5	M	m_5	77
6	A	m_6	65
7	T	m_7	84
8	(Spasi)	m_8	32
9	P	m_9	80
10	A	m_{10}	65
11	G	m_{11}	71
12	I	m_{12}	73

Algoritma 4.1 : Tes Bilangan Prima

Input : Bilangan prima $p \geq 5$.

Output: Pernyataan "*p* prima aman" atau "*p* bukan prima aman" (Hamidah, 2009)

Langkah:

1. Hitung $q = \frac{p-1}{2}$
2. Jika *q* adalah bilangan prima, maka *output* (*p*prima aman)
3. Jika *q* adalah bilangan komposit, maka *output* (*p*bukan prima aman)

4.3.1 Implementasi Algoritma Kriptografi RSA Dengan Bilangan Prima Aman

1. Proses pembentukan kunci algoritma RSA:

   a. Peneliti memberikan contoh bilangan prima p_1 = 107 dan p_2 = 179. Berdasarkan algoritma tes bilangan prima aman, maka:

$$q = \frac{p_1 - 1}{2}$$

$$= \frac{107 - 1}{2}$$

$$= \frac{106}{2}$$

$$= 53$$

Karena *q* = 53 bilangan prima, maka p_1 bilangan prima aman.

Demikian juga untuk p_2 maka:

$$q = \frac{p_2 - 1}{2}$$

$$= \frac{179 - 1}{2}$$

$$= \frac{178}{2}$$

$$= 89$$

Karena q = 89 bilangan prima, maka p_2 bilangan prima aman.

Jadi, p_1 dan $p_2$merupakan bilangan prima aman.

b. Kemudian menghitung nilai n:

$n = p_1 . p_2$

$= 107 . 179$

$= 19153$

c. Setelah mendapat nilai n, langkah selanjutnya mencari nilai ϕnuntuk menyatakan banyaknya bilangan bulat $< n$yang relatif prima terhadap n:

$\phi n=(p_1-1) . (p_2-1)$

$= (107 – 1) . (179 – 1)$

$= 18868$

d. Langkah selanjutnya menentukan nilai e yang relatif prima dengan ϕn:

Pada permasalahan ini peneliti memilih e = 719, karena gcd (18868, 719) =1

Hal ini dapat ditunjukkan sebagai berikut:

$18868 = 26 . 719 + 174$

$719 = 4 . 174 + 23$

$174 = 7 . 23 + 13$

$23 = 1 . 13 + 10$

$13 = 1 . 10 + 3$

$10 = 3 . 3 + 1$

$3 = 1 . 3 + 0$

Karena sisa terakhir sebelum 0 adalah 1, maka *gcd* (18868,719) = 1. Jadi nilai *e* = 719

e. Langkah selanjutnya mencari nilai *d* dengan menghitung:

$d = \frac{1+k\phi(n)}{e}$dengan mencoba nilai nilai k = 1, 2, 3,….,219 menggunakan Microsoft exel, sehingga diperoleh nilai *d* bilangan bulat, yaitu dengan k = 219.

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

$$d = \frac{1 + 219\,.18868}{719}$$

$$d = \frac{1 + 4132092}{719}$$

$$d = 5747$$

Dengan demikian diperoleh kunci publiknya (*e*,*n*) = (719,19153) dan kunci privatnya (*d*,*n*) = (5747,19153)

2. Melakukan proses enkripsi dengan persamaan:

$c_i = m_i^e \bmod n$, yang dalam hal ini *e*adalah kunci publik, sehingga didapat:

$c_1 = 83^{719} \bmod 19153 = 11345$

$c_2 = 69^{719} \bmod 19153 = 6136$

$c_3 = 76^{719} \bmod 19153 = 9176$

$c_4 = 65^{719} \bmod 19153 = 15998$

$c_5 = 77^{719} \bmod 19153 = 12248$

$c_6 = 65^{719} \bmod 19153 = 15998$

$c_7 = 84^{719} \bmod 19153 = 5932$

$c_8 = 32^{719} \bmod 19153 = 13896$

$c_9 = 80^{719} \bmod 19153 = 10718$

$c_{10} = 65^{719} \bmod 19153 = 15998$

$c_{11} = 71^{719} \bmod 19153 = 4090$

$c_{12} = 73^{719} \bmod 19153 = 16746$

3. Melakukan proses dekripsi dengan persamaan:

   $m_i = c_i{}^d \bmod n$, yang dalam hal ini d adalah kunci privat, sehingga didapat:

$m_1 = 11345^{5747} \bmod 19153 = 83$

$m_2 = 6136^{5747} \bmod 19153 = 69$

$m_3 = 9176^{5747} \bmod 19153 = 76$

$m_4 = 15998^{5747} \bmod 19153 = 65$

$m_5 = 12248^{5747} \bmod 19153 = 77$

$m_6 = 15998^{5747} \bmod 19153 = 65$

$m_7 = 5932^{5747} \bmod 19153 = 84$

$m_8 = 13896^{5747} \bmod 19153 = 32$

$m_9 = 10718^{5747} \bmod 19153 = 80$

$m_{10} = 15998^{5747} \bmod 19153 = 65$

$m_{11} = 4090^{5747} \bmod 19153 = 71$

$m_{12} = 16746^{5747} \bmod 19153 = 73$

4.3.2 Implementasi Algoritma Kriptografi Elgamal Dengan Bilangan Prima Aman

1. Proses pembentukan kunci algoritma elgamal:

   a. Peneliti memberikan contoh bilangan prima p = 107 dan dua buah bilangan acak g dan $x$dengan g = 2 dan x = 63

b. Menghitung nilai *y* dengan rumus:

$y = g^x \bmod p$

Sehingga didapat $y = 2^{63} \bmod 107 = 46$. Dengan demikian diperoleh kunci publiknya $(y,g,p) = (46, 2, 107)$ dan kunci privatnya $(x, p) = (63, 107)$

2. Melakukan proses enkripsi menggunakan kunci publik dan memilih bilangan bulat acak k untuk setiap karakter dengan $k_i \in \{1,2,\dots,107-1\}$, $i = 1,2,3,\dots,13$. Kemudian kita hitung $a = g^k \pmod p$, dan $b = y^k\, m \pmod p$

Tabel 4.2 Perhitungan Enkripsi Pada Bilangan Prima Aman

i	m_i	k_i	$a = g^k \pmod p$ $a = 2^k \pmod{107}$	$b = y^k\, m \pmod p$ $b = 46^k\, m \pmod{107}$
1	83	57	91	21
2	69	43	7	78
3	76	65	77	82
4	65	88	89	66
5	77	34	9	98
6	65	46	56	93
7	84	47	5	4
8	32	76	85	22
9	80	87	98	83
10	65	69	55	23
11	71	41	82	11
12	73	35	18	23

3. Melakukan proses dekripsi dengan kunci privat sebagai berikut:

Tabel 4.3 Perhitungan Dekripsi Pada Bilangan Prima Aman

I	*A*	*b*	$a^{-x} = a^{p-1-x} \pmod p$ $a^{-x} = a^{107-1-63} \pmod{107}$	$m = b \,.\, (a^x)^{-1} \pmod p$ $m = b \,.\, (a^x)^{-1} \pmod{107}$	karakter
1	91	21	60	83	S
2	7	78	5	69	E
3	77	82	74	76	L
4	89	66	48	65	A
5	9	98	39	77	M
6	56	93	3	65	A
7	5	4	21	84	T
8	85	22	89	32	(Spasi)

(Lanjutan)

I	***A***	***b***	$a^{-x} = a^{p-1-x} \pmod p$ $a^{-x} = a^{107-1-63} \pmod{107}$	$m = b \,.\, (a^x)^{-1} \pmod p$ $m = b \,.\, (a^x)^{-1} \pmod{107}$	**karakter**
9	98	83	68	80	P
10	55	23	54	65	A
11	82	11	94	71	G
12	18	23	59	73	I

4.3.3 Implementasi Algoritma Kriptografi RSA Dengan Bilangan Prima Tidak Aman

1. Proses pembentukan kunci algoritma RSA:

   a. Peneliti memberikan contoh bilangan prima p_1 = 307 dan p_2 = 353.

   Berdasarkan algoritma tes bilangan prima aman, maka:

$$q = \frac{p_1 - 1}{2}$$

$$= \frac{307 - 1}{2}$$

$$= \frac{306}{2}$$

$$= 153$$

   Karena q = 153 bukan bilangan prima, maka p_1 bilangan prima tidak aman.

   Demikian juga untuk p_2,maka:

$$q = \frac{p_2 - 1}{2}$$

$$= \frac{353 - 1}{2}$$

$$= \frac{352}{2}$$

$$= 176$$

   Karena q = 176 bukan bilangan prima, maka p_2 bilangan prima tidak aman.

   Jadi, p_1 dan p_2 merupakan bilangan prima tidak aman.

b. Kemudian menghitung nilai *n*:

$n = p_1 . p_2$

= 307 . 353

= 108371

c. Setelah mendapat nilai *n*, langkah selanjutnya mencari nilai ϕ*n* untuk menyatakan banyaknya bilangan bulat < *n*yang relatif prima terhadap *n*:

$\phi n=(p_1-1) . (p_2-1)$

= (307 – 1) . (353 – 1)

= 306 . 352

= 107712

d. Langkah selanjutnya menentukan nilai *e* yang relatif prima denganϕ*n*

Pada permasalahan ini peneliti memilih *e* = 719, karena *gcd* (107712, 719) = 1.

Hal ini dapat ditunjukkan sebagai berikut:

107712 = 149 . 719 + 581

719 = 1 . 581 + 138

581 = 4 . 138 + 29

138 = 4 . 29 + 22

29 = 11 . 22 + 7

22 = 3 . 7 + 1

7 = 7 . 1 + 0

Karena sisa terakhir sebelum 0 adalah 1, maka *gcd* (107712,719) = 1.

Jadi nilai *e* = 719

e. Langkah selanjutnya mencari nilai *d* dengan menghitung:

$d = \frac{1+k\phi(n)}{e}$ dengan mencoba nilai-nilai k = 1, 2, 3,….,99 menggunakan microsoft exel sehingga diperoleh nilai *d* bilangan bulat, yaitu dengan k = 99.

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

$$d = \frac{1 + 99\,.107712}{719}$$

$$d = \frac{1 + 10663488}{719}$$

$$d = 14831$$

Dengan demikian diperoleh kunci publiknya (e,n) = (719,108371) dan kunci privatnya (d,n) = (14831,108371)

2. Melakukan proses enkripsi dengan persamaan:

$c_i = m_i{}^e \bmod n$, yang dalam hal ini *e*adalah kunci publik, sehingga didapat:

$c_1 = 83^{719} \bmod 108371 = 106110$
$c_2 = 69^{719} \bmod 108371 = 4027$
$c_3 = 76^{719} \bmod 108371 = 68367$
$c_4 = 65^{719} \bmod 108371 = 42425$
$c_5 = 77^{719} \bmod 108371 = 90131$
$c_6 = 65^{719} \bmod 108371 = 42425$
$c_7 = 84^{719} \bmod 108371 = 61055$
$c_8 = 32^{719} \bmod 108371 = 79004$
$c_9 = 80^{719} \bmod 108371 = 58182$
$c_{10} = 65^{719} \bmod 108371 = 42425$
$c_{11} = 71^{719} \bmod 108371 = 61142$
$c_{12} = 73^{719} \bmod 108371 = 56777$

3. Melakukan proses dekripsi dengan persamaan:

   $m_i = {c_i}^d \bmod n$, yang dalam hal ini d adalah kunci privat, sehingga didapat:

$$m_1 = 106110^{14831} \bmod 108371 = 83$$
$$m_2 = 4027^{14831} \bmod 108371 = 69$$
$$m_3 = 68367^{14831} \bmod 108371 = 76$$
$$m_4 = 42425^{14831} \bmod 108371 = 65$$
$$m_5 = 90131^{14831} \bmod 108371 = 77$$
$$m_6 = 42425^{14831} \bmod 108371 = 65$$
$$m_7 = 61055^{14831} \bmod 108371 = 84$$
$$m_8 = 79004^{14831} \bmod 108371 = 32$$
$$m_9 = 58182^{14831} \bmod 108371 = 80$$
$$m_{10} = 42425^{14831} \bmod 108371 = 65$$
$$m_{11} = 61142^{14831} \bmod 108371 = 71$$
$$m_{12} = 56777^{14831} \bmod 108371 = 73$$
$$m_{13} = 5197^{14831} \bmod 108371 = 65$$

4.3.4 Implementasi Algoritma Kriptografi Elgamal Dengan Bilangan Prima Tidak Aman

1. Proses pembentukan kunci algoritma elgamal:
   a. Peneliti memberikan contoh bilangan prima p = 307 dan dua buah bilangan acak g dan x, dengan g = 2 dan x = 63
   b. Menghitung nilai $y$dengan rumus:

      $y = g^x \bmod p$

      Sehingga didapat $y = 2^{63} \bmod 307$ = 202. Dengan demikian diperoleh kunci publiknya (y,g,p) = (202, 2, 307) dan kunci privatnya (x, p) = (63, 307)

2. Melakukan proses enkripsi menggunakan kunci publik dan memilih bilangan bulat acak k untuk setiap karakter dengan $k_i \in \{1,2,\dots,307-1\}$, $i = 1,2,3,\dots,13$. Kemudian kita hitung $a = g^k \pmod p$, dan $b = y^k\, m \pmod p$

Tabel 4.4 Perhitungan Enkripsi Pada Bilangan Prima Tidak Aman

i	m_i	k_i	$a = g^k \pmod p$ $a = 2^k \pmod{307}$	$b = y^k\, m \pmod p$ $b = 202^k\, m \pmod{307}$
1	83	57	243	142
2	69	43	301	189
3	76	65	298	125
4	65	88	144	232
5	77	34	289	77
6	65	46	259	112
7	84	47	211	58
8	32	76	54	154
9	80	87	72	11
10	65	69	34	236
11	71	41	152	282
12	73	35	271	10

3. Melakukan proses dekripsi dengan kunci privat sebagai berikut:

Tabel 4.5 Perhitungan Dekripsi Pada Bilangan Prima Tidak Aman

I	a	b	$a^{-x} = a^{p-1-x} \pmod p$ $a^{-x} = a^{307-1-63} \pmod{307}$	$m = b\,.\,(a^x)^{-1} \pmod p$ $m = b\,.\,(a^x)^{-1} \pmod{307}$	Karakter
1	243	142	193	83	S
2	301	189	283	69	E
3	298	125	202	76	L
4	144	232	81	65	A
5	289	77	1	77	M
6	259	112	102	65	A
7	211	58	192	84	T
8	54	154	64	32	(Spasi)
9	72	11	91	80	P
10	34	236	38	65	A
11	152	282	34	71	G
12	271	10	38	73	I

4.4 Hasil Enkripsi dan Dekripsi Pada Bilangan Prima Aman:

Tabel 4.6 Hasil Enkripsi dan Dekripsi Pada Bilangan Prima Aman

Kriptografi	**Bilangan Prima**	**Hasil enkripsi**	**Hasil Dekripsi**	**Karakter**
RSA	p_1 = 107 p_2 = 179	11345, 6136, 9176, 15998, 12248, 15998, 5932, 13896, 10718, 15998, 4090, 16746.	83, 69, 76, 65, 77, 65, 84, 32, 80, 65, 71, 73	SELAMAT PAGI
Elgamal	p = 107	(91,21)(7,78) (77,82)(89,66) (9,98)(56,93)(5,4)(85,22) (98,83)(55,23)(82,11)(18,23)	83, 69, 76, 65, 77, 65, 84, 32, 80, 65, 71, 73	SELAMAT PAGI

Dari tabel 4.6 dapat dilihat bahwa proses dekripsi algoritma kriptografi RSA dan algoritma kriptografi Elgamal menggunakan bilangan prima aman semuanya dilakukan dengan baik.

4.5 Hasil Enkripsi dan Dekripsi Pada Bilangan Prima Tidak Aman:

Tabel 4.7 Hasil Enkripsi dan Dekripsi Pada Bilangan Prima Tidak Aman

Kriptografi	Bilangan Prima	Hasil enkripsi	Hasil Dekripsi	Karakter
RSA	p_1 = 307 p_2 = 353	106110, 4027, 68367, 42425, 90131, 42425, 61055, 79004, 58182, 42425, 61142, 56777.	83, 69, 76, 65, 77, 65, 84, 32, 80, 65, 71, 73	SELAMAT PAGI

(Lanjutan)

Kriptografi	Bilangan Prima	Hasil enkripsi	Hasil Dekripsi	Karakter
Elgamal	p = 307	(243,142)(301,189) (298,125)(144,232) (289,77)(259,112) (211,58)(54,154) (72,11)(34,236) (152,282)(271,10)	110, 105, 108, 97, 105, 32,90, 97, 104, 114, 97, 32, 65.	SELAMAT PAGI

Dari tabel 4.7 dapat dilihat bahwa proses dekripsi algoritma kriptografi RSA dan algoritma kriptografi Elgamal menggunakan bilangan prima tidak aman semuanya juga dilakukan dengan baik

BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil analisa dan pembahasan dapat disimpulkan beberapa hal sebagai berikut:

1. Pada algoritma kriptografi RSA dengan menggunakan bilangan prima aman maupun bilangan prima tidak aman, proses pembentukan kunci, proses enkripsi, dan proses dekripsi tetap dapat berjalan dengan baik. Dan proses enkripsi algoritma kriptografi RSA diperoleh dari rumus $c_i = m_i^e \bmod n$, sedangkan proses dekripsi algoritma kriptografi RSA diperoleh dari rumus $m_i = c_i^d \bmod n$
2. Pada algoritma kriptografi Elgamal dengan menggunakan bilangan prima aman maupun bilangan prima tidak aman, proses pembentukan kunci, proses enkripsi, dan proses dekripsi juga tetap dapat berjalan dengan baik. Dan proses enkripsi algoritma kriptografi Elgamal diperoleh dari rumus $a = g^k \pmod p$ dan $b = y^k\, m \pmod p$ sedangakan proses dekripsi algoritma Elgamal diperoleh dari rumus $a^{-x} = a^{p-1-x} \pmod p$ dan $m = b \,.\, (a^x)^{-1} \pmod p$

5.2 Saran

Pada penulisan skripsi ini penulis mengkaji perumusan algoritma kriptografi Asimetri yaiut algoritma kriptografi RSA dan algoritma kriptografi Elgamal.Untuk skripsi selanjutnya bisa dikembangkan dengan mengkaji algoritma kriptografi asimetri yang lain seperti algoritma kriptografi DSA, DH, ECC, dan lain sebagainya.

DAFTAR PUSTAKA

Abdussakir. 2009. *Matematika 1 Kajian Integratif Matematika dan Al-Qur'an.* Malang: UIN Malang Press.

Arifin, Z.. 2009. *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman*, Jurnal Informatika Mulawarman. Pdf (diakses tanggal 4Mei 2014).

Buseng, V.. 2013. *Sistem Bilangan Biner*. *http://catatan-goblog.blogspot.com/2013/04/sistem-bilangan-biner.html* (diakses pada tanggal 27 Mei 2014).

Hamidah, S.N.. 2009. *Konsep Matematis dan Proses Penyandian Kriptografi ElGamal*. Skripsi tidak diterbitkan. Malang: Universitas Islam Negeri Malang.

Hasan., M.I. 2002.. *Pokok-pokok Materi Metodologi Penelitian dan Aplikasinya*. Bogor: Ghalia Indonesia.

Caroline, M.L.. 2011 *http://informatika.stei.itb.ac.id/~rinaldi.munir/ Kriptografi/ Makalah2/Makalah2-IF3058-Sem2-2010-2011-029.pdf* (diakses pada tanggal 12 September 2014)

Muhsetyo, G. 1997. *Dasar-Dasar Teori Bilangan*. Jakarta: PGSM.

Munir, R. 2012. *Matematika Diskrit.* Bandung: Informatika

Respatiadi, F. 2013. Berbagi matematika. *http://faisalrespatiadi25.blogspot.com/2013/07/modulo.html* (diakses pada tanggal 15 januari 2015)

Sadikin, R. 2012. *Kriptografi Untuk Keamanan Jaringan.* Yogyakarta: Andi

Stinson, D.R.. 1995. *Cryptography Theory and Practice*, Florida: CRC Press, Inc

Sugiyono. 2010. *Metode Penelitian Kuantitatif Kualitatif & RND*. Bandung: Alfabeta

LAMPIRAN-LAMPIRAN

Lampiran 1.Tabel Kode ASCII

Tabel 1. Kode ASCII

No.	Kode	No.	Kode
0	NULL (null)	65	A
1	SOH (start of heading)	66	B
2	STX (start of text)	67	C
3	ETX (end of text)	68	D
4	EOT (end of transmission)	69	E
5	ENQ (enquiry)	70	F
6	ACK (acknowledge)	71	G
7	BEL (bell)	72	H
8	BS (backspace)	73	I
9	TAB (horizontal tab)	74	J
10	LF (new line)	75	K
11	VT (vertical tab)	76	L
12	FF (new page)	77	M
13	CR (carriage return)	78	N
14	SO (shift out)	79	O
15	SI (shift in)	80	P
16	DLE (data link espace)	81	Q
17	DC1 (device control 1)	82	R
18	DC2 (device control 1)	83	S
19	DC3 (device control 1)	84	T
20	DC4 (device control 1)	85	U
21	NAK (negative acknowledge)	86	V
22	SYN (synchronus idle)	87	W
23	ETB (end of trans. Blok)	88	X
24	CAN (cancel)	89	Y
25	EM (end of medium)	90	Z
26	SUB (substitute)	91	[
27	ESC (escape)	92	\
28	FS (file separator)	93	]
29	GS (group separator)	94	^
30	RS (record separator)	95	_
31	US (unit separator)	96	‘
32	Space	97	a
33	!	98	b
34	"	99	c

35	#
36	$
37	%
38	&
39	'
40	(
41	)
42	*
43	+
44	,
45	-
46	.
47	/
48	0
49	1
50	2
51	3
52	4
53	5
54	6
55	7
56	8
57	9
58	:
59	;
60	<
61	=
62	>
63	?
64	@

100	d
101	e
102	f
103	g
104	h
105	i
106	j
107	k
108	l
109	m
110	n
111	o
112	p
113	q
114	r
115	s
116	t
117	u
118	v
119	w
120	x
121	y
122	z
123	{
124	|
125	}
126	~
127	DEL

Lampiran 2

Mencarinilai *d*, dengan$\phi(n) = 18868$denganrumus$d = \frac{1+k\phi(n)}{e}$

menggunakan Microsoft Exel:

Tabel .2 Mencari nilai *d*, dengan $\phi(n) = 18868$dengan rumus $d = \frac{1+k\phi(n)}{e}$ menggunakan Microsoft Exel:

No.	Nilai *k*	Hasil nilai *d*
1	1	26,24339
2	2	52,4854
3	3	78,7274
4	4	104,9694
5	5	131,2114
6	6	157,4534
7	7	183,6954
9	8	209,9374
9	9	236,1794
10	10	262,4214
11	11	288,6634
12	12	314,9054
13	13	341,1474
14	14	367,3894
15	15	393,6314
16	16	419,8734
17	17	446,1154
18	18	472,3574
19	19	498,5994
20	20	524,8414
21	21	551,0834
22	22	577,3255
23	23	603,5675
24	24	629,8095
25	25	656,0515
26	26	682,2935
27	27	708,5355
28	28	734,7775
29	29	761,0195
30	30	787,2615
31	31	813,5035
32	32	839,7455
33	33	865,9875
34	34	892,2295
35	35	918,4715
36	36	944,7135
37	37	970,9555
38	38	997,1975
39	39	1023,439
40	40	1049,682

41	41	1075,924
42	42	1102,166
43	43	1128,408
44	44	1154,65
45	45	1180,892
46	46	1207,134
47	47	1233,376
48	48	1259,618
49	49	1285,86
50	50	1312,102
51	51	1338,344
52	52	1364,586
53	53	1390,828
54	54	1417,07
55	55	1443,312
56	56	1469,554
57	57	1495,796
58	58	1522,038
59	59	1548,28
60	60	1574,522
61	61	1600,764
62	62	1627,006
63	63	1653,248
64	64	1679,49
65	65	1705,732
66	66	1731,974
67	67	1758,216
68	68	1784,458
69	69	1810,7
70	70	1836,942
71	71	1863,184
72	72	1889,426
73	73	1915,668
74	74	1941,91
75	75	1968,152
76	76	1994,394
77	77	2020,636
78	78	2046,878
79	79	2073,12
80	80	2099,362
81	81	2125,604
82	82	2151,846
83	83	2178,088
84	84	2204,33
85	85	2230,572
86	86	2256,814
87	87	2283,056
88	88	2309,298
89	89	2335,54
90	90	2361,782
91	91	2388,024

92	92	2414,266
93	93	2440,508
94	94	2466,75
95	95	2492,992
96	96	2519,234
97	97	2545,476
98	98	2571,718
99	99	2597,96
100	100	2624,202
101	101	2650,444
102	102	2676,686
103	103	2702,928
104	104	2729,17
105	105	2755,412
106	106	2781,654
107	107	2807,896
108	108	2834,138
109	109	2860,38
110	110	2886,622
111	111	2912,864
112	112	2939,106
113	113	2965,348
114	114	2991,59
115	115	3017,832
116	116	3044,074
117	117	3070,316
118	118	3096,558
119	119	3122,8
120	120	3149,042
121	121	3175,284
122	122	3201,526
123	123	3227,768
124	124	3254,01
125	125	3280,252
126	126	3306,494
127	127	3332,736
128	128	3358,978
129	129	3385,22
130	130	3411,462
131	131	3437,704
132	132	3463,946
133	133	3490,188
134	134	3516,43
135	135	3542,672
136	136	3568,914
137	137	3595,156
138	138	3621,398
139	139	3647,64
140	140	3673,882
141	141	3700,124
142	142	3726,366

143	143	3752,608
144	144	3778,85
145	145	3805,092
146	146	3831,334
147	147	3857,576
148	148	3883,818
149	149	3910,06
150	150	3936,302
151	151	3962,544
152	152	3988,786
153	153	4015,028
154	154	4041,27
155	155	4067,512
156	156	4093,754
157	157	4119,996
158	158	4146,238
159	159	4172,48
160	160	4198,722
161	161	4224,964
162	162	4251,206
163	163	4277,448
164	164	4303,69
165	165	4329,932
166	166	4356,174
167	167	4382,416
168	168	4408,658
169	169	4434,9
170	170	4461,142
171	171	4487,384
172	172	4513,626
173	173	4539,868
174	174	4566,11
175	175	4592,352
176	176	4618,594
177	177	4644,836
178	178	4671,078
179	179	4697,32
180	180	4723,562
181	181	4749,804
182	182	4776,046
183	183	4802,288
184	184	4828,53
185	185	4854,772
186	186	4881,014
187	187	4907,256
188	188	4933,498
189	189	4959,74
190	190	4985,982
191	191	5012,224
192	192	5038,466
193	193	5064,708

194	194	5090,95
195	195	5117,192
196	196	5143,434
197	197	5169,676
198	198	5195,918
199	199	5222,16
200	200	5248,402
201	201	5274,644
202	202	5300,886
203	203	5327,128
204	204	5353,37
205	205	5379,612
206	206	5405,854
207	207	5432,096
208	208	5458,338
209	209	5484,58
210	210	5510,822
211	211	5537,064
212	212	5563,306
213	213	5589,548
214	214	5615,79
215	215	5642,032
216	216	5668,274
217	217	5694,516
218	218	5720,758
219	**219**	**5747**

Lampiran3

Mencarinilai d, dengan$\phi(n) = 107712$denganrumus$d = \frac{1+k\phi(n)}{e}$ menggunakan Microsoft Exel:

Tabel 3. Mencarinilai d, dengan$\phi(n) = 107712$ dengan rumus $d = \frac{1+k\phi(n)}{e}$ menggunakan Microsoft Exel:

No.	Nilai k	Hasil nilai d
1	1	149,8095
2	2	299,6175
3	3	449,4256
4	4	599,2337
5	5	749,0417
6	6	898,8498
7	7	1048,658
8	8	1198,466
9	9	1348,274
10	10	1498,082
11	11	1647,89
12	12	1797,698

13	13	1947,506
14	14	2097,314
15	15	2247,122
16	16	2396,93
17	17	2546,739
18	18	2696,547
19	19	2846,355
20	20	2996,163
21	21	3145,971
22	22	3295,779
23	23	3445,587
24	24	3595,395
25	25	3745,203
26	26	3895,011
27	27	4044,819
28	28	4194,627
29	29	4344,435
30	30	4494,243
31	31	4644,051
32	32	4793,86
33	33	4943,668
34	34	5093,476
35	35	5243,284
36	36	5393,092
37	37	5542,9
38	38	5692,708
39	39	5842,516
40	40	5992,324
41	41	6142,132
42	42	6291,94
43	43	6441,748
44	44	6591,556
45	45	6741,364
46	46	6891,172
47	47	7040,981
48	48	7190,789
49	49	7340,597
50	50	7490,405
51	51	7640,213
52	52	7790,021
53	53	7939,829
54	54	8089,637
55	55	8239,445
56	56	8389,253
57	57	8539,061
58	58	8688,869
59	59	8838,677
60	60	8988,485
61	61	9138,293
62	62	9288,102

63	63	9437,91
64	64	9587,718
65	65	9737,526
66	66	9887,334
67	67	10037,14
68	68	10186,95
69	69	10336,76
70	70	10486,57
71	71	10636,37
72	72	10786,18
73	73	10935,99
74	74	11085,8
75	75	11235,61
76	76	11385,41
77	77	11535,22
78	78	11685,03
79	79	11834,84
80	80	11984,65
81	81	12134,45
82	82	12284,26
83	83	12434,07
84	84	12583,88
85	85	12733,69
86	86	12883,5
87	87	13033,3
88	88	13183,11
89	89	13332,92
90	90	13482,73
91	91	13632,54
92	92	13782,34
93	93	13932,15
94	94	14081,96
95	95	14231,77
96	96	14381,58
97	97	14531,38
98	98	14681,19
99	**99**	**14831**

RIWAYAT HIDUP

Faurizal Fahmi Firmansyah, lahir di kota Banyuwangi pada tanggal 4 Mei 1991, biasa dipanggil Rizal, tinggal di Jl. Suwari No.08 Kecamatan Besuki Kota Situbondo. Anak kedua dari Bapak Imam Sutrisno dan Ibu Rofiqoh.

Pendidikan dasarnya ditempuh di SDN 4 Besuki Situbondo dan lulus pada tahun 2003, setelah itu melanjutkan ke SMP Negeri 1 Banyuglugur Situbondo dan lulus pada tahun 2006. Kemudian dia melanjutkan pendidikan ke SMK 1 Ibrahimy Sukorejo Situbondo dan lulus tahun 2009. Selanjutnya tahun 2009 menempuh kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil Jurusan Matematika. Selama menjadi mahasiswa, dia pernah mengikuti Unit Kegiatan Mahasiswa (UKM) Seni Religius pada divisi gambus.