KONSEP MATEMATIS DAN PROSES PENYANDIAN KRIPTOGRAFI ELGAMAL

SKRIPSI

Oleh:

SITI NUR HAMIDAH
NIM. 05510044

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN)
MAULANA MALIK IBRAHIM MALANG
2009

KONSEP MATEMATIS DAN PROSES PENYANDIAN KRIPTOGRAFI ELGAMAL

SKRIPSI

Diajukan Kepada:

Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN)
Maulana Malik Ibrahim Malang
Untuk Memenuhi Salah Satu Persyaratan Dalam
Memperoleh Gelar Sarjana Sains (S.Si)

Oleh:

SITI NUR HAMIDAH
NIM. 05510044

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN)
MAULANA MALIK IBRAHIM MALANG
2009

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Siti Nur Hamidah

NIM : 05510044

Fakultas / Jurusan : Sains dan Teknologi/ Matematika

Judul Penelitian : Konsep Matematis dan Proses Penyandian Kriptografi ElGamal

Menyatakan dengan sebenar-benarnya bahwa karya ilmiah saya ini tidak terdapat unsur-unsur penjiplakan karya penelitian atau karya ilmiah yang pernah dilakukan atau dibuat oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata hasil penelitian ini terbukti terdapat unsur-unsur penjiplakan, maka saya bersedia untuk mempertanggung jawabkan, serta diproses sesuai peraturan yang berlaku.

Malang, 10 Oktober 2009

Yang Membuat Pernyataan,

Siti Nur Hamidah
NIM. 05510044

KONSEP MATEMATIS DAN PROSES PENYANDIAN KRIPTOGRAFI ELGAMAL

SKRIPSI

Oleh:

SITI NUR HAMIDAH
NIM. 05510044

Telah disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
Abdussakir, M.Pd	**Ahmad Barizi, M.A.**
NIP. 19751006 200312 1001	**NIP. 19731212 199803 1001**

Tanggal, 10 Oktober 2009

Mengetahui,
Ketua Jurusan Matematika

Abdussakir, M.Pd
NIP. 19751006 200312 1001

KONSEP MATEMATIS DAN PROSES PENYANDIAN KRIPTOGRAFI ELGAMAL

SKRIPSI

Oleh:

SITI NUR HAMIDAH
NIM. 05510044

Telah Dipertahankan di Depan Dewan Penguji Skripsi dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan Untuk Memperoleh Gelar Sarjana Sains (S.Si)

Tanggal, 10 Oktober 2009

Susunan Dewan Penguji		Tanda Tangan
1. Penguji Utama	: Usman Pagalay, M.Si NIP. 19650414 200312 1001	( )
2. Ketua	: Wahyu Henky Irawan, M.Pd NIP. 19710420 200003 1003	( )
3. Sekretaris	: Abdussakir, M.Pd NIP. 19751006 200312 1001	( )
4. Anggota	: Ahmad Barizi, M. A NIP. 19731212 199803 1001	( )

Mengetahui dan Mengesahkan
Ketua Jurusan Matematika

Abdussakir, M.Pd
NIP. 19751006 200312 1001

HALAMAN PERSEMBAHAN

Skripsi ini, penulis persembahkan kepada:

Ibunda tercinta "Siti Tajek Iyah" berserta ayahanda terkasih "Suyono" atas kerja keras, pengorbanan, ajaran, didikan dan do'anya yang tak pernah putus…

Ayunda tersayang "Taj Rosyidah" beserta suami yang senantiasa memotivasi dan mendorong penulis untuk lebih baik serta do'a tulusnya…

Ukhibbukum fillah…

MOTTO

"Hai orang-orang yang beriman apabila kamu mengadakan pembicaraan rahasia. Janganlah kamu membicarakan dengan perbuatan dosa, permusuhan dan perbuatan durhaka kepada Rasul. Dan bicarakanlah tentang membuat kebajikan dan taqwa. Dan bertaqwalah kepada Allah yang kepadaNyalah kamu dikembalikan."

Qs. Al-Mujaadillah (58): 9

"Tidak ada sistem keamanan yang benar-benar aman.
Jadi, persulitlah memasukinya dan merusak didalamnya."

KATA PENGANTAR

Alhamdulillah, segala puji syukur kehadirat *ilahi robbi*, Dzat yang maha memiliki ilmu dan merahmatkan setitik ilmu-Nya bagi seluruh dunia serta kemaha rahman-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul *Konsep Matematis dan Proses Penyandian Kriptografi ElGamal* sebagai persyaratan guna mendapat gelar Strata Satu Sarjana Sains Universitas Islam Negeri Maliki Ibrahim Malang. Sholawat dan salam semoga tercurah pada Rasulullah SAW, yang dengan penuh cinta mengajarkan ilmunya pada seluruh umat di dunia.

Penulis menyadari bahwa skripsi ini tidak akan selesai tanpa dukungan dan bantuan baik moril, spiritual maupun materiil dari pihak lain. Oleh karena itu, penulis sampaikan terima kasih yang tak terhingga kepada:

1. Prof. Dr. Imam Suprayogo, selaku Rektor Universitas Islam Negeri Maliki Malang.
2. Prof. Drs. Sutiman Bambang Sumitro, SU. DSc, selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maliki Malang.
3. Abdussakir, M.Pd, selaku ketua Jurusan Matematika Universitas Islam Negeri Maliki Malang, dan selaku dosen pembimbing I, atas keilmuan, arahan dan masukannya yang sangat berarti dalam penyusunan skripsi ini.
4. Ahmad Barizi, M.A, selaku dosen pembimbing II, arahannya selama penyusunan skripsi ini.

5. Bapak dan ibu dosen serta seluruh civitas akademik Fakultas Sains dan Teknologi Universitas Islam Negeri Maliki Malang yang telah memberikan ilmu dan kemudahan selama penulis belajar.
6. Ibunda dan ayahanda, atas perhatian dan do'anya yang tidak pernah putus.
7. Ayunda dan seluruh keluarga besar penulis atas dukungan serta do'anya.
8. Sahabat penulis, lima matahari atas mimpi dan inspirasinya.
9. Teman-teman ar-riefah: Fajriyana, Ana K., Nora A., Iftahil I., Dyah P., Sayu Imang B., M. Kurnia, Ambar, Nirma, Siti, Yuni. Tim LDK At-Tarbiyah, KAMMI UIN Malang, FORSUA atas *ukhuwah* yang indah.
10. Teman-teman matematika angkatan 2005, khususnya Indah Resti A., dan Dzawin Nuha, atas dukungan dan kerja samanya.
11. Seluruh pihak yang telah membantu dalam penyelesaian skripsi ini.

Akhirnya semoga karya ini mendapatkan ridho-Nya dan bermanfaat bagi penulis khususnya dan seluruh pecinta ilmu pada umumnya.

Malang, 10 Oktober 2009

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR AlGORITMA

ARTI LAMBANG

$x \in X$	: x anggota X
$x \notin X$	: x bukan anggota X
a|b	: a membagi b
a(mod p)	: a modulo p
$a \equiv b$	: a kongruen dengan b
$\emptyset$	: himpunan kosong
$\mathbb{Z}$	: himpunan semua bilangan bulat
$\mathbb{R}$	: himpunan semua bilangan real
$\mathbb{N}$	: himpunan semua bilangan asli
$\mathbb{Z}_p$	: himpunan bilangan bulat modulo p
$\Rightarrow$	: implikasi (jika maka)
$\Leftrightarrow$	: biimplikasi (jika dan hanya jika)
$\sum_{i=1}^{n} a_i$	: penjumlahan $a_1 + a_2 + \cdots + a_n$
$\prod_{i=1}^{n} a_1$	: perkalian $a_1 a_2 \ldots a_n$
$n!$	: n faktorial
C_r^n	: r kombinasi dari n unsur yang berbeda

ABSTRAK

Hamidah, Siti Nur. 2009. **Konsep Matematis dan Proses Penyandian Kriptografi ElGamal.** Skripsi. Jurusan Matematika. Fakultas Sains dan Teknologi, Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang. Pembimbing: Abdussakir, M. Pd. dan Ahmad Barizi, M.A.

Kata kunci: Kriptografi, Kriptografi ElGamal, Enskripsi, Deskripsi, Chiperteks, Plainteks, Bilangan Prima, Masalah Logaritma Diskrit.

Kriptografi adalah seni dan ilmu untuk menyembunyikan sebuah pesan. Didalamnya terdapat proses pembentukan kunci, enkripsi dan deskripsi. Enkripsi adalah proses pembentukan plainteks menjadi chiperteks, sedangkan deskripsi adalah proses untuk mengubah chiperteks menjadi plainteks. Algoritma yang digunakan dalam kriptografi dinamakan algoritma kriptografi dan berdasarkan jenis kunci yang dipakai algoritma kriptografi dibagi menjadi tiga, yaitu algoritma kriptografi simetri, algoritma kriptografi asimetri dan fungsi Hash.

Tujuan penulisan skripsi ini adalah menjelaskan lebih dalam tentang salah satu jenis algoritma kriptografi asimetri, yaitu kriptografi ElGamal dari konsep matematis yang melandasinya, proses pembentukan kunci dan penyandiannya serta kelebihan dan kelemahannya.

Kriptografi ElGamal dalam pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit. Sehingga, dengan memanfaatkan bilangan prima yang besar serta masalah logaritma diskrit yang cukup menyulitkan, maka keamanan kuncinya akan lebih terjamin.

Proses penyandian kriptografi ElGamal didahului pembentukan kunci, oleh penerima pesan. Dua macam pasangan kunci, yaitu kunci publik dan kunci privat. Kunci publik dapat di sebar luaskan sedang kunci privat untuk dirinya sendiri. Untuk membuat sebuah pesan rahasia pesan harus dikonversikan terlebih dahulu dalam bilangan bulat kemudian di kodekan berdasarkan kode ASCII *(American Standard for Information Interchange)*. Kriptografi ElGamal memerlukan penghitungan yang lama dan sulit untuk menghasilkan algoritma yang benar-benar aman.

Kriptografi ElGamal, yang merupakan bagian dari kriptografi simetris memiliki kelebihan dan kelemahan yang tidak jauh berbeda dengan kriptografi asimetri yang lain. Kelebihannya yang berbeda dan utama adalah kriptografi ElGamal menggunakan bilangan acak sehingga chiperteks tidak akan sama walaupun bloknya sama, sedangkan kelemahannya adalah dalam proses penghitungan yang cukup menyulitkan, karena angka-angka yang digunakan cukup besar.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi komputer telah mempengaruhi semua aspek kehidupan manusia. Baik dalam skala kecil maupun skala besar, secara langsung maupun tidak langsung kemajuan teknologi telah mempengaruhi sistem perdagangan, transaksi, informasi tak terkecuali dalam hal berkomunikasi. Salah satu contoh kemajuan teknologi komputer yang paling nyata dan dapat digunakan oleh semua orang adalah internet. Dengan adanya internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan murah. Namun di sisi lain ternyata internet, tidak terlalu aman semua informasi terkirim dalam satu jaringan yang mempunyai tingkat keamanan relatif rendah, sehingga sangat rawan untuk penyadapan informasi oleh pihak-pihak yang tidak berhak untuk mengetahui informasi tersebut. Bagi pengguna internet yang sangat luas, misalnya pada bidang pemerintahan, militer, perbankkan, pendidikan, industri dan lainnya yang kebanyakan mengandung informasi rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi. Rahasia adalah sebuah amanat dan menjaga rahasia sangat dianjurkan oleh Alloh SWT seperti dalam firman-Nya:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ ٢٧

Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu Mengetahui. (Q. S. Al Anfal: 27)

Berbagai cara dilakukan untuk menjamin keamanan informasi tersebut. Salah satunya dengan menyandikan informasi menjadi suatu kode-kode yang tidak dimengerti, sehingga apabila disadap akan kesulitan untuk mengetahui informasi yang sebenarnya. Sistem pengkodean juga diterapkan pada saat turunnya wahyu dari Alloh SWT kepada orang yang dipilih-Nya secara khusus, agar tidak diketahui oleh orang lain, karena wahyu bersifat rahasia. Seperti sabda nabi Muhammad SAW yang diriwayatkan oleh imam Bukhori:

> "Diberitahukan bahwa al Haris bin Hisyam suatu ketika bertanya kepada nabi: "Ya Rosulullah, bagaimanakah wahyu datang kepadamu?" lalu nabi menjawab: "Kadang-kadang ia datang kepadaku seperti gemerincing lonceng, dan hal itu yang paling berat kurasakan. Setelah suara itu lenyap aku mengetahui apa yang kudengar. Namun ada kalanya juga tampak bagiku malaikat berupa seorang lelaki. Ia berbicara kepadaku dan aku mengerti apa yang dikatakannya". (H. R. Bukhori)

Ichwan (2001: 18) menyatakan bahwa “wahyu hanya dapat diterima oleh nabi karena wahyu adalah sesuatu yang rahasia.” Jadi, bunyi gemerincing lonceng dan bahasa yang hanya dapat dipahami oleh nabi itu apakah sebuah kode rahasia.

Metode penyandian yang pertama kali dibuat masih menggunakan metode algoritma rahasia. Metode ini menumpukan pada kerahasiaan algoritma yang digunakan. Namun metode ini tidak efisien saat harus digunakan untuk berkomunikasi dengan banyak orang. Oleh karena itu, seseorang harus membuat algoritma baru apabila akan bertukar informasi rahasia dengan orang lain. Karena penggunanya merasa tidak efisien maka algoritma rahasia mulai ditinggalkan dan dikenalkan suatu metode baru yang disebut dengan algoritma kunci. Metode ini tidak menumpukan keamanannya pada algoritmanya, tetapi pada kerahasiaan kunci yang digunakan pada proses peyandiannya. Algoritmanya dapat diketahui

dan dipelajari oleh siapapun. Metode algoritma kunci mempunyai tingkat efisiensi dan keamanan yang lebih baik dibandingkan dengan algoritma rahasia. Algoritma kunci yang dikenal dengan kriptografi telah melingkupi aspek kehidupan manusia saat ini. Mulai dari transaksi di mesin ATM, transaksi di bank, percakapan melalui telepon genggam, mengakses internet, sampai mengaktifkan peluru kendali. Begitu pentingnya kriptografi, saat berbicara tentang keamanan komputer orang tidak bisa memisahkannya dengan kriptografi (Munir. 2006: 1).

Kriptografi ElGamal merupakan salah satu algoritma kunci publik yang didasarkan pada logaritma diskrit. Kriptografi ElGamal dikembangkan pertama kali oleh ilmuan Mesir Taher ElGamal pada tahun 1984 M. Kriptografi ElGamal merupakan algoritma kriptografi kunci publik. Algoritma kunci publik menggunakan kunci yang berbeda untuk proses transformasinya. Untuk proses enkripsinya menggunakan kunci publik dan untuk proses deskripsinya menggunakan kunci privat. Sampai saat ini kriptografi ElGamal masih dipercaya sebagai metode penyandian, seperti aplikasi PGP *(Pretty Good privacy)* dan GnuPG yang dapat digunakan untuk mengamankan *e-mail* dan tanda tangan digital *(digital signature)* (Munir. 2004: 9)

Kriptografi ElGamal menjadi salah satu kriptografi yang sangat diminati dalam mengamankan pesan dan banyak dibahas pada buku-buku kriptogrfi tapi masih sangat jarang yang menjelaskan secara jelas tentang konsep-konsep matematis yang melandasinya. Berangkat dari hal tersebut, maka penulis mengkaji lebih dalam tentang kriptografi ElGamal dan memberi judul skripsi ini dengan ***"Konsep Matematis dan Proses Penyandian Kriptografi ElGamal"***.

1.2. Rumusan Masalah

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

1. Bagaimana konsep-konsep matematis dapat melandasi pembentukan kriptografi ElGamal?
2. Bagaimana proses penyandian kriptografi ElGamal?
3. Apakah kelebihan dan kelemahan kriptografi ElGamal?

1.3. Tujuan

Berdasarkan rumusan masalah di atas, tujuan penulisan skripsi ini adalah:

1. Dapat mengetahui konsep-konsep matematis yang melandasi pembentukan kriptografi ElGamal.
2. Dapat mengetahui proses penyandian kriptografi ElGamal.
3. Dapat mengetahui kelebihan dan kelemahan kriptografi ElGamal.

1.4. Batasan Masalah

Untuk memfokuskan pembahasan tentang kriptografi ElGamal maka pada skripsi ini terbatas pada konsep matematis dan proses penyandiannya serta kelebihan dan kekurangannya. Skripsi ini tidak membahas cara-cara untuk memecahkan penyandiannya, karena kriptografi ElGamal diciptakan untuk mengamankan data bukan memecahkan algoritmanya. Skripsi ini juga tidak membahas tentang penyelesaian logaritma diskrit walaupun logaritma diskrit mendasari terbentuknya kriptografi ElGamal.

1.5. Manfaat Penelitian

Penulisan skripsi ini diharapkan bermanfaat:

1. Bagi penulis : menambah wawasan penulis untuk mengetahui tentang kriptografi ElGamal baik konsep-konsep matematika yang melandasinya maupun proses-proses yang harus dilakukan dalam penyandiannya.
2. Bagi lembaga :
    1) Sebagai tambahan informasi pembelajaran mata kuliah yang berhubungan dengan kriptografi terutama kriptografi ElGamal.
    2) Sebagai tambahan bahan kepustakaan.
3. Bagi mahasiswa : menambah pengetahuan keilmuan mengenai kriptografi terutama kriptografi ElGamal.

1.6. Metode Penelitian

Metode yang digunakan dalam penulisan skripsi ini adalah studi literatur, dengan memakai literatur-literatur yang ada. Studi literatur berisi suatu topik yang di dalamnya memuat beberapa gagasan yang berkaitan dan harus didukung oleh data yang diperoleh dari berbagai sumber kepustakaan. Studi literatur adalah penelitian yang diadakan dari bermacam-macam material yang berada di ruang perpustakaan seperti, buku, majalah, dokumen, catatan, kisah-kisah sejarah, dan sebagainya (Mardalis, 1989: 28).

Buku utama yang digunakan sebagai literatur adalah *Kriptografi,* karangan Renaldi Munir. Karena dalam buku tersebut memaparkan teori dan definisi tentang kriptografi dan langkah-langkah matematis untuk menyelesaikan masalah

kriptografi. Literatur pendamping adalah beberapa buku dan jurnal yang membahas tentang kriptografi dan teori-teori matematika yang mendasari kriptografi ElGamal.

1.7. Sistematika Penulisan

Penulisan skripsi ini berdiri dari 4 bab yang merupakan rangkaian antara satu bab dengan bab yang lainnya. Materi tersebut disusun secara sistematis sebagai berikut:

Bab I: Pendahuluan

Bab ini berisi tentang latar belakang, rumusan masalah, tujuan pembahasan, batasan masalah, manfaat penelitian, metode penulisan, dan sistematika pembahasan.

Bab II: Kajian Teori

Bab ini berisi tentang kajian teori, berbagai definisi dan teorema yang mendukung pembahasan skripsi ini.

Bab III: Pembahasan

Bab ini berisi tentang kajian pembahasan.

Bab IV: Penutup

Bab ini berisi tentang kesimpulan penelitian dan saran.

BAB II

KAJIAN TEORI

Kriptografi saat ini berkembang dengan pesat, bukan hanya sebagai sebuah seni tapi juga menjadi ilmu. Memahami kriptografi dan menganalisisnya memerlukan ilmu matematika, karena kriptografi menggunakan matematika sebagai landasan perhitungannya. Bab 2 ini merupakan bahasan tentang konsep dasar yang berhubungan dengan kriptografi seperti definisi kriptografi, sejarah kriptografi, algoritma kriptografi, sistem kriptografi serta jenis-jenis kriptografi. Selain itu juga membahas teori-teori matematika yang berguna untuk memahami kriptografi terutama teori bilangan.

2.1. Kriptografi

2.1.1. Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani, *cryptography* terdiri dari kata *kryptos* yang berarti tersembunyi dan *graphein* yang berarti menulis atau tulisan. Menurut terminologi, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Ariyus, 2006: 9). Kriptografi juga dapat disebut dengan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Sebuah pesan rahasia harus terjaga keamanannya, salah satu cara dengan penyandian

pesan yang bertujuan meyakinkan privasi dengan menyembunyikan informasi dari orang-orang yang tidak ditujukan informasi tersebut kepadanya (Munir, 2006 : 3).

Al-Qu'an, wahyu yang di terima oleh Rasulullah juga melalui sebuah proses penyandian. Isyarat-isyarat khusus yang hanya difahami Rasulullah itulah yang menandakan bahwa Allah SWT mengkodekan wahyu tersebut dan hanya manusia pilihannya yang dapat mengerti maksudnya. Ichwan (2001: 25) mengatakan bahwa:

> "Wahyu adalah komunikasi transindental antara Tuhan dan manusia yang dipilihnya tanpa diketahui orang lain dan pada dasarnya wahyu adalah komunikasi linguistik yang terjadi dalam situasi konkrit antara dua orang namun salah satunya berperan aktif dan yang lain berperan pasif. Seperti dalam hal komunikasi pembicara (A) dan yang diajak bicara (B) harus menggunakan sistem isyarat yang bisa dimengerti oleh kedua belah pihak. Namun dalam penurunan wahyu yang merupakan hubungan Tuhan dan manusia sangat berbeda satu sama lain dilihat dari susunan keberadaannya. Tuhan dan manusia bersifat vertikal, maka harus terjadi sesuatu yang luar biasa baik agar komunikasi tersebut dapat berlangsung. Secara sederhana dapat kita katakana wahyu adalah hubungan verbal tiga pihak. Tuhan, malaikat, dan nabi. Tuhan mewahyukan kehendaknya melalui utusan langit kepada Muhammad SAW dan Muhammad SAW harus menyampaikan wahyu tersebut untuk orang-orang selain dirinya".

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptoanalisis. Kriptoanalisis *(cryptoanalysis)*, yaitu suatu ilmu dan seni yang dipelajari untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yang digunakan atau aksi untuk memecahkan mekanisme kriptografi dengan cara mendapatkan plainteks atau kunci dari cipherteks yang digunakan untuk mendapatkan informasi berharga kemudian mengubah atau memalsukan pesan dengan tujuan untuk menipu penerima yang sesungguhnya, memecahkan cipherteks (Flourensia, 2005: 4). Secara sederhana adalah seseorang yang ingin menembus kerahasiaan dari sebuah kode dengan cara membangun

algoritma baru yang bisa memecahkan algoritma yang sudah ada, pelakunya disebut kriptonalis. Munir (2006:8) mengatakan :

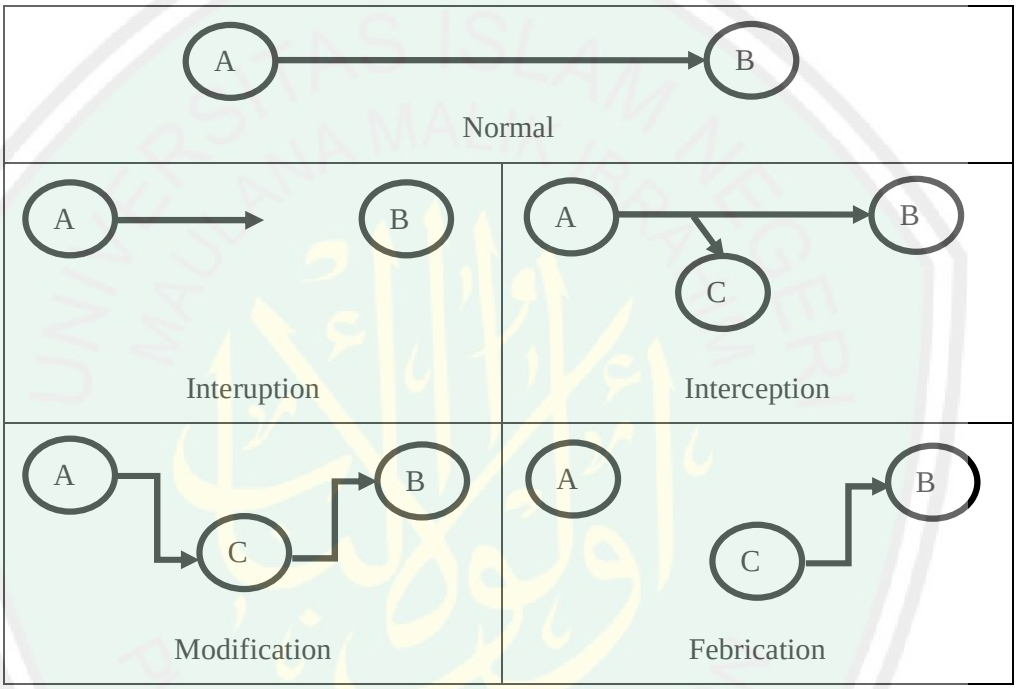
> ”Jika seorang kriptografer mentransformasi plainteks dan chiperteks dengan suatu algoritma dan kunci maka sebaliknya seorang kriptonalis berusaha memecahkan chiperteks untuk menemukan plainteks atau kunci”.

Setiap detiknya dalam dunia internet terjadi banyak sekali pertukaran informasi, Dan banyak pula pencurian informasi oleh pihak-pihak yang tidak bertanggung jawab. Ada beberapa ancaman keamanan yang terjadi terhadap informasi di antaranya:

1. *Interuption,* adalah ancaman terhadap *avaibability* informasi, yaitu data yang ada dalam komputer dirusak atau dihapus sehingga saat informasi tersebut dibutuhkan tidak ada lagi.
2. *Interception,* adalah ancaman terhadap kerahasianan. Informasi yang ada disadap oleh orang yang tidak berhak mendapat akses ke komputer dimana informasi tersebut disimpan.
3. *Modification,* adalah ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan dirubah sesuai keinginan orang tersebut.
4. *Fabrication,* adalah ancaman terhadap integritas. Orang yang tidak berhak berhasil menirukan atau memalsukan suatu informasi yang ada sehingga si penerima informasi mengira telah mendapatkan informasi dari pengirim yang sebenarnya.

Jadi, dari sini dapat di ketahui kriptografi diciptakan dengan tujuan, kerahasiaan, yaitu menjamin bahwa pesan dalam keadaan aman dari pihak yang

tidak berhak, integritas data, yaitu menjamin bahwa pesan masih asli atau tidak dimanipulasi, autentikasi, yaitu megidentifikasi pesan dan pengirim pesan, dan non-repudiation, yaitu mencegah penyangkalan pihak yang berkomunikasi (menolak penyangkalan) (Ariyus, 2006: 7). Secara sederhana ancaman-ancaman keamanan pesan tersebut dapat kita gambarkan sebagai berikut:



Gambar 2.1. Macam-Macam Ancaman Keamanan Pesan

Keterangan: A = pengirim pesan
B = penerima pesan
C = Penyadap pesan
⟶ = Proses perjalanan pesan

2.1.2. Sejarah Kriptografi

Kriptografi memiliki sejarah yang panjang dan mengagumkan. Penulisan rahasia ini dapat dilacak kembali ke 3000 tahun SM saat digunakan oleh bangsa

Mesir. Mereka menggunakan *hieroglyphcs* untuk menyembunyikan tulisan dari orang yang tidak diharapkan. *Hieroglyphcs* diturunkan dari bahasa Yunani, *hieroglyphica* yang berarti ukiran rahasia. Pada tahun 400 SM tentara Sparta di Yunani, menggunakan alat dari daun papyrus yang dililitkan pada sebatang kayu atau silinder berdiameter tertentu yang disebut *scytale* untuk mengirimkan pesan rahasia di medan perang. Sekitar tahun 50 SM, Julius Caesar, kaisar Romawi, menggunakan cipher substitusi, yaitu huruf-huruf alfabet disubstitusi dengan huruf-huruf yang lain pada alfabet yang sama. cipher substitusi digunakan untuk mengirim pesan pada jendral di medan perang agar tidak terbaca oleh musuh dan hanya dapat dibaca oleh jendralnya saja, yang mana sang jendral telah diberi tahu bagaimana cara membacanya. Tahun 1460, Leon Battista Alberti, di Italia mengembangkan disk cipher untuk enkripsi. Sistemnya terdiri dari dua disk konsentris. Setiap disk memiliki alfabet di sekelilingnya, dan dengan memutar satu disk berhubungan dengan yang lainnya, huruf pada satu alfabet dapat ditransformasi ke huruf pada alfabet yang lain. Bangsa arab yang mahir dalam ilmu matematika, statistik, dan linguistik juga mengembangkan kriptografi terbukti dengan ditemukannya buku karangan al Kindi yang ditulis pada abad 9H yang berjudul *"A Manuscript on Deciphering Cryptographic Messages"*. Pada 1790, Thomas Jefferson mengembangkan alat enkripsi dengan menggunakan tumpukan yang terdiri dari 26 disk yang dapat diputar secara individual. Pesan dirakit dengan memutar setiap disk ke huruf yang tepat dibawah batang berjajar yang menjalankan panjang tumpukan disk. Kemudian, batang berjajar diputar dengan sudut tertentu, kemudian dilihat bahwa huruf-huruf yang berada di bawah

batang adalah pesan yang terenkripsi. Penerima akan menjajarkan karakter-karakter cipher dibawah batang berjajar, memutar batang kembali dengan sudut A dan membaca pesan plainteks. Sejak saat itu sistem disk digunakan secara luas terutama pihak militer (Flourensia, 2005:5).

Pada tahun 1920, Boris Hagelin di Scockholm, Swedia. membuat mesin *Hagelin* dikenal sebagai M-209. Dilanjutkan Herbert O. Yardley, yang membuat alat bernama *Black Chamber*, yang digunakan untuk menyadap informasi jepang. Pada tahun 1919, Hugo Koch dari belanda mengembangkan Enigma atau otor mekanis untuk pengkodean dan pendekodean selama perang dunia II. Pengembangan paling mengejutkan dalam sejarah kriptografi terjadi pada tahun 1976 saat Diffie dan Hellman mempublikasikan *New Directions in Cryptography*. Tulisan ini memperkenalkan konsep revolusioner kriptografi kunci publik dan juga memberikan metode baru dan jenius untuk pertukaran kunci, keamanan yang berdasar pada kekuatan masalah logaritma diskrit. Ide dasar dari sistem kriptografi kunci publik adalah bahwa kunci kriptografi dibuat sepasang, satu kunci untuk enkripsi dan satu kunci untuk dekripsi. Pada tahun 1978 Rivest, Shamir dan Adleman menemukan rancangan enkripsi kunci publik dan tanda tangan, yang sekarang disebut RSA. Tahun delapan puluhan menunjukkan peningkatan luas di area ini, sistem RSA masih aman. Kelas lain yang merupakan rancangan kunci publik praktis ditemukan oleh ElGamal pada 1985. Rancangan ini juga berdasar pada masalah logaritma diskret. Pada tahun 1994 pemerintah US mengadopsi *Digital Signature Standard,* sebuah mekanisme yang berdasar pada rancangan kunci publik ElGamal (Flourensia, 2005: 6).

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 (Ariyus. 2006: 10).

2.1.3. Algoritma Kriptografi

Algoritma adalah urutan langkah-langkah logis untuk penyelesaian masalah yang disusun secara sistematis, jadi algoritma kriptografi atau sering disebut dengan *cipher* merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu:

1. Enkripsi, merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirim agar terjaga kerahasiaannya. Pesan asli disebut plainteks yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan sebagai chiper atau kode.
2. Deskripsi, merupakan kebalikan dari enkripsi. Pesan yang telah di enkripsi dikembalikan ke bentuk aslinya. Algoritma yang digunakan berbeda dengan algoritma yang digunakan untuk enkripsi.

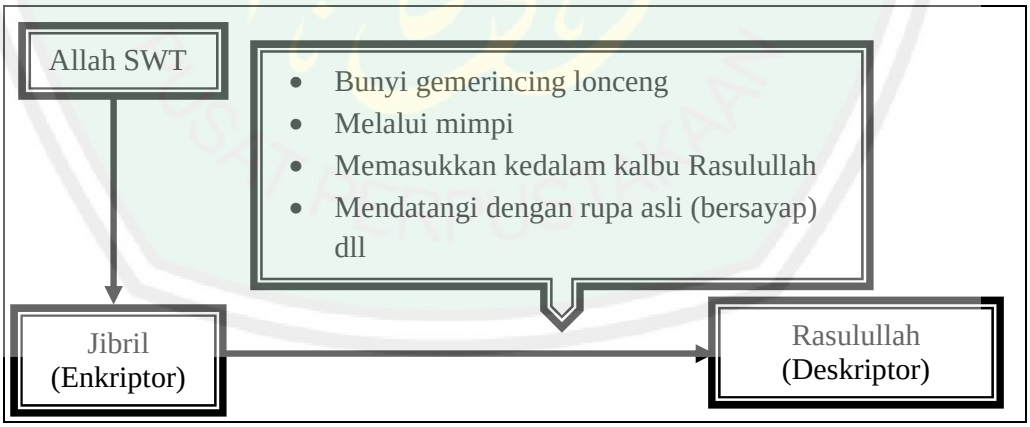
3. Kunci, merupakan kunci yang digunakan untuk proses enkripsi dan deskripsi. Kunci terbagi menjadi dua bagian yaitu kunci rahasia *(private key)* dan kunci umum *(public key)* (Ariyus, 2008: 43).

Proses enkripsi dan deskripsi dalam penurunan Al-Qu'an juga terjadi dengan begitu sempurna. Enkripsi dilakukan oleh Jibril dan Rosulullah SAW melakukan proses deskripsinya. Pencipta algoritma pada proses penurunan wahyu adalah yang maha memiliki ilmu. Walaupun Al-Qu'an telah mengalami proses penyandian yang benar-benar sulit dan tidak masuk akal seperti bunyi gemerincing lonceng namun keautentikannya benar-benar terjaga karena Allah SWT sendiri yang menjaminnya. Seperti firman Allah SWT :

إِنَّا نَحْنُ نَزَّلْنَا ٱلذِّكْرَ وَإِنَّا لَهُۥ لَحَٰفِظُونَ ﴿٩﴾

Sesungguhnya Kami-lah yang menurunkan Al Quran, dan Sesungguhnya kami benar-benar memeliharanya. (Qs. Al-Hijr (15): 9)

Untuk lebih jeasnya, kita lihat skema berikut ini:



Gambar 2.2. Proses Turunnya Wahyu Allah SWT

Al-Qur'an tidak perlu diragukan lagi keasliannya karena yang menjamin adalah Allah SWT. Melalui perantara yang benar-benar terjamin kesuciannya dan dipercayakan kepada orang yang benar-benar terjamin kejujurannya. Seperti firman Allah SWT, yang berbunyi:

وَمَا يَنطِقُ عَنِ ٱلۡهَوَىٰٓ ۝٣ إِنۡ هُوَ إِلَّا وَحۡيٞ يُوحَىٰ ۝٤ عَلَّمَهُۥ شَدِيدُ ٱلۡقُوَىٰ ۝٥ ذُو مِرَّةٖ فَٱسۡتَوَىٰ ۝٦ وَهُوَ بِٱلۡأُفُقِ ٱلۡأَعۡلَىٰ ۝٧ ثُمَّ دَنَا فَتَدَلَّىٰ ۝٨ فَكَانَ قَابَ قَوۡسَيۡنِ أَوۡ أَدۡنَىٰ ۝٩ فَأَوۡحَىٰٓ إِلَىٰ عَبۡدِهِۦ مَآ أَوۡحَىٰ ۝١٠ مَا كَذَبَ ٱلۡفُؤَادُ مَا رَأَىٰٓ ۝١١

Dan tiadalah yang diucapkannya itu (Al-Quran) menurut kemauan hawa nafsunya. Ucapannya itu tiada lain hanyalah wahyu yang diwahyukan (kepadanya). Yang diajarkan kepadanya oleh (Jibril) yang sangat kuat. Yang mempunyai akal yang cerdas; dan (Jibril itu) menampakkan diri dengan rupa yang asli. Sedang dia berada di ufuk yang Tinggi. Kemudian dia mendekat, lalu bertambah dekat lagi. Maka jadilah dia dekat (pada Muhammad sejarak) dua ujung busur panah atau lebih dekat (lagi). Lalu dia menyampaikan kepada hambaNya (Muhammad) apa yang Telah Allah wahyukan. Hatinya tidak mendustakan apa yang Telah dilihatnya. (Qs. An-Najm (53): 3-11)

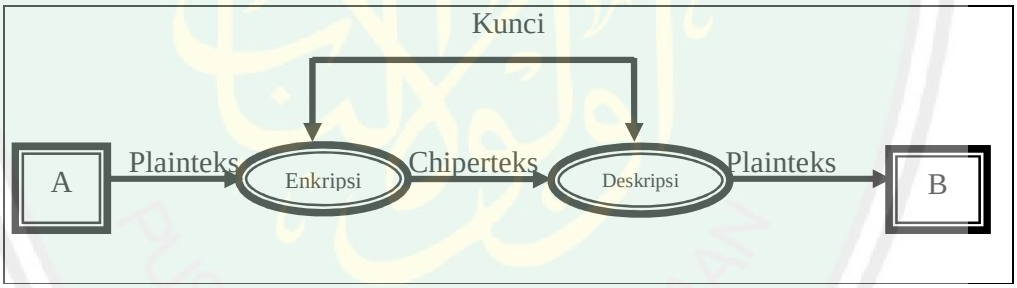
> Ariyus (2006:14) mengatakan bahwa: "Keamanan dari algoritma kriptografi klasik tergantung bagaimana suatu algoritma itu bekerja, maka algoritma seperti ini disebut algoritma terbatas. Algoritma terbatas merupakan suatu algoritma yang dipakai sekelompok orang untuk merahasiakan pesan yang dikirimnya. Jika salah satu anggota kelompok tersebut keluar dari kelompok maka algoritma yang dipakai diganti dengan yang baru. Keamanan dari kriptografi modern hanya dengan merahasiakan kunci, jadi fungsi kunci sama seperti *password*. Orang lain boleh mempelajari algoritmanya dan dapat dipublikasikan. Jika algoritmanya dapat dipecahkan dengan mudah maka algoritmanya belum aman untuk digunakan".

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan dari kunci yang dipakainya:

2.1.3.1. Algoritma Simetri

Algoritma ini juga disebut sebagai algoritma klasik karena memakai kunci yang sama untuk proses enkripsi dan deskripsinya. Keamanan algoritma ini terletak pada kuncinya. Jika kunci telah diketahui oleh orang lain maka informasi

akan terbongkar. Sifat kunci yang seperti ini membuat pengirim harus selalu memastikan bahwa jalur yang digunakan dalam pendistribusian kunci adalah jalur yang aman atau memastikan bahwa seseorang yang ditunjuk membawa kunci untuk dipertukarkan adalah orang yang dapat dipercaya. Masalahnya akan rumit jika sebanyak *n* pengguna dan setiap dua orang harus bertukar kunci yang berbeda. Maka akan terjadi sebanyak $C_2^n = \frac{n!}{(n-2)!2!} = \frac{n(n-1)}{2}$ jumlah kunci agar semuanya aman. Contoh algoritma simetri adalah: subtitusi, transposisi atau permutasi, *Data encryption standard* (DES), *Advanced encryption standard* (AES), *One Time Pad* (OTP), dan sebagainya (Ariyus, 2006: 14). Secara sederhana proses pengiriman pesan dengan algoritma simetris dapat kita gambarkan sebagai berikut:



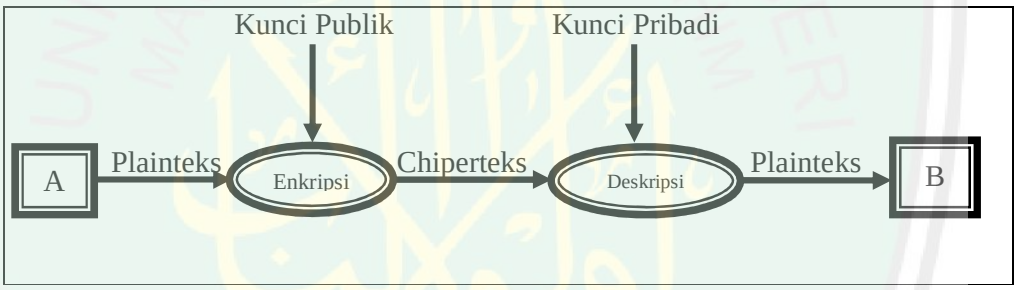
Gambar 2.3. Skema Algoritma Simetri

Keterangan: A = pengirim pesan
B = penerima pesan
⟶ = Proses perjalanan pesan

2.1.3.2 Algoritma Asimetri

Algoritma Asimetri sering disebut algoritma kunci, kerana kunci yang digunakan untuk enkripsi dan deskripsinya berbeda. Pada algoritma kriptografi kunci terbagi menjadi dua bagian, yaitu kunci publik dan kunci pribadi. Kunci

publik adalah kunci yang semua orang boleh mengetahui sedangkan kunci pribadi adalah kunci yang dirahasiakan, hanya boleh diketahui oleh satu orang. Kunci-kunci tersebut saling berhubungan satu dengan yang lainnya. Dengan kunci publik orang dapat mengenkripsi pesan sedangkan untuk mendeskripsi pesan hanya orang yang mempunyai kunci pribadi yang dapat melakukannya. Contoh dari algoritma asimetri adalah *Digital Signature algorithm* (DSA), *Elliptic Curve Cryptografi* (ECC), Diffie-Hellman (DH), ElGamal, dan lain sebagainya (Ariyus, 2006:15). Secara sederhana proses pengiriman pesan dengan algoritma simetris dapat kita gambarkan sebagai berikut:



Gamabar 2.4. Skema Algoritma Asimetri

Keterangan: A = pengirim pesan
B = penerima pesan
⟶ = Proses perjalanan pesan

2.1.3.3. Fungsi Hash

Fungsi Hash atau fungsi Hash satu arah yaitu suatu fungsi matematika yang mengambil input panjang variabel dan mengubahnya dengan urutan biner dengan panjang yang tetap. Fungsi Hash biasanya digunakan untuk membuat sidik jari dari suatu pesan. Sidik jari pada pesan adalah suatu tanda yang merupakan tanda bahwa pesan tersebut benar-benar dari orang yang diinginkan (Ariyus, 2006: 16). Pesan yang sudah diubah menjadi sebuah hasil dari fungsi

Hash tidak bisa diubah menjadi bentuk semula. Dua pesan yang berbeda akan menghasilkan nilai Hash yang berbeda. Kunci dari fungsi Hash tidak dirahasiakan, keamanannya terletak pada satu arahnya tersebut (Munir, 2006: 218).

2.1.4. Sistem Kriptografi

Definisi 2.1.4.1.

Sistem kriptografi adalah suatu 5-*tuple* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ yang memenuhi kondisi sebagai berikut:

1. $\mathcal{P}$ adalah himpunan plainteks
2. $\mathcal{C}$ adalah himpunan chiperteks
3. $\mathcal{K}$ adalah himpunan kunci atau ruang kunci *(Keyspace)*
4. $\mathcal{E}$ adalah himpunan fungsi enkripsi $e_k: \mathcal{P} \rightarrow \mathcal{C}$
5. $\mathcal{D}$ adalah himpunan fungsi deskripsi $d_k: \mathcal{C} \rightarrow \mathcal{P}$
6. Untuk $k \in \mathcal{K}$ terdapat $\mathcal{E}_k \in \mathcal{E}$ dan $d_k \in \mathcal{D}$ setiap $e_k: \mathcal{P} \rightarrow \mathcal{C}$ dan $d_k: \mathcal{C} \rightarrow \mathcal{P}$ merupakan fungsi sehingga $d_k(e_k(x)) = x$ untuk setiap plainteks x $\in \mathcal{P}$

Stinson,1995: 48

Suatu sistem kriptografi terdiri dari suatu algoritma, seluruh kemungkinan plainteks, cipherteks dan kunci-kuncinya. Sistem kriptografi merupakan suatu fasilitas untuk mengkonversikan plainteks menjadi cipherteks, dan sebaliknya.

2.2 Teori Bilangan

Bilangan adalah dasar sebuah perhitungan, untuk memahami dan membuat sesuatu kita harus melakukan perhitungan yang matang. Dengan memahami perhitungan secara menyeluruh, kita akan dapat memahami segala sesuatu yang ada disekitar kita. Hal ini telah diajarkan oleh Allah SWT seperti firmannya:

لِّيَعْلَمَ أَن قَدْ أَبْلَغُوا۟ رِسَٰلَٰتِ رَبِّهِمْ وَأَحَاطَ بِمَا لَدَيْهِمْ وَأَحْصَىٰ كُلَّ شَىْءٍ عَدَدًا ﴿٢٨﴾

Supaya dia mengetahui, bahwa Sesungguhnya rasul-rasul itu Telah menyampaikan risalah-risalah Tuhannya, sedang (sebenarnya) ilmu-Nya meliputi apa yang ada pada mereka, dan dia menghitung segala sesuatu satu persatu. (Qs. Al Jin (72) : 28)

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

2.2.1. Bilangan Bulat

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

bulat berperan sangat penting dalam kriptografi karena banyak algoritma kriptografi yang menggunakan sifat-sifat himpunan bilangan bulat dalam melakukan proses penyandiannya.

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).

2.2.1.1. Keterbagian

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

Definisi 2.2.1.1.1.

Misalnya $a, b \in \mathbb{Z}$, dengan $a \neq 0$. a dikatakan membagi b, ditulis $a|b$, jika dan hanya jika $b = a\,x$, untuk suatu $x \in \mathbb{Z}$.

Abdussakir, 2009: 114

Ada beberapa hal yang dapat diambil dari definisi keterbagian diatas 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 2.2.1.1.1.

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 $b = a \cdot y$. Akibatnya, untuk setiap $x \in \mathbb{Z}$ diperoleh $bx = (ay)x = a(yx)$. Karena pada bilangan bulat berlaku sifat tertutup pada perkalian maka terdapat $p = yx$. 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 $c = by = (ax)y = a(xy)$, 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 $b = ax = (by)x = b(yx)$ 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 $a|b$.

2.2.1.2. Algoritma Pembagian

Definisi 2.2.1.2.1.

Jika $a, b \in \mathbb{Z}$ dan $a > 0$, maka asa bilangan-bilangan $q, r \in \mathbb{Z}$ yang masing-masing tunggal sehingga $b = q \cdot a + r$ dengan $0 \leq r \leq a$. Jika $a \nmid b$, maka r memenuhi ketidaksamaan $0 < r < a$.

Muhsetyo, 1997: 50

Teorema 2.2.1.2.1.

Misalkan a dan b adalah bilangan bulat dengan $a > 0$. Maka terdapat bilangan bulat q dan r yang masing-masing tunggal sehingga $b = aq + r$, $0 \leq r < a$

Abdussakir, 2009: 117

Bukti:

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

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

Selanjutnya ambil himpunan P yang anggotanya anggota himpunan S yang tidak negatif, yaitu:

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

Maka $P \neq \phi$, sebab:

a) Jika $b \geq 0$ dan $q = 0$, maka $b - qa = b - 0a = b \in P$.

b) Jika $b < 0$ dan $q = b$, maka $b - aq = b - ba = b(1 - a)$

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 $a|(r_1 - r_2)$ atau $(r_1 - r_2)$ adalah kelipatan dari a.

Disisi lain karena $0 \leq r_1 < a$ dan $0 \leq r_2 < a$.

Maka $$-a \leq (r_2 - r_1) < a$$

Satu-satunya kelipatan a yang terdapat diantara $-a$ 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 tunggal.

Jadi, $b = aq + r,\ 0 \leq r < a$

Dalam teorema di atas, yaitu $b = aq + r,\ 0 \leq r < a$. b disebut bilangan yang dibagi *(dividend)*, a disebut pembagi *(devisor)*, 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 $b = aq + r$ dan $r = 0$

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

Algoritma pembagian sebenarnya lebih bersifat dalil eksistensi keujudan dari adanya bilangan-bilangan bulat q dan r dari pada suatu algoritma. Namun, uraian tentang pembuktiannya dapat memberikan adanya suatu metode atau cara matematis untuk memperoleh bilangan bulat q dan r sehingga $b = aq + r$.

Misalkan $a = 2$ dan b sebarang bilangan bulat positif, maka menurut teorema 2.2.1.2.1. dapat dinyatakan dengan $b = 2 \cdot q + r$, $0 \leq r < 2$. Ini berarti nilai-nilai b yang mungkin dapat ditentukan oleh nilai-nilai r yang mungkin, yaitu $r = 0$ atau $r = 1$.

Untuk $r = 0$, $b = 2 \cdot q + r = 2 \cdot q$ $b = 2 \cdot q$

Dengan $q \in \mathbb{Z}$ dan selanjutnya disebut bilangan bulat genap

Untuk $r = 1$, $b = 2 \cdot q + r = 2 \cdot q + 1$, $b = 2 \cdot q + 1$

Dengan $q \in \mathbb{Z}$ dan selanjutnya disebut bilangan bulat ganjil.

Disinilah letak dari konsep algoritma pembagian,yaitu suatu algoritma yang dapat digunakan untuk membantu pembuktian sifat-sifat yang lebih lanjut. Algoritma pembagian juga digunakan untuk menyatakan bilangan-bilangan bulat dalam basis tertentu. Misalkan dalam lambang desimal kita biasanya menggunakan basis 10 dalam perpangkatan.

Teorema 2.2.1.2.2.

Jika $b \in \mathbb{Z}$ dan $b > I$, 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 $0 \leq a_i \leq b - I$ untuk $I = 0,1,2, \ldots, k$, dan $a_k \neq 0$

Muhsetyo, 1997: 54

Bukti:

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

$n = b \cdot q_0 + a_0, 0 \leq a_0 \leq b - I$

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

$q_0 = b \cdot q_1 + a_1, 0 \leq a_1 \leq b - I$

Jika langkah serupa dikerjakan, maka diperoleh:

$q_1 = b \cdot q_2 + a_2, 0 \leq a_2 \leq b - I$

$q_2 = b \cdot q_3 + a_3, 0 \leq a_3 \leq b - I$

… … … … … … … … … … … … … … … … … … …

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

$q_{k-1} = b \cdot q_k + a_k, 0 \leq a \leq b - I$

Langkah terakhir ditandai dengan munculnya $q_k = 0$

Karena barisan $q_0, q_1, \ldots, q_k$ adalah barisan bilangan bulat tidak negatif yang menurun, maka paling banyak ada q_0 suku yang positif, dan 1 suku q_k yang bernilai nol. Dari persamaan-persamaan di atas dapat ditentukan bahwa:

$n = b \cdot q_0 + a_0$

$n = b(bq_1 + a_1) + a_0 = b^2 q_1 + ba_1 + a_0$

$n = b^2(bq_2 + a_2) + ba_1 + a_0 = b^3 q_2 + b^2 a_2 + ba_1 + a_0$

… …

$n = b^{k-1} q_{k-2} + b^{k-2} a_{k-2} + b^{k-3} a_{k-3} + \cdots + ba_1 + a_0$

$n = b^k a_{k-1} + b^{k-1} a_{k-1} + b^{k-2} a_{k-2} + \cdots + ba_1 + a_0$

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

Karena $q_k = 0$, maka:

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

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

Contoh:

Tunjukkan dengan algortima pembagian untuk menuliskan 567 dengan basis 2 dan dengan basis 3

Jawab:

Untuk basis 2

$567 = 2 \cdot 283 + 1$
$283 = 2 \cdot 141 + 1$
$141 = 2 \cdot 70 + 1$
$70 = 2 \cdot 35 + 1$
$35 = 2 \cdot 17 + 1$
$17 = 2 \cdot 8 + 1$
$8 = 2 \cdot 4 + 0$
$4 = 2 \cdot 2 + 0$
$2 = 2 \cdot 1 + 0$
$1 = 2 \cdot 0 + 1$

$(567)_{10} = (1000110111)_2$

Untuk basis 3

$567 = 3 \cdot 189 + 0$
$189 = 3 \cdot 63 + 0$
$63 = 3 \cdot 21 + 0$
$21 = 3 \cdot 7 + 0$
$7 = 3 \cdot 2 + 1$
$2 = 3 \cdot 0 + 2$

$(567)_{10} = (210000)_3$

2.2.2. Faktor Persekutuan Terbesar (FPB)

Definisi 2.2.2.1.

Misalkan $a, b \in \mathbb{Z}$ yang tidak keduanya nol. Bilangan d disebut faktor persekutuan dari a dan b jika $d|a$ dan $d|b$. Faktor persekutuan terbesar (FPB) dari a dan b jika d adalah bilangan bulat positif terbesar sehingga $d|a$ dan $d|b$. Karena FPB dari a dan $b > 0$ maka FPB dari a dan $b \geq 1$.

Abdussakir, 2009: 120

Untuk selanjutnya, FPB dari a dan b dinotasikan dengan (a,b).

Berdasarkan definisi FPB di atas, $d = (a, b)$, jika:

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

Contoh:

Carilah faktor persekutuan terbesar dari bilangan berikut:

1) (12,8) = 4

2) (60,24) = 12

Teorema 2.2.2.1.

FPB dari bilangan bulat a dan b yang tidak keduanya nol selalu ada.

Abdussakir, 2009: 120

Bukti:

Misal S = $\{ax + by | ax + by > 0, \text{dengan } x, y \in \mathbb{Z}\}$

Maka $S \subseteq \mathbb{N}$

Ambil $x = a$ dan $y = b$, maka $ax + by = a^2 + b^2 > 0$.

Jadi, $S \neq \emptyset$

Sesuai sifat terurut yang baik, karena $S \subseteq N$, maka S mempunyai unsur terkecil. Misalkan d adalah unsur terkecil di S. Maka jelas bahwa $d > 0$.

Kerena $d \in S$, maka $d = ax_0 + by_0$, untuk suatu $x_0, y_0 \in \mathbb{Z}$.

Selanjutnya akan ditunjukkan bahwa $d|a$ dan $d|b$.

Misalkan $a = dq + r$, $0 \leq r < d$,

Maka $r = a - dq$

$= a - (ax_0 + by_0)q$

$= a - ax_0q - by_oq$

$= a(1 - x_0q) + b(-y_0q)$

Disimpulkan bahwa $r = 0$, sebab jika $r \neq 0$ berarti $r \in S$ dengan $r < d$.

Hal tersebut bertentangan dengan a sebagai unsur terkecil di S.

Akibatnya $a = dq$ dan $d|a$.

Dengan cara yang sama, diperoleh $d|b$.

Misalkan c adalah faktor persekutuan positif dari a dan b, maka $c|a$ dan $c|b$.

Karena $c|a$ dan $c|b$, maka $c|ax + by$, untuk setiap $x, y \in \mathbb{Z}$

Pilih $x = x_0$ dan $y = y_0$ maka $c|ax_0 + by_0$ atau $c|d$

Karena $d > 0$ dan $c > 0$, maka $c \leq d$

Dengan demikian maka berarti bahwa d adalah faktor persekutuan terbesar dari a dan b.

Jadi, d = (a,b).

Teorema 2.2.2.1. biasa disebuat dengan teorema eksistensi FPB. Tapi, selain menyatakan eksistensi FPB dua bilangan bulat tidak keduanya nol, juga menjelaskan bahwa faktor persekutuan terbesar dua bilangan bulat yang tidak keduanya nol adalah bilangan bulat positif terkecil dari kombinasi linier dua bilangan bulat tersebut. Jadi, jika $d = (a,b)$, maka d adalah bilangan bulat positif terkecil yang berbentuk $ax+by$, untuk suatu $x, y \in \mathbb{Z}$.

Teorema 2.2.2.2.

jika $c|ab$ dan $(a, b) = 1$, maka $c|d$

Abdussakir, 2009: 124

Bukti:

Karena $(a, c) = 1$, maka terdapat $m, n \in \mathbb{Z}$ sehingga $ma + nc = 1$

Dan berlaku pula bahwa $mab + ncb = b$

Diketahui $c|ab$, maka $c|mab$ karena $c|c$ maka $c|cnb$

Dengan demikian $c|(mab + ncb)$

Jadi, $c|b$.

Definisi 2.2.5.2.

Bilangan a dan b dikatakan prima relatif jika $(a, b) = 1$

Abdussakir, 2009: 124

Contoh:

1) $(13,5) = 1$ jadi, 13 dan 5 merupakan prima relatif
2) $(24,12) = 2$ jadi, 24 dan 12 bukan merupakan prima relatif

2.2.2.1. Algoritma Euclid

Algoritma ini digunakan untuk mencari nilai pembagi persekutuan terbesar (FPB) dari dua bilangan bulat. Karena dalam kriptografi ElGamal biasanya menggunkan bilangan bulat yang besar, maka penyelesaiannya harus dengan cara yang mudah dan cepat.

Teorema 2.2.2.1.

Misalkan a dan b adalah bilangan bulat dengan $a > 0$. Dengan melakukan pengulangan algoritma pembagian sampai diperoleh sisa pembagi sampai diperoleh sisa pembagi 0. Akan didapatkan urutan persamaan berikut.

$b = aq_1 + r_1, \qquad 0 \leq r_1 \leq a$
$a = r_1q_2 + r_2, \qquad 0 \leq r_2 \leq r_1$
$r_1 = r_2q_3 + r_3, \qquad 0 \leq r_3 \leq r_2$
... ...
$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n \leq r_{n-1}$
$r_{n-1} = r_nq_{n-1},$
Maka, $(a, b) = r_n$ dan r_n adalah sisa pembagian yang tidak nol.

Abdussakir, 2009: 125

Bukti:

Telah diketahui bahwa r_n adalah sisa pembagi terakhir yang tidak nol

Jadi $r_n > 0$

Untuk membuktikan $r_n = (a, b)$ harus ditunjukkan bahwa $r_n|a$ dan $r_n|b$, serta jika $k|a$ dan $k|b$ maka $k|r_n$

Berdasarkan penyataan terakhir, yaitu $r_{n-1} = r_n q_{n-1}$, maka diperoleh

$r_n|r_{n-1}$

Karena $r_{n-2} = r_{n-1}q_n + r_n$, maka diperoleh

$$\begin{aligned} r_{n-2} &= r_{n-1}q_n + r_n \\ &= (r_n q_{n+1})q_n + r_n \\ &= r_n(q_{n+1}q_n + 1) \\ &= r_n p_1, \text{ dengan } p_1 = q_{n+1}q_n + 1 \end{aligned}$$

Jadi, $r_n|r_{n-2}$

Karena $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$, maka diperoleh

$$\begin{aligned} r_{n-2} &= r_{n-2}q_{n-1} + r_{n-1} \\ &= (r_n p_1)q_{n-1} + r_n q_{n+1} \\ &= r_n(p_1 q_{n-1} + q_{n+1}) \\ &= r_n p_2, \text{ dengan } p_2 = p_1 q_{n-1} + q_{n+1} \end{aligned}$$

Jadi, $r_n|r_{n-3}$

Dengan melanjutkan proses ini akan didapatkan bahwa

$r_n|r_{n-4}, r_n|r_{n-5}, \dots, r_n|r_2, r_n|r_1, r_n|a$, dan $r_n|b$

Jadi, terbukti bahwa $r_n|a$ dan $r_n|b$

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

Maka $k|b - aq_1$

Karena $r_1 = b - aq_1$ maka $k|r_1$

Karena $k|r_1$ dan $k|a$ maka $k|a - r_1q_2$. Jadi $k|r_2$

Karena $k|r_1$ dan $k|r_2$ maka $k|r_1 - r_2q_3$. Jadi $k|r_3$

Dengan melanjutkan proses ini maka akan di dapatkan bahwa:

$k|r_3, k|r_4, \dots, k|r_{n-1}$, dan $k|r_n$

Terbukti bahwa $r_j = (a, b)$

Contoh:

Akan dihitung $FPB(1938, 570)$ menggunakan algoritma Euclid

Jawab:

$1936 = 3 \cdot 570 + 228 \qquad 0 \leq 228 \leq 570$

$570 = 2 \cdot 228 + 114 \qquad 0 \leq 114 \leq 228$

$228 = 2 \cdot 114$

Jadi, $FPB(1938, 570) = 114$

2.2.2.2. Fungsi Euler (ϕ)

Fungsi Euler digunakan untuk menyatakan banyaknya bilangan bulat $< n$ yang relatif prima dengan *n*

Definisi 2.2.3.1.

Ditentukan $m \in \mathbb{Z}^+$

Banyaknya residu di dalam suatu system reduksi tereduksi modulo m disebut fungsi euler (ϕ) di *m* dan dinyatakan dengan $\phi(m)$

Muhsetyo,1997: 184

Definisi 2.2.3.2.

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

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

2) $r_i \not\equiv r_j (\text{mod } m)$ untuk semua $i \neq j$

3) Jika $(x, m) = 1$ maka $x \equiv r_j (\text{mod } m)$

Muhsetyo, 1997: 279

2.2.3. Pemangkatan

Perhitungan pemangkatan yang terlalu besar akan menyulitkan jika dihitung dengan cara biasa. Ada beberapa metode yang dapat digunakan untuk menyelesaikan perhitungan pemangktan dengan lebih cepat dan lebih mudah, yaitu:

2.2.3.1. Algoritma Euclid Diperluas

Algoritma ini merupakan perluasan dari algoritma Euclid, digunakan untuk mencari invers terhadap operasi pergandaan. Algoritma ini didasarkan pada pernyataan berikut, diberikan bilangan bulat positif b dan a dengan $b \geq a$. Jika $FPB(b, a) = 1$, maka $a^{-1} (\text{mod } b)$ ada. Jika $FPB(b, a) \neq 1$ maka $a^{-1} (\text{mod } b)$. Kita gunakan rumus rekurensi berikut:

$t_0 = 0 \quad t_1 = 1$

$t_j = t_j - 2 - q_{j-1} \cdot t_{j-1}, \ j \geq 2$

Nilai q_1 diperoleh dari perhitungan $FPB(b, a)$ menggunakan algoritma Euclid. Jika $FPB(b, a) = 1$ berarti $a^{-1} = t_n$ sehingga $r_n = t_n \cdot r$ atau $1 = t_n \cdot r_n$

Contoh:

Akan dihintung $28^{-1} \text{mod } 75$

Jawab:

Diketahui $b = 75$ dan $a = 28$

hitung $FPB(75,28)$ Menggunakan algoritma Euclid:

$75 = 2 \cdot 28 + 19$ $n = 1$ $a_1 = 28$ $q_1 = 2$

$28 = 2 \cdot 19 + 9$ $n = 2$ $a_2 = 19$ $q_2 = 2$

$19 = 2 \cdot 9 + 1$ $n = 3$ $a_3 = 9$ $q_3 = 2$

$9 = 9 \cdot 1$ $n = 4$ $a_4 = 1$ $q_4 = 9$

Jadi, $FPB(75,28) = 1$ berarti $28^{-1} \bmod 75$ ada. Dari penyelesaian algoritma Euclid tersebut diperoleh $n = 4$. Selanjutnya, dengan menggunakan rumus rekurensi, diperoleh:

$t_2 = t_0 - q_1 \cdot t_1 = 0 - 2 \cdot 1 = (-2) = 73$

$t_3 = t_1 - q_2 \cdot t_2 = 0 - 1 \cdot (-2) = 3$

$t_4 = t_2 - q_3 \cdot t_3 = -2 - 2 \cdot 3 = (-8) = 67$

$r_4 = t_4 \cdot r_1 = 67 \cdot 28 = 1 \Leftrightarrow 67 = 28^{-1}$

Dari hasil terakhir di atas, diperoleh $28^{-1} \bmod 75 = 67$

Algoritma Euclid yang diperluas juga bisa digunakan untuk mencari nilai *x* dan *y* dari pernyataan $FPB(b, a) = x \cdot b + y \cdot a$

Contoh:

Cari nilai *x* dan *y* dari $FPB(1938, 570) = x \cdot 1938 + y \cdot 570$ dengan menggunakan algoritma Euclid diperluas.

Dari contoh algoritma Euclid kita dapatkan:

$114 = 570 - 2 \cdot 228$

$228 = 1983 - 3 \cdot 570$

Sehingga: $114 = 570 - 2 \cdot 228$

$= 570 - \{1938 - (3 \cdot 570)\}$

$= 7 \cdot 570 - 2 \cdot 1938$

Jadi, $a = 7$ dan $b = -2$

2.2.3.2. Metode *Fast exponentiation*

Metode *fast exponetiation* ini digunakan untuk menghitung operasi pemangkatan besar bilangan bulat modulo dengan cepat. Metode ini memanfaatkan ekspansi biner dari bilangan z, yaitu:

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

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

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

Jadi metode *fast exponenxiation* didasarkan pada pernyataan berikut ini:

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

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 $73 = (1001001)_2$

Selanjutnya hitung

$6^{2^0} = 6$

$6^{2^1} = 36$

$6^{2^2} = 36^2 = 96 (\text{mod } 100)$

$6^{2^3} = 16 (\text{mod } 100)$

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

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

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

Sehingga diperoleh:

$6^{73} = 6 \cdot 6^{2^3} \cdot 6^{2^4} (\text{mod } 100)$

$= 6 \cdot 16 \cdot 96 (\text{mod } 100)$

$= 16 (\text{mod } 100)$

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

2.2.4. Aritmetika Modulo dan Kekongruenan

Definisi 2.2.4.1.

Misalkan *a* adalah bilangan bulat dan *m* adalah bilangan bulat > 0. Operasi *a* mod *m*. bilangan *m* disebut modulus atau modulo. Dan hasil aritmatika modulo *m* terletak di dalam himpunan {0,1,2,…,*m*-1)

a mod *m* = *r* sedemikian sehingga $a = mq+r$, dengan $0 \leq r < m$.

Munir. 2006: 38

Aritmatika modulo cocok di gunakan pada kriptografi karena dua alasan:

1. Karena nilai-nilai aritmatika modulo berada pada himpunan berhingga (0 sampai modulo m – 1), maka hasilnya selalu di dalam himpunan.
2. Karena kita bekerja dengan bilangan bulat, maka tidak akan kehilangan informasi akibat pembulatan (*round off*) sebagaimana operasi bilangan riil.

Definisi 2.2.4.1.

Diketahui $a, b, m \in \mathbb{Z}$. A disebut kongruen dengan b modulo m, ditulis $a \equiv b(\text{mod } m)$, jika $(a - b)$habis dibagi m, yaitu $m|(a - b)$. Jika $(a - b)$ tidak habis dibagi m, yaitu $m \nmid (a - b)$, maka ditulis $a \not\equiv b(\text{mod } m)$, 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: $a \equiv b(\text{mod } m)$ jika dan hanya jika, $b \equiv a(\text{mod } m)$

Muhsetyo,1997: 138

Contoh:

1) $17 \equiv 2(\text{mod } 3)$ (3 habis membagi$17 - 2 = 15 \rightarrow 15 \div 3 = 5$)
2) $-7 \not\equiv 15(\text{mod } 3)$ (3 tidak habis membagi $-7 - 15 = -22$)

Teorema 2.2.4.1.

Misalkan m adalah bilangan bulat positif.

Jika $a \equiv b (\text{mod } m)$ dan c adalah sebarang bilangan bulat maka:

i. $(a + c) \equiv (b + c) (\text{mod } m)$

ii. $ac \equiv bc \ (\text{mod } m)$

Munir, 2006: 39

Bukti:

i. $a \equiv b (\text{mod } m)$ berarti:

$\Leftrightarrow a = b + km$

$\Leftrightarrow a - b = km$

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

$\Leftrightarrow (a + c) = (b + c) + Km$

$\Leftrightarrow (a + c) = (b + c) \ (\text{mod } m)$

ii. $a \equiv b (\text{mod } m)$ berarti:

$\Leftrightarrow a = b + km$

$\Leftrightarrow a - b = km$

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

$\Leftrightarrow ac = bc + Km$

$\Leftrightarrow ac = bc \ (\text{mod } m)$

2.2.5. Bilangan Prima

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 lebih mendalam. Banyak dalil dan sifat dikembangkan berdasarkan bilangan prima. Bilangan prima juga memainkan peranan yang penting pada beberapa algoritma kunci publik, seperti kriptografi ElGamal.

Definisi 2.2.5.1.

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.

Muhsetyo,1997: 92

Untuk menguji apakah p merupakan bilangan prima atau bilangan komposit, kita bisa menggunakan cara yang paling sederhana, yaitu cukup membagi p dengan sejumlah bilangan prima, yaitu $2, 3, \ldots,$ bilangan prima $\leq \sqrt{p}$. Jika p habis di bagi 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 2.2.5.1.

Jika p adalah suatu bilangan prima dan $p|ab$, maka $p|a$ atau $p|b$.

Muhsetyo,1997: 100

Bukti:

Anggaplah $p \nmid a$

Karea p adalah suatu bilangan prima dan $p|a$, maka p hanya mempunyai pembagi 1 dan p, sehingga (a,p) = 1.

Menurut teorema, jika $a|ab$ dan (a,p) = 1, maka $p|b$.

Dengan cara serupa, dan dianggap $p|b$, maka dapat dibuktikan bahwa $p|a$.

Teorema 2.2.5.2.

Setiap bilangan bulat $n > 1$ dapat dinyatakan sebagai perkalian bilangan-bilangan prima (dimungkinkan hanya mempunyai satu faktor)

Abdussakir, 2009: 131

Bukti:

Karena $n > 1$ maka ada dua kemungkinan, yaitu *n* bilangan prima atau *n* bilangan komposit.

Jika *n* bilangan prima maka *n* adalah faktor prima bagi dirinya sendiri

Jika *n* bilangan komposit maka dapat difaktorkan

Misalkan $n = n_1 n_2$. Jika n_1 dan n_2 adalah bilangan prima, berarti *n* merupakan perkalian bilangan-bilangan prima.

Jika n_1 bukan prima, n_1 difaktorkan, misalkan $n_1 = n_3 n_4$, maka dengan $1 < n_3 < n_4 < n_1$.

Jika n_2 juga bukan prima, maka n_2 juga difaktorkan dengan cara yang sama, misalkan $n_2 = n_5 n_6$ dengan $1 < n_5 < n_6 < n_2$

Jadi, $n = n_3 n_4 n_5 n_6$. Jika n_3, n_4, n_5, n_6 adalah bilangan-bilangan prima maka terbukti.

Jika tidak, maka kita lakukan proses yang sama sehingga faktor-faktornya makin kecil. Karena faktor-faktornya adalah bilangan bulat yang lebih dari 1, maka faktor-faktornya menjadi bilangan-bilangan bulat.

Jadi *n* dapat menuliskan sebagian perkalian bilangan-bilangan prima

Karena faktor-faktor prima tersebut tidak harus berbeda, maka hasilnya dapat dituliskan dalam bentuk

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \wedge p_n^{\alpha_n}$$

Dimana $p_1, p_2, p_3, \dots, p_n$adalah bilangan-bilangan prima yang berbeda dan $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$ adalah bilangan bulat positif.

Teorema 2.2.5.3.

Banyaknya bilangan prima adalah tak terhingga

Abdussakir, 2009: 134

Bukti:

Adaikan banyaknya bilangan prima adalah berhingga, yaitu $p_1, p_2, p_3, \dots, p_n$

Misalkan $p = (p_1, p_2, p_3, \dots, p_n) + 1$

Karena $p > 1$, maka P dapat dinyatakan sebagai perkalian bilangan-bilangan prima.

1) Jika p adalah prima maka p bukan salah satu dari p_i, $i = 1,2,3, \dots, n$. Jadi, ada bilangan prima lain selain $p_1, p_2, p_3, \dots, p_n$
2) Jika p komposit, maka p dapat dinyatakan sebagai perkalian bilangan-bilangan prima

Andaikan p_i adalah faktor dari p untuk suatu i, $i = 1,2,3, \dots, n$

Karena $p_i | (p_1, p_2, p_3, \dots, p_n)$ dan $p_i | (p_1, p_2, p_3, \dots, p_n) + 1$ maka diperoleh bahwa $p_i | 1$

Berarti $p_i = 1$. Hal ini tidak mungkin karena p_i adalah bilangan prima. Jika faktor prima dari p adalah selain $p_1, p_2, p_3, \dots, p_n$. Jadi, ada bilangan prima lain selain $p_1, p_2, p_3, \dots, p_n$

Jadi hal ini kontradiksi dengan pengandaian bahwa bilangan prima hanyalah $p_1, p_2, p_3, \dots, p_n$. Dengan demikian, maka terbukti bahwa banyaknya bilangan prima adalah tak terhingga.

Teorema 2.2.5.4. (Teorema Fermat)

Jika p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi dengan p, yaitu FPB(a,p) = 1, maka

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

untuk sebarang $a \in \mathbb{Z}_p$

Munir, 2006: 46

Bukti:

$a \in \mathbb{Z}_m$ dan m adalah bilangan bulat, berlaku $a^{\varphi m} \equiv 1 (\text{mod } m)$. Dari sini diambil $m = p$ sehingga diperoleh $a^{p-1} = a^{\varphi m} \equiv 1 (\text{mod } p)$

BAB III

PEMBAHASAN

Kriptografi kunci publik sangat ditentukan oleh kuncinya. Semakin sulit pemecahan algoritma kuncinya maka tingkat keamanannya semakin tinggi. Bab 3 ini adalah bahasan mengenai konsep-konsep matematis yang melandasi pembentukan kriptografi ElGamal, sehingga dapat memperkuat kuncinya. Juga proses penyandian dalam kriptografi ElGamal dan kelebihan serta kelemahan kriptografi ElGamal.

3.1. Konsep Matematis dalam Kriptografi ElGamal

Matematika menjadi dasar dalam banyak disiplin ilmu. Teori bilangan yang merupakan bagian ilmu matematika banyak mendasari disiplin ilmu mengenai komputer dan salah satunya adalah dalam bidang kriptografi terutama kriptografi ElGamal. Kriptografi ElGamal menggunakan bilangan prima sebagai salah satu kuncinya dan mendasarkan kekuatan keamanannya pada masalah logaritma diskrit. Jadi, bilangan prima dan logaritma diskrit adalah bagian dari konsep matematika yang melandasi kriptografi ElGamal.

3.1.1. Bilangan Prima

Bilangan prima memiliki peranan yang sangat penting pada kriptografi ElGamal. Bilangan prima digunakan sebagai salah satu kunci dalam kriptografi ElGamal. Jadi, sangat penting untuk mencari bilangan prima yang besar agar

keamanan kunci lebih besar pula. Untuk mencari bilangan prima yang besar kita dapat menguji keprimaan sebuah bilangan bulat menggunakan tes-tes keprimaan berikut:

3.1.1.1. Tes Keprimaan

3.1.1.1.1. Tes Lehmann

Tes yang paling sederhana adalah menggunakan algoritma Lehmann sebagai berikut:

Algoritma 3.1. (Algoritma Lehmann):

Input: p (yang akan diuji keprimaannya)

Output: p adalah bilangan prima atau bilangan komposit

Langkah:

1) Bangkitkan bilangan acak a yang lebih kecil dari p
2) Hitung $a^{(p-1)/2} \pmod p$
3) Jika $a^{(p-1)/2} \not\equiv 1$ atau $(-1) \pmod p$, maka p tidak prima
4) Jika $a^{(p-1)/2} \equiv 1$ atau $(-1) \pmod p$, maka peluang p bukan prima adalah lima puluh persen

Pengujian menggunakan algoritma Lehmann dianjurkan diulangi sebanyak lima kali dengan nilai a yang berbeda. Jika hasil perhitungan langkah ke-dua sama dengan 1 atau (-1), maka peluang p adalah prima mempunyai kesalahan tidak lebih dari lima puluh persen. Bilangan acak yang digunakan pada algoritma Lehmann dapat dipilih nilai yang kecil agar perhitungan lebih cepat. Algoritma Lehmann menentukan keprimaan suatu bilangan dengan cara yang sangat sederhana dan masih sangat diragukan kevalidannya

3.1.1.1.2. Tes Fermat

Tes fermat adalah tes yang umum dilakukan untuk mencari keprimaan sebuah bilangan. Kita buat algoritma dari teorema 2.2.2.1. dan sedikit kita rubah, yaitu:

Algoritma 3.2. (Algoritma Fermat):

Input: p (yang akan diuji keprimaannya)

Output: p adalah bilangan prima atau bilangan komposit

Langkah:

1. Ambil sebarang bilangan bulat positif a, $2 \leq a \leq p-1$
2. Hitung $y \equiv a^{p-1} (\text{mod } p)$
3. Jika $y \neq 1$ maka *output* "komposit"
4. *Output* "prima"

Namun, teorema fermat memiliki kelemahan. Tidak selamanya nilai p yang diperoleh dari $a^{p-1} \equiv 1 (\text{mod } p)$ menghasilkan p sebuah bilangan prima.

Contoh:

Diberikan p = 341 dan a = 2. Maka menurut teorema fermat

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

$a^{340} \equiv 1 (\text{mod } 341)$

Padahal, $341 = 11 \cdot 13$, habis di bagi oleh bilangan prima, maka 341 adalah sebuah bilangan komposit bukan bilangan prima.

Bilangan bulat seperti 341 ini disebut dengan bilangan prima semu (*pseudo primes*). Dan bilangan prima semu relatif jarang muncul, maka tes keprimaan suatu bilangan dengan teorema fermat masih dapat digunakan. Tetapi,

tes fermat memiliki kelemahan yang lain yaitu tidak dapat mendeteksi kekompositan bilangan tertentu yang disebut dengan bilangan *Carmichael.*

3.1.1.1.3. Tes Rabin-Miller

Tes Rabin-Miller melengkapi kekurangan dari tes fermat. Segala kekurangan tes fermat telah dapat disempurnakan oleh tes Rabin-Miller. Dapat kita buat algoritma Rabin-Miller sebagai berikut:

Algoritma 3.3. (Algoritma Rabin-Miller):

Input : p, m, dan *b*

Output : p adalah bilangan prima atau bilangan komposit

Langkah:

1) Bangkitkan bilangan acak *a* yang lebih kecil dari *p.*
2) Nyatakan $j = 0$ dan hitung $z = a^m \pmod p$
3) Jika $z = 1$ atau $z = p - 1$, maka p lolos dari pengujian dan mungkin prima
4) Jika $z > 0$ dan $z = 1$, maka p bukan prima
5) Nyatakan $j = j + 1$. Jika $j < b$ dan $z \neq p - 1$, nyatakan $z = z^2 \pmod p$ dan kembali kelangkah (4) jika $z = p - 1$, maka p lolos pengujian dan mungkin prima.
6) Jika $j = b$ dan $z \neq p - 1$, maka p tidak prima.

3.1.1.2. Keprimaan Aman

Setalah kita membuktikan bahwa sebuah bilangan bulat adalah bilangan prima, kita perlu membuktikan apakah bilangan tersebut bilangan prima yang benar-benar aman. Karena kekuatan bilangan prima ini juga menentukan kuatnya

kunci kriptografi ElGamal. Maka, kita harus mencari bilangan prima yang benar-benar aman keprimaannya dengan melakukan perhitungan menggunakan algoritma bilangan prima aman sebagai berikut.

Algoritma 3.4 (Algoritma Bilangan Prima Aman):

Input : Bilangan prima p

Output : q adalah bilangan prima aman atau bilangan prima yang tidak aman.

Langkah :

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

Contoh:

Diberikan bilangan $p = 2579$, tentukan keamanan bilangan prima tersebut.

Jawab:

Di cek dengan tes keprimaan didapatkan 2579 adalah bilangan prima.

Selanjutnya, dihitung dengan rumus algoritma tes keprimaan bilangan prima aman dan tidak aman, untuk melihat keamanan sebuah bilangan prima.

$q = \frac{p-1}{2} = \frac{2579-1}{2} = \frac{2578}{2} = 1289$

Dari tes keprimaan, diperoleh bahwa 1289 merupakan sebuah bilangan prima. Jadi, 2579 adalah bilangan prima aman.

3.1.1.3. Elemen Prima Primitif

Diketahui order dari $\mathbb{Z}_p$ yang dibaca bilangan bulat modulo prima adalah $p - 1$. Jika digunakan bilangan prima p yang sama dengan $p = 2 \cdot q + 1$ dan q adalah bilangan prima, maka dapat digunakan untuk mengecek apakah suatu $\mathbb{Z}_p$

merupakan elemen primitif atau tidak. Karena $p-1=2\cdot q$, jelas 2 dan q merupakan pembagi prima dari $p-1$, sehingga harus dicek apakah $g^2 (\mathrm{mod}\ p) \neq 1$ dan $g^q (\mathrm{mod}\ p) \neq 1$. Jika keduanya dipenuhi, maka α adalah elemen primitif.

Untuk mempermudah menentukan elemen primitif, digunakan bilangan prima p sedemikian hingga $p=2\cdot q+1$, dengan q adalah bilangan prima. Bilangan prima p seperti ini disebut dengan bilangan prima aman. Karena bilangan prima telah diketahui, selanjutnya menentukan elemen primitif, elemen primitif sangat penting agar kita dapat mengetahui pembangunnya. Jadi, harus dibuat algoritma untuk menentukan sebuah elemen primitif.

Algoritma 3.5. (Algoritma Elemen Primitif) :

Input : Bilangan prima aman p dan $g \in \mathbb{Z}_p$

Output : g adalah elemen primitif atau bukan elemen primitif.

Langkah :

1) Hitung $q=\frac{p-1}{2}$.
2) Hitung $g^2 (\mathrm{mod}\ p)$ dan $g^q (\mathrm{mod}\ p)$
3) Jika $g^2 (\mathrm{mod}\ p) = 1$, maka g bukan elemen primitif.
4) Jika $g^q (\mathrm{mod}\ p) = 1$, maka g bukan elemen primitif.

Contoh:

Dengan $p = 2579$ tentukan apakah g merupakan elemen primitif dari $\mathbb{Z}_p$

Jawab:

g dikatakan elemen primitif jika $g^2 (\mathrm{mod}\ p) \neq 1$ dan $g^q (\mathrm{mod}\ p) \neq 1$

Maka, kita hitung $g^2 (\mathrm{mod}\ 2579)$ dan $g^{1289} (\mathrm{mod}\ 2579)$ apakah $\neq 1$

Untuk lebih memudahkan penghitungan kita dapat membuat sebuah table, seperti berikut:

Tabel 3.1. Perhitungan Elemen Primitif

g	2	3	4	5	6	7	8
$g^2 \pmod{2579}$	4	9	16	25	36	49	64
$g^{1289} \pmod{2579}$	2579	1	1	1	2579	1	2579

Jadi, dari sini dapat kita ketahui bahwa 2, 6, 8, merupakan elemen primitif dari $\mathbb{Z}_p$.

3.1.2. Logaritma Diskrit

Keamanan kriptografi ElGamal terletak pada sulitnya menghitung logaritma diskrit (Munir, 2006: 184). 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 $g^x \equiv y \pmod{p}$, maka x inilah yang disebut dengan masalah algoritma diskrit. Salah satu metode yang dapat digunakan untuk mencari nilai logaritma diskret 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 diskret yang besar seperti $g = 2^{225}$. 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, aritmetika modulo, dan kekongruenan dan lainnya.

3.2. Proses Penyandian Kriptografi ElGamal

Kriptografi ElGamal merupakan bagian dari kriptografi asimetris. Pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985. Kriptografi ElGamal pada mulanya digunakan untuk *digital signature*, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan deskripsi. Kriptografi ElGamal digunakan kedalam perangkat lunak sekuriti yang dikembangkan oleh GNU, program PGP, dan pada sistem sekuriti lainnya. Kriptografi ElGamal tidak dipatenkan oleh pembuatnya melainkan didasarkan atau penyempurnaan dari pada

kriptografi Diffei-Hellman, yaitu sebuah kriptografi kunci publik yang dikenalkan oleh Whitfield Diffie dan Martin Hellman. Sehingga hak paten kriptografi Diffie-Hellman mencakup kriptografi ElGamal. Dan hak paten ini telah berakhir pada tahun 1997 sehingga mulai saat itu kriptografi ElGamal dapat di komersilkan secara umum (Mulyana, 2009)

Berikut ini diberikan sistem kriptografi ElGamal yang untuk selanjutnya penulisan penotasian akan mengacu pada sistem kriptografi ElGamal berikut:

Diberikan bilangan prima p dan sebuah elemen primitif $g \in \mathbb{Z}_p$.

Ditentukan:

$\mathcal{P} = \mathbb{Z}_p$, $C = \mathbb{Z}_p \times \mathbb{Z}_p$ dan $x \in \{0,1, \dots, p-2\}$ didefiniskan

$$\mathcal{K} = \{(p, g, x, y) : y = g^x \bmod p\}$$

Nilai p, y, dan g dipublikasikan dan nilai x dirahasiakan. Untuk $\mathcal{K} = (p, g, x, y)$, *plainteks* $m \in \mathbb{Z}_p$ dan untuk suatu bilangan acak rahasia $k \in \{0,1,2, \dots, p-2\}$, di definisikan

$$e_k(m, k) = (a, b)$$

Dengan

$$a = g^k (\bmod p)$$

Dan

$$b = y^k \cdot m (\bmod p)$$

Untuk $a, b \in \mathbb{Z}_p$, didefinisikan

$$d_k(a, b) = b \cdot (a^x)^{-1} (\bmod p)$$

(Stinson, 1995)

Secara singkat dapat dituliskan besaran-besaran dalam kriptografi ElGamal yang untuk selanjutkan akan dijadikan acuan penotasian dalam penulisan skripsi ini adalah:

1) Bilangan prima, p (besifat tidak rahasia)
2) Bilangan acak, g $(g < p)$ (besifat tidak rahasia)
3) Bilangan acak, x $(x < p)$ (bersifat rahasia dan merupakan kunci privat)
4) $y = g^x \bmod p$ (bersifat tidak rahasia dan merupakan kunci publik)
5) m merupakan plainteks (bersifat rahasia)
6) a dan b merupakan chiperteks (bersifat rahasia)

3.2.1. Membangkitkan Pasangan Kunci

Membangkitkan pasangan kunci yang terdiri dari kunci rahasia dan kunci umum adalah proses pertama yang harus dilakukan dalam kriptografi ElGamal. Prosedur yang pertama dilakukan adalah memilih sembarang bilangan prima p. Selanjutnya memilih dua bilangan acak, elemen primitif g dan x dengan syarat $g < p$ dan $x \in \{0,1, \dots, p-2\}$. Maka dapat kita hitung $y = g^x \bmod p$.

Kunci umum kriptografi ElGamal berupa pasangan 3 bilangan *(tripel)*, yaitu (y, g, p), dengan $y = g^x \bmod p$. Sedangkan kunci rahasia kriptografi ElGamal berupa pasangan bilangan, yaitu (x, p).

Kriptografi ElGamal menggunakan bilangan bulat prima dalam proses perhitungan penyandiannya, maka pesan harus dikonversi ke dalam suatu bilangan bulat. Berdasarkan sistem kriptografi ElGamal di atas dapat di buat algoritmanya sebagai berikut:

Algoritma 3.6. (Algoritma Pembentukan Kunci):

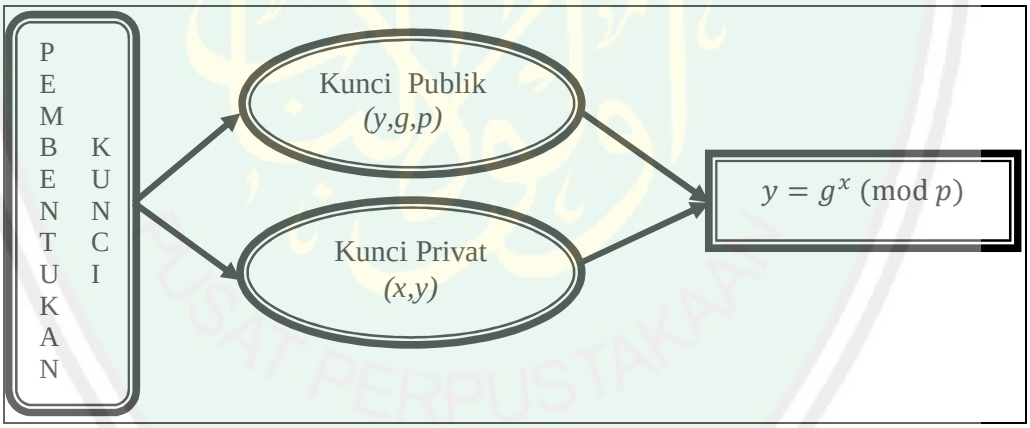
Input : Bilangan prima aman p dan elemen primitif $g \in \mathbb{Z}_p$

Output : Kunci publik (y, g, p) dan kunci privat (x, p).

Langkah :

1) Pilih sebarang bilangan prima p
2) Pilih dua buah bilangan acak, g dan x dengan syarat $(g < p)$ dan $x \in \{0,1, \ldots p-2\}$ atau $1 \leq x \leq p-2$
3) Hitung $y = g^x \pmod p$
4) Publikasikan nilai $y, g,$ dan p serta rahasiakan nilai x.

Untuk lebih jelasnya tentang segala sesuatu yang diperlukan dalam pembentukan kunci kriptografi ElGamal. Dapat dilihat skemanya sebagai berikut:



Gambar 3.1. Proses Pembentukan Kunci Kriptografi ElGamal

3.2.2. Enkripsi Pesan

Pada proses ini pesan di enkripsi menggunakan kunci publik (y, g, p) dan sebarang bilangan acak rahasia $k \in \{0,1, \ldots, p-2\}$. Misalkan *m* seperti yang telah dimisalkan sebelumnya adalah pesan yang akan dikirim atau pesan dalam bentuk

plainteks. Selanjutnya, m diubah ke dalam blok-blok karakter dan setiap karakter dikonversikan pada bilangan bulat, sehingga diperoleh plainteks $m_1, m_2,\ldots,m_n$ dengan $m_i \in \{0,1,\ldots,p-2\}, i = 1,2,\ldots,n$. Proses enkripsi pada algoritma ElGamal dilakukan dengan menghitung:

$$a = g^k \pmod p$$

dan

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

Dengan $k \in \{0,1,\ldots,p-2\}$ acak. Diperoleh cipherteks (a,b).

Dalam proses enkripsi, kunci privat adalah bilangan acak *k*. Bilangan acak *k* ditentukan oleh pihak pengirim dan harus dirahasiakan, jadi hanya pengirim saja yang mengetahuinya. Bilangan acak *k* hanya digunakan saat melakukan enkripsi saja jadi tidak perlu disimpan.

Algoritma 3.7. (Algoritma Enkripsi):

Input : Pesan yang akan di enkripsi dan kunci publik (p,g,y)

Output : Cipherteks $(a,b), i = 1,2,\ldots,n$

Langkah :

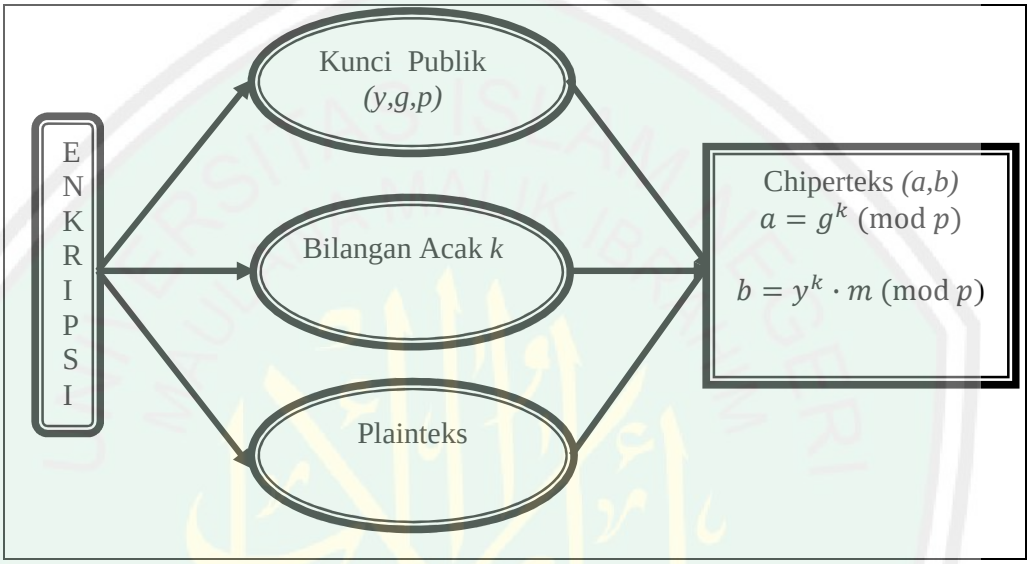
1) Susun plainteks menjadi blok-blok $m_1, m_2,\ldots,m_n$, sedemikian hingga setiap blok mempresentasikan nilai di dalam selang $[0, p-1]$
2) Pilih bilangan acak *k*, yang ada pada selang $1 \leq k \leq p-2$
3) Setiap blok *m* di enkripsi dengan rumus

$$a = g^k \pmod p$$

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

4) Diperoleh chiperteks (a,b)

Pasangan a dan b adalah sebuah chiperteks untuk blok pesan m. jadi, ukuran chiperteks dua kali ukuran plainteksnya. Untuk lebih jelasnya tentang segala sesuatu yang diperlukan dalam proses enkripsi. Dapat dilihat skema berikut:



Gambar 3.2. Proses Enkripsi Kriptografi ElGamal

3.2.3. Dekripsi Pesan

Setelah menerima cipherteks (a, b), proses selanjutnya adalah mendekripsi cipherteks menggunakan kunci publik p dan kunci rahasia x. Dapat ditunjukkan bahwa plainteks m dapat diperoleh dari cipherteks menggunakan kunci rahasia x. Seperti halnya keterangan tentang sistem kriptografi ElGamal yang dijelaskan diawal bab ini. Kita juga dapat merujuk pada teorema 3.2.3.1. dibawah ini.

Teorema 3.2.3.1.

Diberikan (p, g, y) sebagai kunci publik dan x sebagai kunci privat pada kriptografi ElGamal. Jika diberikan cipherteks (a, b), maka

$$m = b \cdot (a^x)^{-1} \pmod p$$

dengan *m* adalah plainteks.

Stinson, 1995: 68

Bukti:

Diketahui kunci publik (p, g, y) dan kunci privat *x* pada kriptografi ElGamal.

Diberikan cipherteks (a, b), dari persamaan diatas diperoleh bahwa:

$$\begin{aligned} b \cdot (a^x)^{-1} &\equiv (y^k \cdot m) \cdot (a^x)^{-1} \pmod p \\ &\equiv y^k \cdot m \cdot a^{-1} \pmod p \\ &\equiv (g^x)^k \cdot m \cdot (g^k)^{-x} \pmod p \\ &\equiv g^{x \cdot k} \cdot m \cdot g^{-x \cdot k} \pmod p \\ &\equiv m \cdot g^0 \pmod p \\ &\equiv m \pmod p \end{aligned}$$

Dengan demikian didapatkan:

$$b \cdot (a^x)^{-1} \equiv m \pmod p$$

$$m = b \cdot (a^x)^{-1} \bmod p$$

Karena $\mathbb{Z}_p$ mempunyai orde $p - 1$ dari $x \in \{0,1, \dots, p-2\}$, Maka:

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

Algoritma 3.8 (Algoritma Dekripsi):

Input : Cipherteks (a, b), kunci publik (p, g, y) dan kunci privat *x*.

Output : Pesan asli.

Langkah :

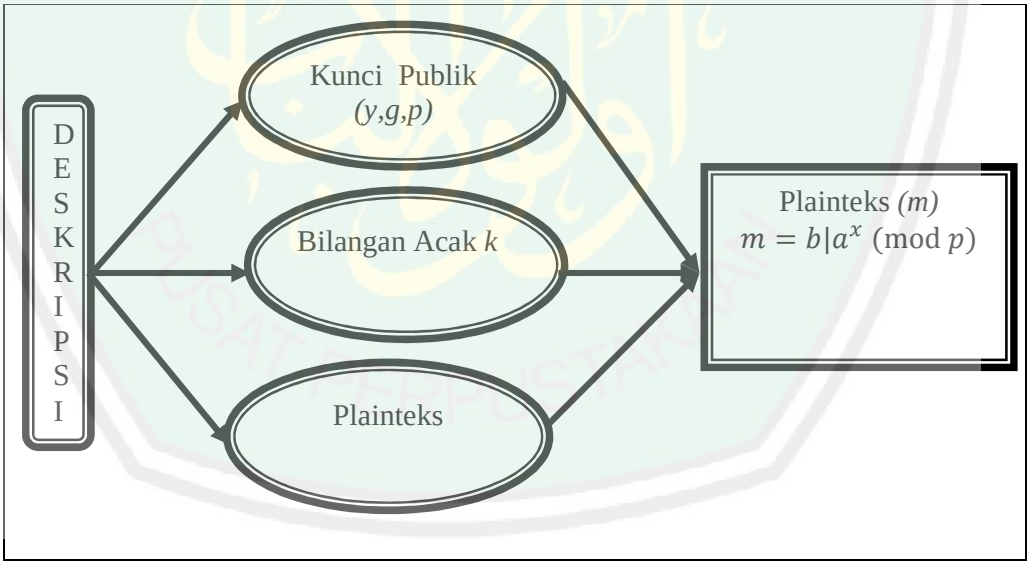
1) Gunakan kunci privat *x* untuk mendeskripsikan *a* dan *b* menjadi plainteks *m* dengan persamaan $m = b|a^x \pmod p$

2) Diperoleh plainteks $m_1, m_2, \ldots, m_n$.

Dalam menghitung algoritma deskripsi harus di ingat beberapa catatan berikut ini:

1) $(a^x)^{-1} = a^{-x} = a^{p-1-x} \pmod p$. Harus diingat bahwa "$^{-1}$" menyatakan invers modulo.
2) $a^x \equiv g^{k \cdot x} \pmod p$ maka
   $b|a^x \equiv y^k \cdot m|a^x$
   $\equiv g^{x \cdot k} \cdot m|a^{x \cdot k}$
   $\equiv m \pmod p$
3) Plainteks dapat ditemukan kembali dari pasangan chiperteks (a, b)

Untuk lebih jelasnya tentang segala sesuatu yang diperlukan dalam proses enkripsi dapat di lihat dalam skema berikut:



Gambar 3.3. Proses Deskripsi Kriptografi ElGamal

Kriptografi ElGamal diciptakan untuk mengamankan pesan atau informasi-informasi rahasia yang tidak boleh diketahui oleh pihak-pihak yang tidak berhak. Kriptografi ElGamal adalah bagian dari kriptografi kunci-publik

yang berarti dalam mengamankan pesannya menggunakan dua buah kunci. Untuk mengubah pesan menjadi plainteks yang dinamakan kunci publik dan mengubah plainteks menjadi chiperteks yang dinamakan kunci privat. Pihak yang membuat kunci publik dan kunci rahasia adalah penerima, sedangkan pihak pengirim hanya mengetahui kunci publik yang diberikan oleh penerima, dan kunci publik tersebut digunakan untuk mengenkripsi pesan. Jadi, pemegang kendali keamanan penuh adalah penerima pesan. Maka dengan menggunakan kriptografi kunci publik adalah tidak ada permasalahan pada distribusi kunci apabila jumlah pengirim sangat banyak serta tidak ada kepastian keamanan jalur yang digunakan.

3.2.4. Pengiriman Pesan Rahasia

Setelah kita mengetahui segala sesuatu yang dibutuhkan dalam penyandian menggunakan kriptografi ElGamal. Sekarang kita mempelajarinya melewati contoh agar lebih jelas. Misalkan suatu saat, Anwar dan Dani ingin membagi sebuah informasi rahasia tentang nilai matematika salah seorang temannya yang berbunyi "matematika susi dapat A" dan pesan ini merupakan pesan rahasia maka yang perlu mereka lakukan adalah sebagai berikut:

1. Proses pembentukan kunci kriptografi ElGamal
    - Anwar membangkitkan pasangan kunci privat dan kunci publik dengan memilih bilangan prima (p), bilangan bulat acak (g, x) dan melakukan perhitungan dengan menggunakan rumus, berikut:

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

      Dengan, $p = 2579$, $g = 2$ dan $x = 765$

      Maka didapatkan $y = 2^{765} \pmod{2579} = 949$

- Maka Anwar mendapatkan pasangan kunci publik $(y, g, p) = (949, 2, 2579)$ dan pasangan kunci privat $(x, p) = (765, 2579)$
- Anwar memberikan kunci publik pada siapapun yang dikehendakinya termasuk Dani sementara kunci privat disimpan untuk dirinya sendiri.

2. Proses enkripsi kriptografi ElGamal

Dani ingin mengirimkan pesan rahasia pada Anwar yang berbunyi "matematika Susi dapat A". Maka yang perlu dilakukan Dani adalah:

- Memotong pesan menjadi blok-blok karakter
- Menkonversikan blok-blok karakter kedalam bilangan bulat kode ASCII (lihat lampiran 1)

  Kode ASCII *(American Standard for Information Interchange)*, merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255. Berdasarkan sistem kriptografi ElGamal di atas, maka harus digunakan bilangan prima yang lebih besar dari 255. Kode ASCII berkorespondensi 1-1 dengan karakter pesan.

Tabel 3.2. Konversi Pesan ke dalam Kode ASCII

i	Karakter	Plaintek *m*	Kode ASCII
1	m	m_1	109
2	a	m_2	97
3	t	m_3	84
4	e	m_4	101
5	m	m_5	109

i	Karakter	Plaintek m	Kode ASCII
6	a	m_6	97
7	t	m_7	84
8	i	m_8	105
9	k	m_9	107
10	a	m_{10}	97
11	(spasi)	m_{11}	32
12	S	m_{12}	83
13	u	m_{13}	117
14	s	m_{14}	115
15	i	m_{15}	105
16	(spasi)	m_{16}	32
17	d	m_{17}	100
18	a	m_{18}	97
19	p	m_{19}	112
20	a	m_{20}	97
21	t	m_{21}	84
22	(spasi)	m_{22}	32
23	A	m_{23}	65

Dari table diatas dapat kita ketahui bahwa pesan tersebut mempunyi 23 blok karakter.

- Mengenkripsi pesan menggunakan kunci publik dan memilih bilangan bulat acak k untuk setiap karakter

  Dengan $k_i \in \{1,2,\dots,2579-2\}$; $i = 1,2,\dots,23$. Kemudian kita hitung nilai $a = g^k \pmod p$ dan $b = y^k \cdot m \pmod p$sebagai berikut:

Tabel 3.3. Perhitungan Enkripsi

i	m_i	k_i	$a = g^k \pmod p$ $a = 2^k \pmod{2579}$	$b = y^k \cdot m \pmod p$ $b = 949^k \cdot m \pmod{2579}$
1	109	1843	1512	1252
2	97	1404	313	1998
3	84	1414	716	814
4	101	1527	711	344
5	109	146	22	359
6	97	2298	520	1516
7	84	1414	716	814
8	105	990	875	1089
9	107	2183	1259	257
10	97	2154	329	1233
11	32	1012	998	1790
12	83	998	2206	1672
13	117	1091	195	1173
14	115	1012	998	1790
15	105	869	2473	2104
16	32	1236	2145	2305
17	100	1664	363	960
18	97	2298	520	1516

i	m_i	k_i	$a = g^k \pmod p$ $a = 2^k \pmod{2579}$	$b = y^k \cdot m \pmod p$ $b = 949^k \cdot m \pmod{2579}$
19	112	2483	1742	830
20	97	1404	313	1998
21	84	1414	716	814
22	32	1606	2183	275
23	65	218	561	1800

- Dani mendapatkan pasangan chiperteks dan mengirimkannya pada Anwar, sebagai berikut:

Tabel 3.4. Pasangan Chiperteks

i	Chiperteks	i	Chiperteks	I	chiperteks	i	chiperteks
1	(1512,1252)	7	(716,814)	13	(195,1173)	19	(1742,830)
2	(313,1998)	8	(875,1089)	14	(998,1790)	20	(313,1998)
3	(716,814)	9	(1259,257)	15	(2473,2104)	21	(719,814)
4	(771,334)	10	(329,1233)	16	(2145,2305)	22	(2183,275)
5	(22,359)	11	(998,1790)	17	(363,960)	23	(516,1800)
6	(520,1516)	12	(2206, 1672)	18	(520,1516)		

3. Proses deskripsi kriptografi ElGamal

Anwar telah mendapatkan chiperteks pesan rahasia dari Dani, maka Anwar melakukan proses deskripsi menggunakan kunci privatnya sebagai berikut:

Tabel 3.5. Perhitungan Deskripsi

i	a	b	$a^{-x} = a^{p-1-x} \pmod p$ $a^{-x} = a^{2579-1-765} \pmod{2579}$	$m = b\|a^x \pmod p$ $m = b\|a^x \pmod{2579}$	Karakter
1	1521	1252	2301	109	m
2	313	1998	133	97	a
3	716	814	1090	84	t
4	711	344	2047	101	e
5	22	359	1825	109	m
6	520	1516	1771	97	a
7	716	814	1090	84	t
8	875	1089	1826	105	i
9	1259	257	1887	107	k
10	329	1233	2098	97	a
11	998	1790	925	32	(spasi)
12	2206	1672	665	83	S
13	195	1173	1128	117	u
14	998	1790	925	32	s
15	2473	2104	1330	105	i
16	2145	2305	847	32	(spasi)
17	363	960	2203	100	d
18	520	1516	1771	97	a

i	a	b	$a^{-x} = a^{p-1-x} \pmod p$ $a^{-x} = a^{2579-1-765} \pmod{2579}$	$m = b\|a^x \pmod p$ $m = b\|a^x \pmod{2579}$	Karakter
18	520	1516	1771	97	a
19	1742	830	286	112	p
20	313	1998	133	97	a
21	716	814	1090	84	t
22	2183	275	394	32	(spasi)
23	516	1800	2098	97	A

Jadi, setelah melakukan proses deskripsi dengan kunci privat yang dimilikinya Anwar dapat mengetahui pesan yang sebanarnya yaitu "matematika Susi dapat A"

3.3 . Kelebihan dan Kelemahan Kriptografi ElGamal

Kriptografi ElGamal yang merupakan bagian dari algoritma kriptografi asimetri dan mempunyai kelebihan serta kekurangan seperti kriptografi kunci yang lainnya. Saat kita membicarakan kelebihan dan kelemahan kriptografi ElGamal secara otomatis telah mencakup kelebihan dan kelemahan kriptografi asimetri secara umum. Kriptografi ElGamal merupakan penyempurnaan dari kriptografi Diffie-Hellman, jadi, jelas mempunyai banyak kelebihan. Namun, kriptografi ElGamal yang mendasarkan perhitungannya pada masalah logaritma diskrit melalui proses perhitungnan yang tidak mudah. Dari penjelasan tentang

kriptografi ElGamal sebelumnya maka kita dapatkan kesimpulan tentang kelebihan dan kelemahan algoritma ElGamal sebagai berikut:

1. Kelebihan Kriptografi ElGamal
   a) Kriptografi ElGamal juga dikenal sebagai kriptografi *digital signature* karena dapat difungsikan secara baik untuk mengirimkan sebuah tanda tangan digital pada sebuah pesan dan lebih sempurna dibandingkan kriptografi Diffie-Hellman.
   b) Sebuah plaintek yang sama dapat diubah menjadi chiperteks yang berbeda karena dalam kriptografi ElGamal, kita dapat memilih secara acak bilangan bulat untuk membuat sebuah kunci.
   c) Dalam kriptografi ElGamal sama seperti beberapa jenis kriptografi kunci yang lain. Hanya kunci privat yang perlu dijamin kerahasiannya. Tetapi, autentikasi kunci publik juga harus tetap dijaga.
   d) Pasangan kunci publik dan kunci privat pada kriptografi ElGamal tidak perlu diubah dalam periode waktu yang panjang.
   e) Kriptografi ElGamal bisa dimanfaatkan untuk mengirimkan sebuah pesan rahasia yang sangat rahasia, yaitu kunci dari sebuah kriptografi simetris
2. Kelemahan kriptografi ElGamal
   a) Kriptografi ElGamal yang menitik beratkan perhitungannya pada logaritma diskrit dan pencarian bilangan-bilangan prima yang besar dan operasi perpangkatan yang juga besar memerlukan waktu yang sangat lama pada proses enkripsi dan deskripsinya.
   b) Ukuran chiperteks lebih besar dari pada plainteks

c) Ukuran kunci relatif lebih besar dari pada ukuran kunci kripografi simetri
d) Kunci publik yang dikirimkan kesemua orang yang berhubungan dengan pembuat kunci, menjadikan autentikasi pengirim tidak jelas.
e) Walaupun kriptografi ElGamal melalui proses perhitungannya dengan tahapan yang tidak mudah, tapi karena kriptografi ElGamal mendasarkan perhitungannya pada sulitnya memecahkan persoalan-persoalan aritmetik maka para kriptoanalisis yang benar-benar mempelajari algoritma dapat memecahkannya lambat-laun.

Kriptografi ElGamal bukanlah kriptografi terbaik yang dapat digunakan. Sangat tidak dibenarkan jika seseorang mengatakan salah satu kriptografi sebagai kriptografi yang terbaik. Karena, baik kriptografi simetri maupun asimetri akan saling melengkapi kekurangan yang lainnya.

BAB IV

PENUTUP

4.1. Kesimpulan

Kesimpulan yang dapat diambil penulis setelah menyelesaikan pembuatan skripsi ini adalah :

1. Kriptografi ElGamal, mendasarkan kekuatannya pada masalah logaritma diskrit dan dalam proses pembuatan kuncinya menggunakan bilangan prima. Pemecahan masalah logaritma diskrit yang cukup menyulitkan dan bilangan prima yang besar menambah kekuatan keamanan kriptografi ElGamal.
2. Proses penyandian kriptografi ElGamal adalah pembentukan kunci, enkripsi dan deskripsi.
   a) Algoritma pembentukan kunci

      Input : Bilangan prima aman p dan elemen primitif $g \in \mathbb{Z}_p$

      Output : Kunci publik (y, g, p) dan kunci privat (x, p).

      Langkah :

      1) Pilih sebarang bilangan prima p
      2) Pilih dua buah bilangan acak, g dan x dengan syarat $(g < p)$ dan $x \in \{0,1, \dots p-2\}$ atau $1 \leq x \leq p-2$
      3) Hitung $y = g^x \bmod P$
      4) Publikasikan nilai $y, g,$ dan p serta rahasiakan nilai x.

   b) Algoritma enkripsi

      Input : Pesan yang akan di enkripsi dan kunci publik (p, g, y)

Output : Cipherteks $(a, b), i = 1,2, \dots, n$

Langkah :

1) Susun plainteks menjadi blok-blok m_1, m_2,…,m_n, sedemikian hingga setiap blok mempresentasikan nilai di dalam selang $[0, p-1]$
2) Pilih bilangan acak *k*, yang ada pada selang $1 \leq k \leq p-2$
3) Setiap blok *m* di enkripsi dengan rumus
   a. $a = g^k \pmod p$
   b. $b = y^k \cdot m \pmod p$
4) Diperoleh chiperteks (a, b)

c) Algoritma deskripsi

Input : Cipherteks (a, b), kunci publik (p, g, y) dan kunci privat *x*.

Output : Pesan asli.

Langkah :

1) Gunakan kunci privat *x* untuk mendeskripsikan *a* dan *b* menjadi plainteks *m* dengan persamaan $m = b|a^x \pmod p$
2) Diperoleh plainteks m_1,m_2,…,m_n.

3. Kriptografi ElGamal, mempunyai beberapa kelebihan dan kelemahan sama seperti kriptografi asimetri yang lain. Salah satu kelebihannya, kriptografi ElGamal menggunakan bilangan bulat acak untuk membuat kuncinya. Jadi, chiperteks bisa berbeda walaupun berkarakter sama. Dan salah satu kelemahannya adalah perhitungan kuncinya yang memerlukan waktu yang cukup lama.

4.2. Saran

1. Usahakan untuk menyimpan chiperteks dalam bentuk hasil enkripsi dengan algoritma ElGamal dan menyimpan kunci publik dengan baik
2. Pembaca dapat mengkaji lebih dalam tentang kriptografi ElGamal sehingga dapat mengimplementasikannya dalam *digital signature*, mengamankan ATM, mengamankan kartu seluler dan sebagainya.
3. Pesan yang berupa video, *image*, dan sebagainya memerlukan pengkajian lebih mendalam lagi.

DAFTAR PUSTAKA

Al-Qur'an dan terjemahnya. 1998. Departemen Agama.

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

Ariyus, Doni. 2006. *Kriptografi.* Yogyakarta: CV. Andi *offset*

_____, 2008. *Pengantar Ilmu Kriptografi*. Yogyakarta: CV. Andi *offset*

Ichwan, Nur Muhammad. 2001. *Memasuki Dunia Al-Qur'an.* Semarang: Lubuk Raya.

Munir, Rinaldi. 2003. *Matematika Diskrit.* Bandung: Informatika Bandung

_____, 2006. *Kriptografi.* Bandung: Informatika Bandung

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

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

Flourensia. Sapty Rahayu .2005. Cryptografi *(e-book online)* http://cryptografi/124p/04/final0.1. diakses tanggal 06 Agustus 2009

Mulyana, Sandi. 2009. FLOWCHART & SOURCE CODE ELGAMAL (*online*). http://www.algoritma_9.kriptogrsfi/elgamal/102/. Diakses tanggal 02 Juli 2009

Munir, Rinaldi. 2004. Algoritma RSA dan ElGamal. *(online)* http://www.alg2.kriptografi/if5054/398/88/. Diakses tanggal 2 Juli 2009

Lampiran 1. Tabel Kode ASCII

Kode ASCII (0-127)

No.	Kode	No.	Kode	No.	Kode
0	NULL (null)	47	/	94	^
1	SOH (start of heading)	48	0	95	_
2	STX (start of text)	49	1	96	`
3	ETX (end of text)	50	2	97	a
4	EOT (end of transmission)	51	3	98	b
5	ENQ (enquiry)	52	4	99	c
6	ACK (acknowledge)	53	5	100	d
7	BEL (bell)	54	6	101	e
8	BS (backspace)	55	7	102	f
9	TAB (horizontal tab)	56	8	103	g
10	LF (new line)	57	9	104	h
11	VT (vertical tab)	58	:	105	i
12	FF (new page)	59	;	106	j
13	CR (carriage return)	60	<	107	k
14	SO (shift out)	61	=	108	l
15	SI (shift in)	62	>	109	m
16	DLE (data link espace)	63	?	110	n
17	DC1 (device control 1)	64	@	111	o
18	DC2 (device control 1)	65	A	112	p
19	DC3 (device control 1)	66	B	113	q
20	DC4 (device control 1)	67	C	114	r
21	NAK (negative acknowledge)	68	D	115	s
22	SYN (synchronus idle)	69	E	116	t
23	ETB (end of trans. Blok)	70	F	117	u
24	CAN (cancel)	71	G	118	v
25	EM (end of medium)	72	H	119	w
26	SUB (substitute)	73	I	120	x
27	ESC (escape)	74	J	121	y
28	FS (file separator)	75	K	122	z
29	GS (group separator)	76	L	123	{
30	RS (record separator)	77	M	124	|
31	US (unit separator)	78	N	125	}
32	space	79	O	126	~
33	!	80	P	127	DEL
34	"	81	Q		
35	#	82	R		
36	$	83	S		
37	%	84	T		
38	&	85	U		
39	'	86	V		
40	(	87	W		
41	)	88	X		
42	*	89	Y		
43	+	90	Z		
44	,	91	[		
45	-	92	\		
46	.	93	]		