BAB II

LANDASAN TEORI

2.1 Kriptografi

Kriptografi mempunyai peranan penting dalam dunia komputer. Hal ini disebabkan karena banyaknya informasi rahasia yang disimpan dan dikirimkan melalui media-media komputer. Informasi-informasi ini biasanya berisi dokumen-dokumen penting yang tidak boleh diketahui oleh pihak-pihak yang tidak berkepentingan. Oleh karena itu kriptografi setiap saat selalu dikembangkan untuk menjaga informasi-informasi tersebut.

2.1.1 Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita (Bruce Schneier - *Applied Cryptography*). Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (A. Menezes, P. van Oorschot and S. Vanstone - *Handbook of Applied Cryptography*). Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

- Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
- Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
- Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
- Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

2.1.2 Sejarah Kriptografi

Sejak 4000 tahun lalu kriptografi telah dikenal oleh orang-orang Mesir lewat ***hieroglyph*** walaupun bukan dalam bentuk tulisan standard. Pada zaman Rumawi Kuno, Julius Caesar mengirimkan pesan rahasia kepada panglima perang

di medan perang dengan mengganti semua susunan alfabet dari: *a b c d e f g h i j k l m n o p q r s t u v w x y z,* menjadi: *d e f g h i j k l m n o p q r s t u v w x y z a b c.*

Pada zaman Rumawi Kuno, telah ada alat untuk mengirim pesan rahasia dengan nama Scytale yang digunakan oleh tentara Sparta. Scytale merupakan alat yang memiliki pita panjang dari daun papirus dan sebatang silinder. Pesan ditulis diatas pita yang dililitkan pada sebatang silinder, setelah itu pita dilepas dari batang silinder lalu dikirim. Untuk membaca pesan, pita tersebut dililitkan kembali pada sebatang silinder yang diameternya sama sehingga yang menjadi kunci pada Scytale adalah diameter silinder.

Seiring dengan perkembangan zaman, kriptografi mengalami pengembangan untuk menjaga kerahasiaan pesan (informasi) agar orang tidak berhak tidak dapat melihat/membaca pesan tersebut sehingga metode penyadian pesan semakin berkembang.

Perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena itu dikembangkanlah cabang ilmu

yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Algoritma kriptografi berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis yaitu :

- **Algoritma Simetri *(Kriptografi Klasik)***

  Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi adalah kunci yang sama

- **Algoritma Asimetri (Kriptografi Publik)**

  Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

Sedangkan berdasarkan besar data yang diolah dalam satu kali proses, maka algoritma kriptografi dapat dibedakan menjadi dua jenis yaitu :

- Algoritma *block cipher*

  Informasi/data yang hendak dikirim dalam bentuk blok-blok besar (misal 64-bit) dimana blok-blok ini dioperasikan dengan fungsi

enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok yang berukuran sama.

- Algoritma stream cipher

  Informasi/data yang hendak dikirim dioperasikan dalam bentuk blok-blok yang lebih kecil (byte atau bit), biasanya satu karakter persatuan persatuan waktu proses, menggunakan tranformasi enkripsi yang berubah setiap waktu.

2.1.3 Konsep Kriptografi

Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

- **Plaintext** (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- **Ciphertext** (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.

- **Enkripsi** (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
- **Dekripsi** (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
- **Kunci** adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti.

2.2 Algoritma Kriptografi ElGamal

Algoritma ElGamal merupakan salah satu algoritma kriptografi kunci publik (asimetris) yang ditemukan oleh seorang ilmuwan Mesir Taher ElGamal pada tahun 1985. Kekuatan dari algoritma ElGamal ini terletak pada sulitnya menghitung logaritma diskrit. Algoritma ini menggunakan dua jenis kunci, yaitu kunci publik dan kunci rahasia. Algoritma ElGamal mempunyai kunci publik berupa tiga pasang bilangan dan kunci rahasia berupa satu bilangan.

Algoritma ini melakukan proses enkripsi dan dekripsi pada blok-blok plainteks dan dihasilkan blok-blok cipherteks yang masing-masing terdiri dari dua pasang bilangan. Untuk proses enkripsi menggunakan kunci publik, sedangkan proses dekripsi menggunakan kunci privat.

Sebelum proses enkripsi dilakukan, hal pertama yang harus dilalui adalah proses pembangkitan kunci, keluaran dari proses ini adalah berupa kunci publik yang nantinya akan dikirimkan kepada pengirim pesan untuk meng-enkripsi pesan rahasia.

2.2.1 Pembentukan Kunci

Proses pertamaadalahpembentukankunciyangterdiridarikunci rahasiadankuncipublik.Padaproses inidibutuhkansebuahbilanganprima$p$ yang digunakanuntukmembentukgrup $\mathbb{Z}_p^*$,elemenprimitifα dansebarang $a \in \{0,1,..., p - 2\}$.

KuncipublikalgoritmaEl-Gamalberupapasangan3bilangan,yaitu(p,α ,β), dengan $\beta = \alpha^a \bmod p$. *S*edangkan kuncirahasianya adalah bilangan$a$ tersebut.

Diketahuiorderdari$\mathbb{Z}_p^*$ adalah$p-1$.Jikadigunakanbilanganprima$p$ dengan$p = 2.q + 1$ dan q adalah bilangan prima, makadapatdigunakan untuk mengecek apakah suatu $\alpha \in \mathbb{Z}_p^*$ merupakan elemen primitif atau tidak. Karena $p - 1 = 2.q$, jelas2 dan$q$merupakan pembagi prima dari $p - 1$, sehinggaharusdicekapakah$\alpha^2 \bmod p \neq 1$dan$\alpha^q \bmod p \neq 1$.Jikakeduanya dipenuhi, makaα adalahelemen primitif.

Agarmempermudahdalammenentukan elemenprimitif,digunakan bilangan prima$p$ sedemikian hingga$p = 2.q + 1$, dengan$q$adalah bilangan prima.Bilangan prima$p$ seperti inidisebutdengan bilangan*prima aman*. Untuk menentukan apakah suatu bilangan itu prima atau komposit, dapat digunakanteskeprimaanseperti teskeprimaan biasadan tesMiller-Rabbin. Kerenadigunakanbilanganbulatyang

besarmakaperhitunganpemangkatan modulo dilakukan menggunakan metode*fastexponentiation*.

2.2.1.1TesBilanganPrima Aman

Input:Bilangan prima$p \geq 5$.

Output:*Pernyataan*"primaaman" atau "bukan primaaman".

Langkah:

1. Hitung$q=\frac{p-1}{2}$

2. Jika*q*adalah bilangan prima,maka*output*("primaaman").3. Jika*q* komposit, maka*output*("bukan prima aman").

2.2.1.2TesElemenPrimitif

Input:Bilangan prima aman$p \geq 5$ dan $\alpha \in \mathbb{Z}_p^*$.

Output:Pernyataan"α adalahelemenprimitif"atau "α bukanelemen primitif".

Langkah:

1. Hitung$q=\frac{p-1}{2}$

2. Hitung$\alpha^2 \bmod p$ dan $\alpha^q \bmod p$.

3. Jika$\alpha^2 \bmod p = 1$, maka*output*("α bukanelemen primitif").

4. Jika$\alpha^q \bmod p \neq 1$, maka*output*("α bukan elemen primitif").

5. *Output*(“α adalah elemen primitif”).

Karenapadaalgoritma El-Gamalmenggunakan bilangan bulatdalam proses perhitungannya, makapesanharus dikonversikedalamsuatubilangan bulat.Untukmengubahpesan menjadibilanganbulat,digunakankodeASCII (*AmericanStandardforInformation Interchange*).KodeASCII merupakan representasinumerikdarikarakter-karakteryang digunakanpadakomputer, sertamempunyainilaiminimal0dan maksimal255. Oleh karenaitu, berdasarkan sistem kriptografi El-Gamal di atas maka harus digunakanbilanganprimayanglebihbesardari255.KodeASCIIberkorespondensi1-1 dengan karakter pesan.

2.2.1.3Algoritma PembentukanKunci

Input :Bilangan prima aman$p > 255$ danelemen primitif$\alpha \in \mathbb{Z}_p^*$.

Output:Kuncipublik (p,α ,β) dan kuncirahasia$a$.

Langkah:

1. Pilih$a \in \{0,1,..., p-2\}$.
2. Hitung$\beta = \alpha^a \bmod p$.
3. Publikasikan nilai$p$, α danβ , sertarahasiakan nilai$a$.

Pihakyang membuatkuncipublikdankuncirahasiaadalahpenerima, sedangkanpihakpengirimhanyamengetahuikuncipublikyangdiberikan oleh penerima, dan kunci publik tersebut digunakan untuk mengenkripsi pesan.

Jadi, kentungan menggunakan algoritma kriptografi kunci publik adalah tidakadapermasalahanpadadistribusikunciapabilajumlahpengirim sangatbanyaksertatidakadakepastian keamananjalur yangdigunakan. Berikutinidiberikansebuahcontohkasus penggunaanalgoritmaEl- Gamaluntuk pengamanan suatu pesan rahasia.

2.2.2 Enkripsi

Padaproses inipesandienkripsimenggunakankuncipublik(p,α,β) dansebarangbilanganacakrahasia$k \in \{0,1,...,p-2\}$.Misalkan$m$ adalah pesanyang akandikirim.Selanjutnya,$m$diubahkedalamblok-blokkarakter dansetiapkarakterdikonversikankedalamkode ASCII,sehinggadiperoleh plainteks$m_1,m_2....m_n$ dengan$\{1,2,...,1\}$ $_i m \in p-$,i=1,2,...,n.Untuk nilaiASCIIbilangan 0 digunakanuntuk menandaiakhir darisuatuteks.

Proses enkripsi pada algoritma El-Gamal dilakukan dengan menghitung$\gamma = \alpha^k \bmod pDan\delta = \beta^k . m_i \bmod$ dengan$k \in \{0,1,..., p-2\}$ acak. Diperoleh cipherteks(γ,δ) .Bilangan acak k ditentukan oleh pihak pengirim dan harus dirahasiakan,jadihanyapengirimsajayangmengetahuinya,tetapinilai k hanyadigunakan saat melakukanenkripsisajadan tidak perlu disimpan.

2.2.2.1AlgoritmaEnkripsi

Input:Pesanyangakan dienkripsidan kuncipublik (p,α,β) .

Output:Cipherteks(γ_i, δ_i), i=1, 2,..., n.

Langkah:

1. Pesan dipotong-potongkedalambentuk blok-blok pesan dengan setiap blokadalah satu karakter pesan.
2. Konversikan masing-masingkarakter kedalamkodeASCII, maka diperolehplainteks sebanyak$n$ bilangan,yaitu$m_1, m_2,\ldots m_n$.
3. Untuk $i$dari1 sampai$n$ kerjakan :

   3.1 Pilih sebarangbilangan acak rahasia$k_i \in \{0,1,..., P\text{-}2\}$

   3.2 Hitung$\gamma_i=\alpha^{ki} \bmod p$

   3.3 Hitung$\delta_i = \beta^{ki}\, m_i \bmod p$.
4. Diperoleh cipherteksyaitu (γ_i,δ_i), i=1, 2,..., n .

2.2.3 Dekripsi

Setelah menerimacipherteks (γ,δ), prosesselanjutnyaadalah mendekripsicipherteksmenggunakankuncipublik $p$dankuncirahasia$a$. Dapatditunjukkanbahwaplainteks$m$ dapatdiperolehdaricipherteks menggunakan kuncirahasia$a$.

2.2.3.1AlgoritmaDekripsi

Input :Cipherteks(γ_i,δ_i),i=1,2,...,n.,kuncipublik$p$dankunci rahasia$a$.

Output:Pesan asli.

Langkah:

1.Untuk*i*dari1 sampai*n* kerjakan :

1.1 Hitung$\gamma_i^{\,p-1-a} \bmod p$.

1.2 Hitung$m_i = \delta_i \cdot \gamma_i^{\,p-1-a} \bmod p$.

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

3.Konversikanmasing-masingbilangan$m_1, \; m_2 \; , \ldots, m_n$ kedalam karakter sesuaidengankodeASCII-nya,kemudianhasilnya digabungkan kembali.