BAB II
TINJAUAN PUSTAKA

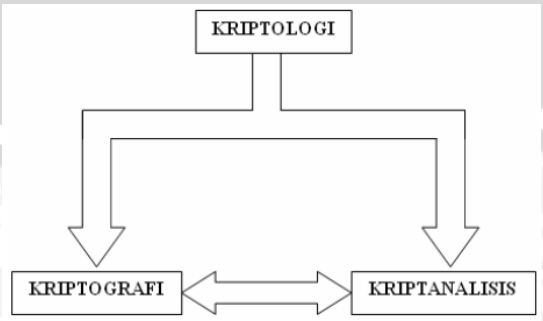
2.1 Kriptografi

2.1.1 Definisi Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani yang terdiri dari 2 kata yaitu *κρυπτό* yang berarti "rahasia atau tersembunyi" dan *γραφή* yang berarti "tulisan". Maka Kriptografi dapat diartikan sebagai "tulisan rahasia".

Secara umum kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan berita [bruce Schneier - Applied Cryptography]. Arti lain Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, sertaautentikasi data [A. Menezes, P. van Oorschot and S. Vanstone - Handbook of Applied Cryptography]. Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Yang dimaksud dengan kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Namun, tidak semua aspek keamanan informasi ditangani oleh kriptografi. Enkripsi erat kaitannya dengan dekripsi, untuk itulah muncul istilah kriptanalisis. Kriptanalisis adalah ilmu dan seni untuk memecahkan informasi yang telah dienkripsi tanpa mengetahui kunci yang digunakan. Pelaku kriptanalisis disebut dengan kriptanalis.[1]



Gambar 2.1. Pohon Kriptografi

2.1.2 Tujuan Kriptografi

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

a. **Kerahasiaan (*confidentiality*),** adalah menjaga isi dari informasi dengan enkripsi (penyadian) dari siapapun kecuali yang memiliki otoritas atau kunci rahasia.
b. **Keutuhan data (*integrity*),** adalah 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.
c. **Jaminan atas identitas dan keabsahan (*authenticity*),** 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.
d. **Anti penyangkalan (*non-repudiation*),** adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan/membuat.

2.1.3 Prinsip Kriptografi

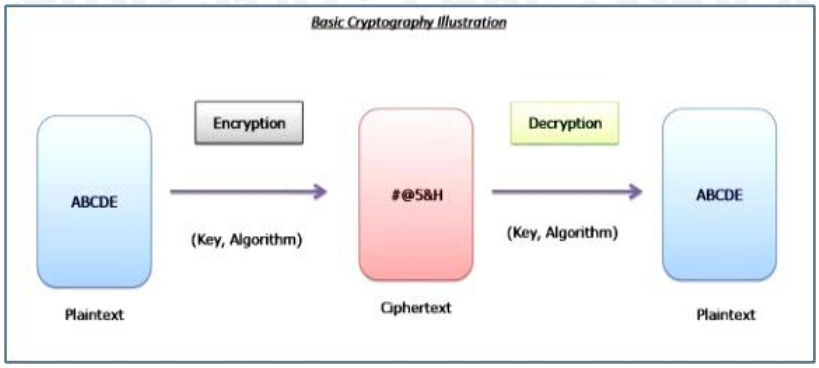
Pada prinsipnya, Kriptografi memiliki 4 komponen utama yaitu:

1. ***Plaintext***, yaitu pesan yang dapat dibaca
2. ***Ciphertext***, yaitu pesan acak yang tidak dapat dibaca
3. ***Key***, yaitu kunci untuk melakukan teknik kriptografi
4. ***Algorithm***, yaitu metode untuk melakukan enkrispi dan dekripsi

Adapun proses dasar pada Kriptografi yaitu:

1. **Enkripsi** (*Encryption*)
2. **Dekripsi** (*Decryption*)

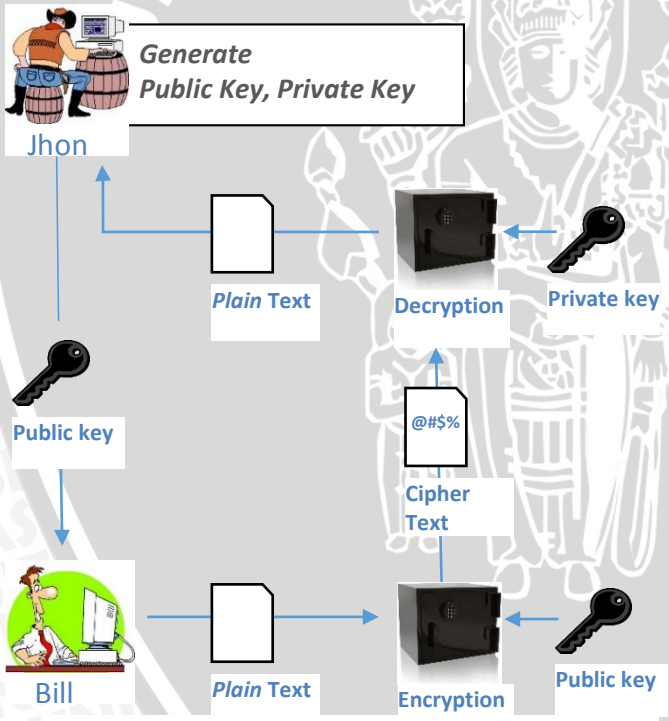
Berikut adalah ilustrasi 4 komponen dan 2 proses yang digunakan dalam teknik kriptografi.



Gambar 1.2. Ilustrasi kriptografi

2.2 Algoritma ElGamal

Algoritma ElGamal adalah sebuah algoritma untuk kriptografi kunci *public*. Algoritma ini dibuat oleh Taher ElGamal pada tahun 1985. Algoritma ini memiliki keamanan yang terletak pada kesulitan dalam menghitung logaritma diskrit. [3]



Gambar 2.3. Diagram Algoritma Kunci Publik

Properti algoritma ElGamal:

1. Bilangan prima, p (tidak rahasia)
2. Bilangan acak, g (g < p) (tidak rahasia)
3. Bilangan acak, r (r < p) (rahasia, kc. privat)

4. $z = g^r \bmod p$ (tidak rahasia, kunci. publik)
5. m atau f(x,y) (*plain*teks) (rahasia)
6. a dan b (a dan b adalah *cipher*teks) (tidak rahasia)

Algoritma kriptografi ElGamal menggunakan beberapa persamaan untuk melakukan proses *generate key*, proses enkripsi dan proses dekripsi.

- **Proses *generate key***

  Pada gambar 2.3 Bill ingin mengirim sebuah pesan melalui jalur yang aman kepada Jhon. Jhonakan memberikan kunci *public*nya kepada Bill, sedangkan kunci privat disimpan untuk dirinya sendiri. Berikut persamaan proses pembangkitan kunci.

  $z = g^r \bmod p$.

  Hasil dari algoritma ini:

  - Kunci publik: tripel (z, g, p)
  - Kunci privat: pasangan (r, p)

- **Proses Enkripsi**

  Pada gambar 2.3 Bill ingin mengirim pesan rahasia kepada Jhon. Kemudian Bill menerima kunci *public* dari Jhon. Dengan menggunakan kunci *public*, Bill akan mengenkripsi pesan rahasia tersebut kemudian dikirimkan kepada Jhon dalam bentuk *ciphertext*. Berikut langkah-langkah pada proses enkripsi :

  - Pilih bilangan acak k, yang dalam hal ini $1 \leq k \leq p - 2$.
  - Nilai m harus masih berada didalam range $0 \leq p - 1$.
  - Setiap blok dienkripsi dengan rumus

    $a = g^k \bmod p$

    $b = z^k m \bmod p$
  - Pasangan a dan b adalah *cipher*teks. Jadi, ukuran *cipher*teks dua kali ukuran *plain*teksnya.

- **Proses Dekripsi**

  Pada gambar 2.3 Jhon menerima *ciphertext*. Kemudian Jhon akan menggunakan kunci privat untuk mendekripsi *ciphertext* tersebut agar dapat

diketahui *plaintext*nya. Berikut langkah-langkah untuk mendekripsi *ciphertext* :

- Gunakan kunci privat *r*untukmenghitung
  $(a^r)^{-1} = a^{p-1-r} \bmod p$
- Hitung *plain*teks dengan persamaan:
  $m = b/a^r \bmod p = b(a^r)^{-1} \bmod p$

Plaintext dapat ditemukan kembali dari pasangan *ciphertext* a dan b.

2.3 Citra

Citra adalah suatu representasi (gambaran), kemiripan, atau *inisiasi* dari suatu objek. Citra sebagai keluaran suatu sistem perekaman *data* dapat bersifat *optic* berupa foto, bersifat *analog* berupa *sinyal – sinyal video* seperti gambar pada monitor televisi,atau bersifat *digital* yang dapat langsung disimpan pada suatu media penyimpan.

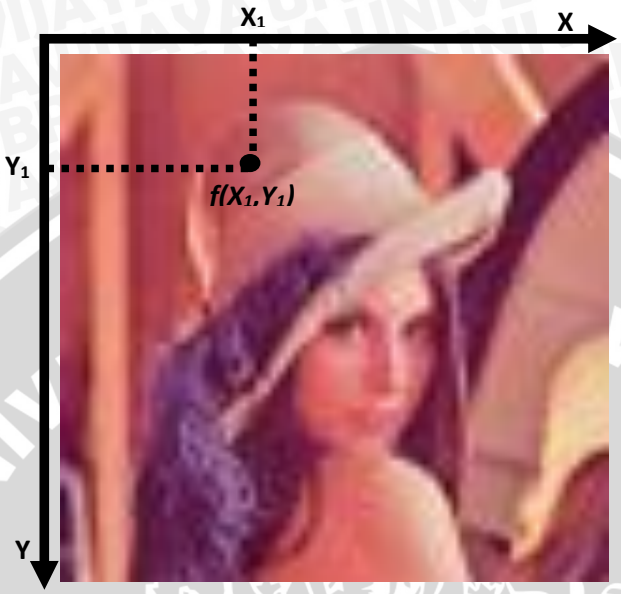
2.3.1 Citra Digital

Citra *digital* merupakan citra yang berbentuk *array* dua dimensi yang terdiri dari blok – blok kecil yang disebut dengan *pixel*. *Pixel* merupakan elemen penyusun warna terkecil yang menyusun suatu citra.Citra dibentuk dari kotak-kotak persegi yang teratur sehingga jarak *horizontal* dan *vertical* antara *pixel* adalah sama pada seluruh bagian citra. Setiap *pixel* diwakili oleh bilangan bulat (*integer*) untuk menunjukkan lokasinya dalam bidang citra. Sebuah bilangan bulat juga digunakan untuk menunjukkan cahaya atau keadaan terang gelap *pixel* tersebut.

Sebuah citra didefinisikan sebagai sebuah fungsi dua dimensi, yaitu f(x,y), dimana x dan y merupakan koordinat spasial dan besaran atau nilai dari fungsi dari setiap koordinat (x,y) yang merupakan intensitas atau tingkat keabuan dari citra pada koordinat tersebut.

Citra digital dapat direpresentasikan dalam bentuk matriks. Misalkan citra dengan ukuran M x N diman M adalah ukuran baris dan N adalah ukuran kolom, maka representasi citranya ditunjukkan dalam Gambar 2.4.

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,N-1) \\ f(1,0) & f(1,1) & \cdots & f(1,N-1) \\ \vdots & \vdots & \ddots & \vdots \\ f(M-1,0) & f(M-1,1) & \cdots & f(M-1,N-1) \end{bmatrix}$$



Gambar 2.4. Representasi Citra

2.3.2 Definisi *Digital Image Processing*

Digital Image Processing adalah proses pengolahan gambar dua dimensi oleh perangkat computer *digital*(*Jain,1989,pl*). Adapun menurut Gonzalez dan Woods (*2001,p2-3*), *digital image processing* merupakan proses pengambilan atribut – atribut pada gambar dengan *input* dan *output* yang berupa gambar. *Digital image processing* mempunyai banyak macam aplikasi pada berbagai bidang, seperti : penajaman gambar, pendeteksian objek pada gambar, pengurangan *noise*, konversi gambar berwarna ke *grayscale* dan sebaliknya, kompresi *data* pada gambar,dan sebagainya.[5]

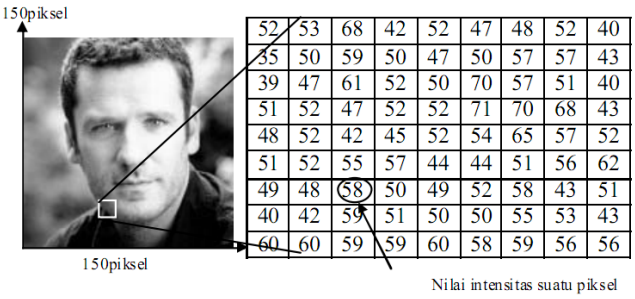
2.3.3 Pengubahan Citra Berwarna menjadi Citra *Grayscale* (*Grayscaling*)

Citra berwarna diubah menjadi citra *grayscale* dengan mengubah format citra yang awalnya adalah *RGB* menjadi *YUV* lalu diambil *Y*-nya saja. Secara matematis, perhitungan citra *grayscale* akan menjadi :

Keterangan : R = Merah, G = Hijau, B = Biru,

Grayscale = 0.299R + 0.587G + 0.114B

Dengan cara ini, maka citra berwarna akan berubah menjadi *grayscale* tanpa mengubah keaslian dari *RGB*. [4]



52	53	68	42	52	47	48	52	40
35	50	59	50	47	50	57	57	43
39	47	61	52	50	70	57	51	40
51	52	47	52	52	71	70	68	43
48	52	42	45	52	54	65	57	52
51	52	55	57	44	44	51	56	62
49	48	58	50	49	52	58	43	51
40	42	59	51	50	50	55	53	43
60	60	59	59	60	58	59	56	56

Gambar 2.5. Citra *Grayscale* 150 x 150 *pixel*

2.4 Analisis Korelasi

Korelasi adalah ukuran yang menyatakan kekuatan hubungan linier antara dua peubah acak. Korelasi dari dua buah peubah acak diskrit yang masing-masing beranggotakan *n* elemen dinyatakan dengan koefisien korelasi yang dihitung dengan rumus sebagai berikut [7]:

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}}$$

yang dalam hal ini "cov" adalah kovariansi dan "D"adalah standard deviasi:

$$\text{cov}(x, y) = \frac{1}{n}\sum_{i=1}^{b}[x_i - E(x)][y_i - E(y)]$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{b}[x_i - E(x)]^2$$

$$E(x) = \frac{1}{n}\sum^{n} x_i \qquad \text{(rata-rata)}$$

Di dalam *natural-image*, *pixel-pixel* yang bertetangga memiliki hubungan linier yang kuat. Ini ditandai oleh koefisien korelasinya yang tinggi (mendekati +1 atau -1). Di dalam citra acak, korelasi antar *pixel* bertetangga tidak ada atau koefisien korelasinya nol. Enkripsi citra bertujuan membuat korelasi *pixel-pixel* yang bertetangga di dalam *cipher-image* menjadi lemah atau dengan kata lain membuat koefisien korelasinya mendekati nol. Untuk mengetahui korelasi *pixel-*

pixel di dalam *plain-image* maupun *cipher-image*, maka dihitung koefisien korelasi antara dua *pixel* bertetangga secara horizontal [*f*(*i*,*j*) dan *f*(*i*, *j*+1)], dua *pixel* bertetangga secara vertkal [*f*(*i*,*j*) dan *f*(*i*+1, *j*)], dan dua *pixel* bertetangga secara diagonal *f*(*i*,*j*) dan *f*(*i*+1,*j*+1)]. Secara acak dipilih 1000 pasang *pixel* bertetangga pada setiap arah (vertikal, horizontal,dan diagonal), masing-masing pada citra *plainimage* dan *cipher-image*. Tanpa kehilangan generalisasi, analisis korelasi dilakukan pada citra*grayscale* saja. Dalam hal ini *x* dan *y* adalah nilai keabuan dari dua*pixel* bertetangga.

2.5 Analisis Histogram

Di dalam bidang pengolahan citra histogram memperlihatkan distribusi nilai pixel di dalam sebuah citra. Histogram digunakan penyerang (attacker) untuk melakukan kriptanalisis dengan memanfaatkan frekuensi kemunculan pixel di dalam histogram. Penyerang berharap nilai pixel yang sering muncul di dalam *plain*-image berkorelasi dengan nilai pixel yang sering muncul di dalam *cipher*-image. Dengan menganalisis frekuensi kemunculan nilai pixel, penyerang mendeduksi kunci atau pixel-pixel di dalam *plain*-image.

Agar penyerang tidak dapat menggunakan histogram untuk melakukan analisis frekuensi, maka histogram *plain*-image dan histogram *cipher*image seharusnya berbeda secara signifikan atau secara statistik tidak memiliki kemiripan. Oleh karena itu, histogram *cipher*-image seharusnya datar (flat) atau secara statistik memiliki distribusi (relatif) uniform. Distribusi yang (relatif) uniform pada *cipher*-image adalah sebuah indikasi bahwa algoritma enkripsi citra memiliki tingkat keamanan yang bagus. [7]