BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian tentang implementasi Kriptografi dengan algoritma *one time pad* pernah dilakukan dan memuat teori-teori dari penelitian sejenis. Di bawah ini adalah kutipan dan acuan dari beberapa antara peneliti antara lain:

Pada penelitiannya yang berjudul "Implementasi Algoritma *One time pad* pada Penyimpanan Data Berbasis *Web*" Penelitian ini akan mengimplementasikan algoritma *One Time Pad* (OTP) untuk melakukan penyandian terhadap data dan informasi yang disimpan. Data atau informasi yang disimpan dalam aplikasi akan berbentuk *ciphertext* sehingga *user* akan mendapatkan kunci untuk mengakses data atau informasi tersebut. dimana pihak yang dapat mengakses data atau informasi yang asli hanya pihak yang memiliki kunci (Mulyono, 2013).

Pada penelitiannya yang berjudul " kriptografi vernam cipher untuk mencegah pencurian data pada semua ekstensi *file* "Dalam makalah ini akan digunakan algoritma *vernam cipher*. Algoritma ini termasuk algoritma kunci *simetrik* yaitu adanya kesamaan kunci antara enkripsi dan dekripsi. Keunggulan *vernam cipher* dibanding *cipher* yang lain yaitu menggunakan *pseudorando-key* . Kunci acak pada *vernam cipher* berfungsi untuk menyulitkan kriptanalis dalam menemukan plainteks asli (Rachmawanto, 2016)

Pada penelitiannya yang berjudul "analisis perbandingan algoritma kriptografi klasik *vigenere cipher* dan *one time pad*" Algoritma *Vigenere Cipher* dan algoritma *One Time Pad* memiliki rumus yang sama dalam enkripsi dan dekripsi. Perbedaan kedua algoritma ini terletak pada deretan kunci yang digunakan. Algoritma *Vigenere Cipher* menggunakan kunci yang selalu berulang sepanjang pesan yang akan dienkripsi, sedangkan algoritma *One Time Pad* menggunakan kunci yang benar-benar acak dan tidak memiliki pola tertentu, dimana ukuran panjang kuncinya juga sepanjang pesan yang akan dienkripsi. Dari segi keamanan, algoritma *One Time Pa*d lebih sulit untuk ditembus oleh para kriptanalis. Kunci acak yang digunakan oleh algoritma *One Time Pad* membuat algoritma ini memiliki tingkat keamanan yang sempurna (Harhap, 2016)

Pada penelitiannya yang berjudul "Penggunaan Kriptografi *One Time Pad* (Algoritma *Vernam*) dalam Pengamanan Informasi" Algoritma *Vernam* atau *One time pad* merupakan algoritma enkripsi data dan informasi yang cukup sederhana dan mudah digunakan namun cukup aman dalam menjamin kerahasiaan informasi atau data yang ingin dikirimkan oleh pengirim pesan kepada penerima pesan tanpa dapat diketahui oleh pihak lain. Keamanan algoritma enkripsi ini sangat bergantung pada kerahasiaan kunci rahasia (*secret key*) dan *pad* yang digunakan baik dalam enkripsi maupun dekripsi data atau informasi, kunci yang di *generate* harus benar-benar acak dan hanya dapat dipergunakan sebanyak satu kali saja (Saragih, 2013)

Pada penelitiannya yang berjudul "aplikasi kriptografi dengan metode vernam cipher dan metode permutasi *biner*" Aplikasi yang di buat ini menggunakan dua metode enkripsi dan dekripsi agar lebih aman dan terjamin kerahasiaan data. Menggunakan *header* untuk menyimpan informasi-informasi seperti nama *file*, atribut *file* dan tanggal *file* sebelum dienkripsi, supaya pada saat didekripsi nama *file*, atribut *file* dan tanggal *file* tidak berubah. Aplikasi enkripsi dan dekripsi diberi kunci agar tidak sembarang *user* dapat melakukan enkripsi dan dekripsi *file* adapun Waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dipengaruhi oleh kecepatan komputer yang digunakan dan ukuran *file* (Sholeh, 2011)

2.2 Landasan Teori

2.2.1 Teks

Teks adalah wacana (berarti lisan) yang difiksasikan dalam bentuk tulisan. Dengan demikian jelas bahwa teks adalah fiksasi atau pelembagaan sebuah peristiwa wacana lisan dalam bentuk tulisan.

Salah satu definisi teks yang paling dikenal luas adalah pandangan *de Beaugrande* dan *Dressler* yang mengatakan bahwa teks adalah sebuah peristiwa komunikatif yang harus memenuhi beberapa syarat, yakni tujuh kriteria teks yang akan dikaji pada pembahasan selanjutnya.

Menurut definisi ini, tanda lalu lintas, artikel di surat kabar, argument, dan novel semuanya merupakan teks yang berhubungan dengan kaidah genre-genre atau tipe teks tertentu semua genre yang disebutkan memiliki ciri-ciri linguistik tertentu, memenuhi fungsi tertentu dan terikat pada situasi-situasi pemroduksian dan penerimaan tertentu. Oleh sebab itu, terdapat kondisi-kondisi makna yang bersifat internal teks maupun eksternal teks yang akhirnya berhadapan dengan cara mendefinisikan konteks ekstralinguistik (Adisaputra, 2011).

Dalam teori bahasa, apa yang dinamakan teks tidak lebih dari himpunan huruf yang membentuk kata dan kalimat, yang dirangkai dengan sistem tanda yang yang disepakati oleh masyarakat, sehingga sebuah teks ketika dibaca bisa mengungkapkan makna yang dikandungnya.

2.2.2 Pengertian Kriptografi

Kriptografi adalah ilmu untuk mempelajari penulisan secara rahasia dengan tujuan bahwa komunikasi dan data dapat dikodekan (*encode/encrypt*) dan dikodekan (*decode/decrypt*) kembali untuk mencegah pihak-pihak lain yang ingin mengetahui isinya. Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata *kryptos* yang artinya tersembunyi. Kriptografi dapat diartikan sebagai tulisan yang dirahasiakan atau dapat diartikan juga sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data, informasi dan dokumen dikonversi kebentuk tertentu yang sulit untuk dimengerti (Sadikin, 2012).

Proses yang dilakukan untuk mengubah *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *encipherment* sedangkan proses untuk mengubah *ciphertext* kembali ke *plaintext* disebut dekripsi (*decryption*) atau *decipherment*. Kriptografi memerlukan parameter untuk proses konversi yang dikendalikan oleh sebuah kunci atau beberapa kunci. Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi terutama dalam pengiriman pesan rahasia. Pengiriman pesan rahasia sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, pengubahan pesan yang dikirim dan lain-lain. Kriptografi dapat meningkatkan keamanan dalam pengiriman pesan atau komunikasi data dengan cara menyandikan pesan tersebut berdasarkan algoritma dan kunci tertentu yang

hanya diketahui oleh pihak-pihak yang berhak atas data, informasi dan dokumen tersebut. Di dalam kriptografi akan sering menemukan berbagai istilah atau terminologi. Beberapa istilah yang harus diketahui yaitu (Mahardika, 2010):

a. Pesan, *plaintext* dan *ciphertext*

   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas. Agar pesan tidak dapat dimengerti maknanya oleh pihak lain yang tidak berkepentingan, maka pesan perlu disandikan kebentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut *ciphertext* atau kriptogram. *Ciphertext* harus dapat ditransformasikan kembali menjadi *plaintext* semula agar dapat diterima dan bisa dibaca.

b. Pengirim dan penerima

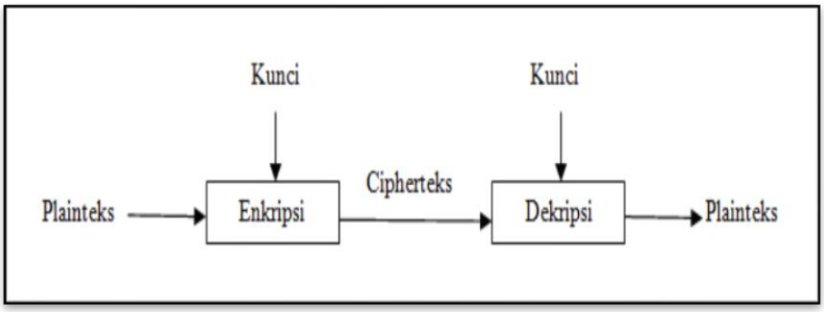
   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Pengirim tentu menginginkan pesan dapat dikirm secara aman, yaitu pengirim yakin bahwa pihak lain tidak dapat membaca isi pesan yang dikirim. Solusinya adalah dengan cara menyandikan pesan menjadi *ciphertext*.

c. Enkripsi dan dekripsi

   Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* disebut dekripsi (*decryption*) atau *deciphering*.

d. Cipher dan kunci

   Algoritma kriptografi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk *enciphering* dan *deciphering*.



Gambar 2.1 Skema Enkripsi dan Dekripsi

e. Sistem kriptografi

Kriptografi membentuk sebuah sistem yang dinamakan sistem Kriptografi. Sistem kriptografi (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma kriptografi, semua *plaintext* dan *ciphertext* yang mungkin dan kunci. Di dalam kriptografi, *cipher* hanyalah salah satu komponen saja.

f. Penyadap

Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk mendapatkan informasi sebanyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan *ciphertext*. Nama lain penyadap : *enemy, adversary, intruder, interceptor, bad guy*.

g. Kriptanalisis dan kriptologi

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. Kriptanalisis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Jika seorang kriptografer (*cryptographer*) mentransformasikan *plaintext* menjadi *ciphertext* dengan suatu algoritma dan kunci maka sebaliknya seorang kriptanalis berusaha untuk memecahkan *ciphertext* tersebut untuk menemukan *plaintext* atau kunci. Kriptologi (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis.

2.2.3 Dasar Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Prinsip-prinsip yang mendasari kriptografi yakni (Wahyudi, 2010):

1. *Secrecy* (kerahasiaan), layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka maupun menghapus informasi yang telah disandi.
2. *Authentication,* berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Dimana inforamsi yang dikirimkan melalui kanal harus diautentifikasi keaslian, isi datanya, waktu pengiriman dan lain-lain.
3. Hak Akses terhadap suatu *file* atau fasilitas lain dalam sebuah sistem pemrosesan informasi masih dalam area lain dimana gagasan kriptografi telah diterapkan.

2.2.4 Tujuan Kriptografi

Kriptografi bertujuan untuk layanan keamanan yang memiliki beberapa aspek keamanan yang memiliki beberapa aspek keamanan, antara lain sebagai berikut (Rojali, 2014) :

1. *Confidelity* (kerahasiaan)

   layanan agar isi pesan yang dikirimkan tetaprahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima/pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
2. *Data integrity* (keutuhan data)

   layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
3. *Authentication* (keotentikan)

layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.

4. *Non-repudiation* (anti-penyangkalan)
   layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

2.2.5 Serangan Kriptografi

Tujuan utama kriptografi adalah untuk menjaga agar *plaintext* tetap aman dari para penyadap yang mencoba untuk mendapatkan informasi tentang *plaintext*. Kriptografi diharapkan dapat pula menjamin integritas pesan. Kriptanalisis merupakan ilmu yang mempelajari serangan kriptografi. Serangan terhadap kriptografi dikelompokan menjadi beberapa cara (Fithria, 2009) :

a. Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi atas dua macam, yaitu :
   1. Serangan pasif (*passive attack*) pada jenis serangan ini, penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima, namun penyerang menyadap semua pertukaran pesan antara kedua entitas tersebut. Tujuanya adalah untuk mendapatkan sebanyak mungkin informasi yang digunakan untuk kriptanalisis. Beberapa metode penyadapan antara lain :
      a. *Wiretapping* : penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambungan perangkat keras.
      b. *Electromagnetic eavesdropping* : penyadap mencegat data yang ditrasnmisikan melalui saluran *wireless*, misalnya radio dan *microwave*.
      c. *Acoustic eavesdropping* : menangkap gelombang suara yang dihasilkan oleh suara manusia.
   2. Serangan aktif (*active attack*), pada jenis serangan ini, penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya. Misalnya penyerang mengubah aliran pesan seperti menghapus sebagian *ciphertext*, mengubah *ciphertext*, menyisipkan

potongan *ciphertext* palsu, me-*replay* pesan lama, mengubah informasi yang tersimpan dan sebagainya.

b. Berdasarkan banyaknya informasi yang diketahui oleh kriptanalis, dikelompokan menjadi beberapa jenis (Hapsari, Perdana, & Risvelina, 2013).:
   1. *Ciphertext-only attack,* ini adalah jenis serangan yang paling umum namun paling sulit, karena informasi yang tersedia hanyalah *ciphertext* saja.
   2. *Known-plaintext attack,* ini adalah jenis serangan dimana kriptanalis memiliki pasangan *plaintext* dan *ciphertext* yang berkoresponden.
   3. *Chosen-plaintext attack,* serangan jenis ini lebih hebat dari pada *known-plaintext attack,* karena kriptanalis dapat memilih *plaintext* yang dimilikinya untuk di*enkripsi*kan, yaitu *plaintext-plaintext* yang lebih banyak dan banyak yang mengarahkan penemuan kekunci tersebut.
   4. *Chosen-ciphertext attack,* ini adalah jenis serangan dimana kriptanalis memilih *ciphertext* untuk diserang dan didekripsi*k*an dan memiliki *akses* ke *plaintext* hasil dekripsi.

c. Berdasarkan Teknik yang digunakan dalam menemukan kunci, serangan dibagi atas :
   1. *Exhaustive attack,* atau *bruforce attack* adalah serangan untuk mengungkap *plaintext* menggunakan semua kemungkinan kunci.
   2. *Analytical attack,* adalah serangan dengan menganalisis kelemahan algritma kriptografi untuk mengurangi kemungkinan kunci yang tidak mungkin ada.

2.2.6 Jenis Kriptografi

a. Kriptografi`Klasik

Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada kata terang (*plaintext*). Kriptografi ini hanya melakukan pengacakan pada huruf A-Z, dan

sangatlah tidak disarankan untuk mengamankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern (Hartini & Primaini, 2013)

b. Kriptografi Modern

Kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Pada kriptogarfi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern (Adisaputra, 2011) :

a. Algoritma *Simetris*

Algoritma *simetris* adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriprografi *simetris* sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriprografi *simetris* adalah waktu proses untuk enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci. Karena prosesnya cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi digital secara *real time*.

b. Algoritma *Asimetris*

Algoritma *Asimetris* adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi *deskripsi*. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia itu, yang dalam hal ini kunci rahasia untuk melakukan pembongkaran terhadap kode yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci *asimetris* adalah RSA (*Rivest, Shamir dan Adleman*).

2.2.7 Karakteristik Sistem Kriptografi

Di dalam kriptografi dapat dikarakteristikan berdasarkan:

1. Tipe operasi yang dipakai dalam enkripsi dan dekripsi.

a. Subtitusi: Elemen pada pesan seperti karakter, ditukar atau disubtitusikan dengan elemen lain dari ruang pesan. Misalkan subtitusi sederhana A ditukar B, B ditukar D, dan C ditukar Z, sehingga pesan "BACA" menjadi "DBZB".
b. Transposisi: Elemen pada pesan berpindah posisi, missal posisi 1 menjadi posisi 4 dan posisi 2 menjadi posisi 3, posisi 3 menjadi posisi 1, dan posisi 4 menjadi posisi 2, sehingga pada pesan "KAMI" menjadi "MAIK".Sistem kriptografi modern mencakup kedua operasi tersebut.

2. Tipe kunci yang dipakai.
   a. Kunci simetrik: Pada umumnya sistem kriptografi klasik dan beberapa sistem kriptografi modern menggunakan kunci yang sama pada sisi penyandi dan penyulih sandi, sistem kriptografi seperti ini disebut dengan kriptografi dengan kunci simetrik.
   b. Kunci asimetrik: Tahun 1976 sistem kriptografi yang membolehkan kunci yang tidak sama diusulkan oleh Whitfield Deffie dan Martin Hellman, (deffie & Hellman 1976). Sistem kriptografi seperti ini disebut dengan kriptografi dengan kunci asimetrik.
3. Tipe pengolahan pesan.
   a. *Block cipher:* Dalam penyandian pesan yang akan dienkripsi atau dekripsi diolah per-satuan blok elemen.
   b. *Stream cipher:* Dalam penyandian pesan yang akan dienkripsi ataupun didekripsi dianggap sebagai aliran elemen secara terus menerus.

2.2.7.1 Kunci Simetri

Kunci *simetri* jenis kriptografi yang paling umum dipergunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis. Siapapun yang memiliki kunci tersebut – termasuk pihak-pihak yang tidak diinginkan – dapat membuat dan membongkar rahasia *ciphertext*. Masalah yang paling jelas disini terkadang bukanlah masalah pengiriman *ciphertext*-nya, melainkan masalah bagaimana menyampaikan kunci *simetri* tersebut kepada pihak yang diinginkan. Contoh algoritma kunci *simetri* adalah

DES (*Data Encryption Standard*), RC-2, RC-4, RC-5, RC-6, *TwoFish, Rijndael, International* Data *Encryption* Algoritma (IDEA), *Advanced Encryption Standard* (AES), *One Time Pad* (OTP), dan lainnya.

Kelebihan kunci *simetri*:

a. Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma *asimetri.*
b. Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real-time.*

Kelemahan kunci *simetri*:

a. Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
b. Permasalahan dalam pengiriman kunci itu sendiri yang disebut *key distribution problem.*

2.2.7.2 Kunci Asimetri

Pada pertengahan tahun 70-an Whitfield Diffie dan Martin Hellman menemukan teknik enkripsi *asimetrik* yang merevolusi dunia kriptografi. Kunci *asimetrik* adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk enkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci *privat* untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.

Dengan cara seperti ini, jika Alia mengirim pesan untuk Yulius, Alia dapat merasa yakin bahwa pesan tersebut hanya dapat dibaca oleh Yulius, karena hanya Yulius yang bisa melakukan dekripsi dengan kunci *privat*. Tentunya Alia harus memiliki kunci *publik* Yulius untuk melakukan enkripsi. Alia bisa mendapatkannya dari Yulius, ataupun dari pihak ketiga seperti Annita.

Teknik enkripsi *asimetri* ini jauh lebih lambat daripada enkripsi dengan kunci *simetri.* Oleh karena itu, biasanya bukanlah pesan itu sendiri yang

disandikan dengan kunci *asimetri*, namun hanya kunci *simetri*lah yang disandikan dengan kunci *asimetri.* Sedangkan pesannya dikirim setelah disandikan dengan kunci *simetri* tadi. Contoh algoritma yang menggunakan kunci *asimetri* adalah *RSA* (merupakan singkatan penemunya yakni Rivest, Shamir dan Adleman), *Digital Signature Algorithm* (DSA), *Protokol Diffie-Hellman*, Kriptografi *Quantum, ElGamal*, dan *Pohlig-Hellman.*

Kelebihan kunci *asimetrik:*

a. Masalah keamanan pada distribusi kunci dapat lebih baik.
b. Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit.

Kelemahan kunci *asimetrik:*

a. Kecepatan yang lebih rendah bila dibandingkan dengan algoritma *simetrik.*
b. Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma *simetrik.*

2.2.8 One time Pad

One Time Pad (OTP) atau yang lebih dikenal dengan sebutan *Vernam Cipher* diciptakan oleh Mayor J. Maugborne dan G. Vernam pada tahun 1917. Algoritma *One Time Pad* (OTP) merupakan algoritma berjenis *symetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan mod 65 antara menjumlahkan *plaintext* dan *key.* proses enkripsi *one time pad* teks sandi dari suatu pesan diperoleh dengan menjumlahkan teks aslinya terhadap kunci. Sedangkan untuk mendapatkan kembali teks aslinya tersebut dilakukan pengurangan teks sandi terhadap kunci tersebut sebagai kebalikan dari proses menyandi. Atau dengan kata lain proses enkripsi data (Sholeh 2011).

Kriptografi *one-time pad* merupakan salah satu jenis teknik kriptografi yang menggunakan metode substitusi dengan cara memberikan syarat-syarat khusus terhadap kunci yang digunakan yaitu terbuat dari karakter atau huruf yang acak (kunci acak atau *pad*), dan pengacakannya tidak menggunakan rumus tertentu. Dengan kata lain *one time pad* adalah suatu sistem di mana suatu kunci

rahasia yang dibuat acak digunakan hanya sekali untuk melakukan enkripsi pesan yang kemudian di dekripsi lagi dengan kunci yang sama.

2.2.8.1 Sistem One Time Pad

Enkripsi Persamaan 2.1

Ci = (Pi + Ki) mod 65 …….. Persamaan 2.1

Sebagai contoh kalimat “AGUS” akan dilakukan proses enkripsi dengan menggunakan kunci “GSUS” :

Perhitungan :

(A + G) mod 65 = (65 + 71) mod 65 = 6 + 65 = G

(G + S) mod 65 = (71 + 83) mod 65 = 24 + 65 = Y

(U + U) mod 65 = (85 + 85) mod 65 = 40 + 65 = i

(S + S) mod 65 = (83 + 83) mod 65 = 36 + 65 = e

Jadi hasil dari enkripsi adalah : “GYie”

Keterangan :

- Ci : Ciphertext
- Pi : Plaintext
- Ki : Kunci

Dekripsi Persamaan 2.2

Pi = (Ci + Ki) mod 65 …….**.....** Persamaan 2.2

Selanjutnya adalah proses dekripsi dari karakter ”GYie” dengan menggunakan Kunci “GSUS”.

(G - G) mod 65 = (71 - 71) mod 65 = (0 + 65) = A

(Y - S) mod 65 = (89 - 83) mod 65 = (6 + 65) = G

(i - U) mod 65 = (105 - 85) mod 65 = (20 + 65) = U

(e - S) mod 65 = (101 - 83) mod 65 = (18 + 65) = S

Keterangan :

- Pi : Plaintext
- Ci : Ciphertext
- Ki : Kunci