BAB II

TINJAUAN PUSTAKA

II.1.PenelitianTerdahulu

Penelitian sebelumnya yang terkait dengan penelitian ini adalah penelitian yang dilakukan oleh Munawar, (2012) yang berjudul "Perancangan Algoritma Sistem Keamanan Data Dengan Menggunkan Metode Kriptografi Asimetri" membahas tentang sistem enkripsi dan dekripsi menggunakan dua kunci. Algoritma yang dipakai adalah algoritma Kriptografi Asimetri, hal yang mendasar pada metode ini yaitu penggunaan kunci untuk enkripsi yang berbeda dengan kunci yang digunakan untuk dekripsi. Kunci enkripsi diberitahukan kepada umum dan disebut kunci publik (*public key*). Kunci dekripsi dijaga kerahasiaannya, dan hanya diketahui oleh pemilik sebagai penerima data disebut sebagai kunci pribadi (*private key*). Kedua kunci tersebut memiliki hubungan yang matematis oleh karena itu disebut juga sistem asimetris. Pada penelitian tersebut membahas tentang algoritma Kriptografi Asimetri yang memiliki tingkat keamanan relatif baik namun kecepatan prosesnya rendah, selain itu terdapat dua kali pembesaran ukuran dari file *plaintext*, ini merupakan kelebihan dan kekurangan. Adapun penelitian dengan judul "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File, Dokumen, Dan File Dokumen Menggunakan Algoritma *Advaced Encriyption Standard*" AES digunakan untuk enkripsi file dokumen dan gambar.

Berdasarkan penelitian yang pernah dilakukan tentang penerapan algoritma *One Time Pad* dan *Scytale* maka akan dilakukan penelitian tentang

Implementasi Modifikasi Kriptografi *One Time Pad* (*OTP*) untuk Pengamanan Data *File*. Berdasarkan pada penelitian sebelumnya, penelitian yang diangkat pada skripsi ini dengan judul "Implementasi Enkripsi dan Dekripsi Dokumen Menggunakan Metode *One Time Pad* Dan Metode *Scytale*", *One Time Pad* yang digunakan untuk enksripsi file dokumen. Hasil enkripsi yaitu *chipertext* akan disimpan oleh aplikasi *One Time Pad* dan *Scytale* yang dibuat.

II.2. Kriptografi

Kriptografi **(***Cryptography)* adalah cabang ilmu matematika tentang persandian untuk menjaga keamanan data. *Cryptographic system* atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan *plaintext* ke *ciphertext* dan sebaliknya. *Plaintext* adalah data asli, data yang masih bisa dibaca dan dimengerti. Sedangkan *ciphertext* adalah data yang tidak bisa dibaca maupun dimengerti (Munawar, 2012).

Setiap *cryptosytem* yang baik harus memiliki karakteristik sebagai berikut :

a. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
b. *Cryptosystem* yang baik memiliki ruang kunci (*keyspace*) yang besar.
c. *Cryptosystem* yang baik akan menghasilkan *ciphertext* yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.

II.2.1. Sejarah Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher*) dan algoritma substitusi (*substitution cipher*). *Cipher* transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan *cipher* substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain (Pabokory, dkk, 2015).

II.2.2. Tujuan kriptografi

Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk member layanan keamanan. Yang dinamakan aspek-aspek keamanan:

1. Kerahasiaan (*confidentiality*) Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data (*data integrity*) Adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi (*authentication*) Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak- pihak yang berkomunikasi (*user autehentication*).
4. *Non-repudiation* Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan.

Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah *plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *ciphertext* (teks sandi). Di dalam kriptografi kita akan sering menemukan berbagai istilah atau *terminology*.

Beberapa istilah yang harus diketahui yaitu :

1. 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 (*cleartext*).

2. 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.

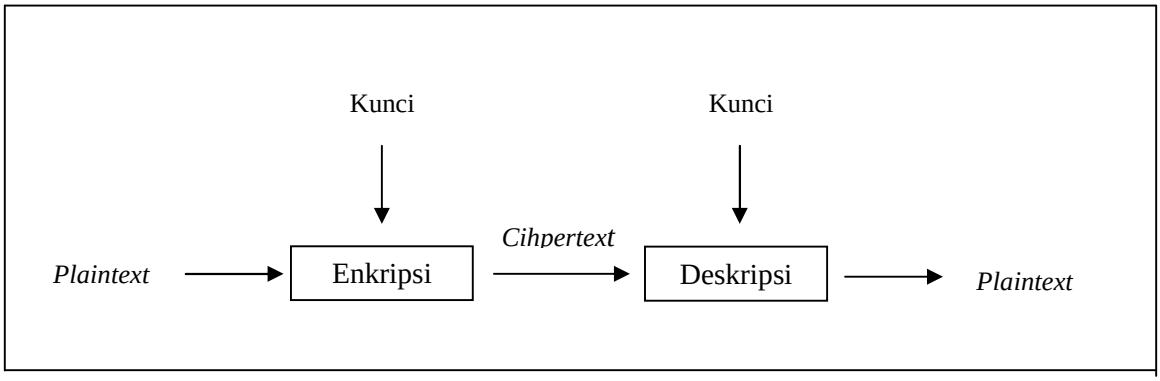
3. Enkripsi dan dekripsi

Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering* (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* semula disebut dekripsi (*decryption*) atau *deciphering* (*standard* nama menurut ISO 7498-2).

4. *Cipher* dan kunci

Algoritma kriptogarfi 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 enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen *plaintext* dan himpunan yang berisi *ciphertext*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut. Misalkan *P* menyatakan *plaintext* dan *C* menyatakan*ciphertext*, maka : $E(P) = C \rightarrow$ fungsi enkripsi *E* memetakan *P* ke *C* $D(C) = P \rightarrow$ fungsi dekripsi *D* memetakan *C* ke *P* Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka persamaan $D(E(P)) = P$ harus benar.

Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaannya. Kunci (*key*) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa *string* atau deretan bilangan. Dengan menggunakan kunci *K*, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai skema diperlihatkan pada Gambar.II.1.(Pabokory, dkk,2015).



Gambar II.1 : Skema Enkripsi dan Deskripsi dengan menggunakan kunci
(Sumber : Pabokory, dkk,2015)

II.2.3. Komponen Kriptografi

Pada dasarnya, kriptografi terdiri dari beberapa komponen sebagai berikut:

1. Algoritma, merupakan himpunan aturan matematis yang digunakan dalam enkripsi dan dekripsi.
2. Enkripsi, adalah transformasi data ke dalam bentuk yang tidak dapat terbaca tanpa sebuah kunci tertentu.
3. Dekripsi, merupakan kebalikan dari enkripsi, yaitu transformasi data terenkripsi kembali ke bentuknya semula.
4. Kunci (*Key*), digunakan pada saat melakukan enkripsi dan dekripsi. Pada kriptografi modern, keamanan enkripsi tergantung pada kunci, dan tidak tergantung kepada algoritmanya apakah dilihat orang lain atau tidak.
5. Diproses menggunakan algoritma kriptografi tertentu untuk menjadi *ciphertext*.
6. *Ciphertext*, merupakan pesan yang telah melalui proses enkripsi yang merupakan himpunan karakter acak.

7. Kriptologi, merupakan studi tentang kriptografi dan kriptanalisis.
8. Kriptanalisis(*Cryptanalysist*), merupakan aksi memecahkan mekanisme kriptografi dengan cara menganalisisnya untuk menemukan kelemahan dari suatu algoritma kriptografi sehingga akhirnya dapat ditemukan kunci atau teks asli.
9. Kriptosistem, adalah perangkat keras atau implementasi perangkat lunak kriptografi yang diperlukan dalam mentransformasi sebuah pesan asli menjadi *ciphertext* dan juga sebaliknya.

II.2.4. Enkripsi

Enkripsi adalah suatu proses mengubah pesan atau data menjadi sandi yang merupakan salah satu proses dari kriptografi. Data yang disandikan berupa file sebagai *input* dan dengan menggunakan suatu kunci, file tersebut diubah menjadi file enkripsi yang tidak bisa dibaca. Adapun tujuan dari enkripsi ini adalah menyembunyikan data atau informasi dari orang tidak berhak (Munawar, 2012).

II.2.5. Dekripsi

Dekripsi adalah proses sebaliknya dari enkripsi yaitu mengembalikan sandi-sandi atau informasi yang telah dilacak ke bentuk file aslinya dengan menggunakan kunci pula (Munawar, 2012).

II.3. Algoritma *One Time Pad*

Dalam kriptografi dikenal beberapa algoritma, diantaranya adalah algoritma *One Time Pad (OTP). O/7ne Time Pad* adalah salah satu metode kriptografi dengan algoritma jenis simetri. Ditemukan pada tahun 1917 oleh *Major Yoseph Mouborgne dan Gilbert Vernam* pada perang dunia ke dua. Metode ini telah diklaim sebagai satu-satunya algoritma kriptografi sempurna yang tidak dapat dipecahkan. Suatu algoritma dikatakan aman, apabila tidak ada cara untuk menemukan *plaintext*-nya. Sampai saat ini, hanya algoritma *One Time Pad* (OTP) yang dinyatakan tidak dapat dipecahkan meskipun diberikan sumber daya yang tidak terbatas. (Febryan, 2014).

Dalam proses enkripsi *One Time Pad*, *ciphertext* diperoleh dengan melakukan penjumlahan *modulo* 26 dari satu *bit plaintext* dengan satu *bit* kunci.

Seperti terlihat pada Rumus:

$$C_{i=}(P_i + K_i) \bmod 256$$

Dimana :

Ci = *ciphertext*

Pi = *plaintext*

Ki = kunci

II.3.1. Proses Enkripsi dan Dekripsi

Prinsip enkripsi pada algoritma ini adalah dengan mengkombinasikan masing-masing karakter pada *plaintext* dengan satu karakter pada kunci. Oleh

karena itu, panjang kunci harus sama dengan panjang *plaintext*. Enkripsi dapat dinyatakan sebagai penjumlahan *modulo* 256 (menggunakan kode ASCII 8 *bit*) dari satu karakter *plaintext* dengan satu karakter kunci OTP :

$$ci = (pi + ki) \bmod 256$$

Dalam hal ini, *pi* adalah *plaintext* ke-I, ki adalah kunci ke-I, dan *ci* adalah huruf *ciphertext* ke-i. Panjang kunci sama dengan panjang *plaintext*, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi. Setelah pengirim mengenkripsikan pesan dengan kunci, ia menghancurkan kunci tersebut. Penerimaan pesan menggunakan kunci yang sama untuk mendekripsikan karakter- karakter *ciphertext* menjadi karakter-karakter *plaintext* dengan persamaan:

$$pi = (ci - ki) \bmod 256$$

Kelebihan dari algoritma *One Time Pad* adalah sistem *One Time Pad* tidak dapat dipecahkan, karena:

1. Barisan kunci acak yang ditambahkan ke pesan *plaintext* yang tidak acak menghasilkan *ciphertext* yang seluruhnya acak.
2. Beberapa barisan kunci yang digunakan untuk mendekripsi *ciphertext* mungkin menghasilkan pesan-pesan *plaintext* yang mempunyai makna, sehingga kriptanalis tidak punya cara untuk menentukan *plaintext* mana yang benar.

Sedangkan *bit shifting* adalah operasi yang dilakukan pada semua *bit* dari nilai biner di mana mereka dipindahkan oleh sejumlah tempat-tempat yang ditentukan ke kiri ataupun ke kanan. *Bit shifting* digunakan ketika operan sedang digunakan sebagai rangkaian *bit* daripada sebagai keseluruhannya. Dengan kata lain, operan diperlakukan sebagai *bit* individu yang berdiri sebagai sesuatu hal dan bukan sebagai suatu nilai. *Bit shifting* sering digunakan dalam pemrograman dan memiliki setidaknya satu variasi dalam setiap bahasa pemrograman. *Bit shifting* mungkin juga dikenal sebagai operasi *bitwise*.

Ada dua variasi *bit shifting*, bergeser ke kanan dan bergeser ke kiri, dan itu lebih ditentukan oleh jumlah tempat di mana pergeseran harus terjadi. Sebagai contoh, menggeser operan satu nilai ke kiri atau menggeser *bit* sebesar “n” ke kanan. Ada juga dua jenis *bit shifting*, *logical* dan *arithmetics*. *Logical bit shifting* mungkin berguna untuk mengalikan atau membagi *integer* tidak bertanda dengan dua. Misalnya, jika nilai "0001" atau "1" digeser kiri, akan menjadi "0010" atau "2", digeser ke kiri lagi menjadi "0100" atau "4". Pergeseran ke kanan memiliki efek berlawanan dari membagi nilai dengan dua tiap pergeseran. Dalam kebanyakan kasus, pergeseran diberlakukan secara melingkar sehingga ketika bergeser ke kiri, nilai paling kiri menjadi nilai paling kanan, dan sebaliknya (Febryan, dkk, 2014).

Prinsip enkripsi pada algoritma ini adalah dengan mengkombinasikan masing-masing karakter pada *plaintext* dengan satu karakter pada kunci. Oleh karena itu, panjang kunci setidaknya harus sama dengan panjang *plaintext*. Enkripsi dapat dinyatakan sebagai penjumlahan *modulo* 26 dari satu karakter

plaintext dengan satu karakter kunci OTP:

ci = (pi + ki) mod 26

Dalam hal ini, pi adalah *plaintext* ke-i, dan ci adalah huruf *ciphertext* ke-i. Panjang kunci sama dengan panjang *plaintext*, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi. Setelah pengirim mengenkripsikan pesan dengan kunci, ia menghancurkan kunci tersebut. Penerimaan pesan menggunakan kunci yang sama untuk mendekripsikan karakter-karakter *ciphertext* menjadi karakter-karakter *plaintext* dengan persamaan:

pi = (ci + ki) mod 26

Angka 26 muncul karena sistemnya menggunakan abjad. Artinya hanya abjad A Z saja yang dapat dikodekan dengan sistem seperti ini. Bila diinginkan pengkodean sembarang data, baik teks, gambar, suara maupun video, maka OTP ini diperluas dengan penggunaan sistem bilangan biner. Semua tipe data dapat dianggap sebagai data biner. Dan karena bilangan biner hanya mengenal 0 dan 1, maka basis 26 diubah menjadi basis 2. Penjumlahan *modulo* 2 ini dinyatakan dengan XOR. Dan inilah yang sering digunakan dalam sistem digital sekarang ini. *Ciphertext* diperoleh dengan melakukan penjumlahan *modulo* 2 satu *bit plaintext* dengan satu *bit* kunci:

ci = (pi + ki) mod 2

Dalam hal ini, pi : *bit plaintext*, ki : *bit* kunci, ci : *bit ciphertext*. *Plaintext* diperoleh dengan melakukan penjumlahan *modulo* 2 satu *bit chipertext* dengan satu *bit* kunci:

pi = (ci + ki) mod 2

Mengingat operasi penjumlahan *modulo* 2 identik dengan operasi *bit* dengan operator XOR, maka persamaan enkripsi dapat ditulis sebagai:

ci = pi ki

dan proses dekripsi menggunakan persamaan:

pi = ci ki

Pada proses chipering, *bit* hanya mempunyai dua buah nilai, sehingga proses enkripsi hanya menyebabkan dua keadaan pada *bit* tersebut, berubah atau tidak berubah. Dua keadaan tersebut ditentukan oleh kunci enkripsi yang disebut aliran kunci *(keystream).* Aliran kunci dibangkitkan dari sebuah pembangkit yang dinamakan pembangkit aliran kunci (*keystream generator*) (Sugianto, Teguh Yuniarto, 2014).

Aliran kunci di-XOR-kan dengan aliran *bit- bit plaintext* p1, p2, ..., pi, untuk menghasilkan aliran *bit-bit ciphertext*:

ci = pi ki

Disisi penerima, *bit-bit ciphertext* di-XOR-kan dengan aliran kunci yang sama untuk menghasilkan *bit-bit plaintext*:

pi = ci ki

karena proses enkripsi dua kali berturut-turut menghasilkan kembali *plaintext* semula.

ci ki = (pi ki) ki = pi (ki ki) = pi 0 = pi

II.4. Algoritma *Scytale*

Dalam kriptografi, sebuah sa*bit* (sajak dengan Italia, dan juga ditransliterasikan sebagai *scytale*, dalam bahasa Yunani, tongkat) adalah alat yang digunakan untuk melakukan cipher transposisi, yang terdiri dari sebuah silinder dengan potongan kulit yang mengelilinginya dimana ada pesan tertulis. Orang-orang Yunani kuno dan Spartan secara khusus, menggunakan sandi ini untuk berkomunikasi selama kampanye militsaidary. Penerima menggunakan batang dengan diameter yang sama di mana ia membungkus kertas untuk membaca pesan. Ini memiliki keuntungan menjadi cepat dan tidak rentan terhadap kesalahan, properti yang diperlukan saat berada di medan perang. Hanya si penerima yang tahu ukuran grid, baris dan Nomor kolom bisa mengambil pesan tersembunyi. Di Untuk meningkatkan tingkat kerahasiaan pesan Dapat dienkripsi menggunakan beberapa algoritma enkripsi seperti AES dan teks sandi serta kuncinya bisa jadi Diatur dengan cara yang berbeda menggunakan dua grid yang berbeda (Farhan Khan, dkk) .

Algoritma *Scytale* Merupakan salah satu algoritma tradisional, yang menggunakan media perkamen atau kain yang dililitkan ke sebuah batang atau stik kayu. Digunakan untuk mengirimkan pesan yang terenkripsi. Harus diketahui besarnya keliling dari batang atau stik kayu yang menjadi media penulisan untuk dijadikan acuan proses enkripsi. Proses enkripsi dimulai dengan melilitkan media tulis pada batang, dan kemudian menuliskan pesan asli baris demi baris secara mendatar. Ketika lilitan media tulis dilepaskan dari batang, maka akan didapatkan hasil enkripsi Proses enkripsi dimulai dengan melilitkan media tulis pada batang,

dan kemudian menuliskan pesan asli baris demi baris secara mendatar. (Yusuf Triyuswoyo ST, dkk; 2014).

Ketika lilitan media tulis dilepaskan dari batang, maka akan didapatkan hasil enkripsi. Contohnya:

Isi pesan : saya mahasiswa gunadarma

Penulisan pada batang :

S A Y A M A H A

S I S W A G U N

A D A R M A X X

Hasil enkripsi menjadi :

SSAAIDYSAAWRMAMAGAHUXANX