# BAB II

# TINJAUAN PUSTAKA

## II.1. Analisis

Pengertian analisis diartikan sebagai penguraian suatu pokok atas berbagai penelahan bagian itu sendiri, serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan. Analisis juga merapakan suatu kegiatan berfikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu.

Dari pendapat data diatas dapat disimpulkan bahwa analisis atau analisa adalah kegiatan berfikir untuk menguraikan suatu pokok hal menjadi bagian-bagian atau komponen sehingga dapat diketahui ciri atau tanda tiap bagian, kemudian hubungan satu sama lain serta fungsi masing-masing bagian dari keseluruhan.

## II.2. Perancangan

Menurut (Insap Santoso, 2009) salah satu kriteria penting dari sebuah antarmuka adalah tampilan yang menarik. Ada pepatah yang mengatakan " cinta pada pandangan pertama". Jika pepatah ini dikaitkan dengan sebuah antarmuka, maka tampilan yang dihadapi oleh penggunalah yang pertama kali akan menarik perhatian pengguna untuk mengoperasikannya.

Dokumentasi rancangan dapat dikerjakan atau dilakukan dengan beberapa cara yaitu:

1. Membuat sketsa pada kertas
2. Menggunakan puranti purwarupa GUI
3. Menuliskan keterangan yang menjelaskan tentang kaitan antara satu jendela dengan jendela yang lain.
4. Menggunakan peranti bantu yang disebut CASE *(Computer-Aided-Software-Engineering)*, (Insap Santoso, 2009).

Kadang-kadang teknik tersebut dianggap sebagai teknik yang saling bersaing, tetapi seringkali untuk beberapa jenis proyek tertentu diperlukan kombinasi dari beberapa diantaranya sehingga saling melengkapi satu sama lain.

## II.3. Keamanan Data.

Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan adalah data yang bersifat rahasia, dimana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan.

Untuk mendapatkan informasi didalamnya, biasanya dilakukan berbagai cara yang tidak sah. Terjadi banyak pertukaran informasi setiap detiknya di internet. Juga banyak terjadi pencurian atas informasi oieh pihak-pihak yang tidak bertanggungjawab.

Ancaman keamanan yang terjadi terhadap informasi adalah:

1. *Interruption* : menapakan ancaman terhadap *availability* informasi, data yang ada dalam sistem komputer dirusak atau dihapus sehingga jika data atau informasi tersebut dibutuhkan maka pemiliknya akan mengalami kesulitan untuk mengaksesnya, bahkan mungkin informasi itu hilang,
2. *Interception* : merupakan ancaman terhadap kerahasiaan *(secrecy).* Informasi disadap sehingga orang yang tidak berhak dapat mengakses komputer di mana informasi tersebut disimpan.
3. *Modification :* merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu-lintas informasi yang sedang dikirim, dan kemudian mengubahnya sesuai keinginan orang tersebut.
4. *Fabrication* : merupakan ancaman terhadap integritas. Orang tidak berhak berhasil meniru atau memasulkan sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi, (Dony Ariyus, 2010).

Agar dapat mengamankan system computer dengan benar kita harus tahu karekteristik penganggu yang mungkin akan mendatangi sistem komputer kita. Hal lain yang perlu kita ingat adalah bahwa semakin aman sistem yang kita gunakan, sistem komputer kita akan menjadi semakin merepotkan.

Kata aman dapat didefenisikan sebagai terhindar dari serangan atau kegagalan. Sistem keamanan komputer digunakan untuk menjamin agar sumber daya tidak digunakan atau dimodifikasi orang yang tidak diotorisasi. Pengamanan

termasuk masalah teknis, manajerial, legalitas dan politis. Keamanan system terbagi menjadi tiga yaitu :

1. Keamanan eksternal adalah pengamanan yang berhubungan dengan fasilitas computer dari penyusup dan bencana, misalnya bencana alam.
2. Keamanan interface pemakai, berkaitan dengan identifikasi pemakai sebelum diijinkan mengakses program dan data yang tersimpan dalam sistem.
3. Keamanan internal, berkaitan dengan beragam pengamanan yang dibangun pada perangkat keras dan system operasi untuk menjamin operasi yang handal untuk menjaga keutuhan program serta data. (Janner, 2006).

## II.4. Algoritma

Ditinjau dari asal usul katanya, kata algoritma sendiri mempunyai sejarah yang aneh. Orang hanya menemukan kata algorism yang berarti proses menghitung dengan angka arab. Anda dikatakan algorist jika anda menggunakan. dengan angka arab. Para ahli bahasa berusaha menemukan asal kata ini namun hasilnya kurang memuaskan. Akhirnya para ahli sejarah matematika menemukan asal kata tersebut yang berasal dari penulis buku arab yang terkenal yaitu Abu Ja'far Muhammad Ibnu Musa Al-Khuwarizmi menulis buku yang berjudul Kitab Aljabar Walmuqabala yang artinya "buku pemugaran dan pengurangan "*(The book off restoration and reduction*).

Dari judul buku itu kita juga memperoleh akar kata "Aljabar" *(Algebro)*

perabahan dari kata algorism menjadi algorithm muncul karena kata algorism sering dikelirukan dengan arithmetic, sehingga akhiran-sm berubah menjadi thm. Karena perhitungan dengan angka arab sudah menjadi ha yang bisa, maka lambat laut kata algorithm berangsur-angsur dipakai sebagai metode perhitungan (komputasi) secara umum, sehingga kehilangan makna kata aslinya. Dalam bahasa Indonesia, kata algorithm diserap menjadi algoritma. "Algoritma adalah urutan langka-langka logis penyelesaian masalah yang disusun secara sistematik dan logis". Kata logis merupakan kata kunci dalam algoritma. Langkah-langkah dalam algoritma haras logis dan haras dapat ditentukan bernilai salah atau benar.

Alogaritma kriptografi merupakan fungsi sistematis yang digunakan untuk proses enkripsi dan deskripsi. Alogaritma kritografi ini bekerja dalam kombinasi dengan menggunakan kunci *(key)* seperti kata, nomor atau frase tertentu. (Janner, 2006).

## II.5. Algoritma Transposisi

Seperti yang telah dijelaskan pada bagian sebelumnya, algoritma kriptografi klasik jenis transposisi bekerja dengan cara mengubah susunan karakter dalam pesan yang dienkripsi. Terdapat banyak cara/aturan dalam mengubah susunan karakter itu, namun sesuai bagian ini akan membahas tiga jenis utama metode transposisi, yaitu:

1. Transposisi grup
2. Transposisi serial

3. Transposisi kolom/baris

### II.5.1. Transposisi Grup

Pada metode ini, plainteks dibagi ke dalam blok-blok/grup yang ukurannya sama. Kemudian, kepada setiap blok pesan ini diaplikasikan suatu susunan karakter yang telah didefinisikan. Misalkan sebuah susunan karakter didefinisikan pada sebuah grup karakter yang panjangnya delapan, sebagai "mengumpulkan dan menguratkan karakter bernomor prima dan diikuti sisanya". Maka hasil permutasinya (II) ialah II = c2, c3, c5, c7, cl, c4, c6, c8 dengan en adalah karakter ke-n dalam blok karakter.

Misalkan plainteksnya adalah "TOLONG PERMUTASIKAN PESAN INI YA", maka langkah pertama ialah mengelompokkan plainteks itu ke dalam blok-blok yang panjangnya delapan karakter, sebagai berikut (spasi diperhitungkan)

```
TOLONG P
ERMUTASI
KAN PESA
N INI YA
```

Langkah berikutnya, aturan permutasi yang telah ada (II), diterapkan ke masing-masing blok pesan, menjadi

```
OLN TOGP
RMTSEUAI
ANPSK EA
```

IIYNN A

Terakhir, blok-blok pesan itu disatukan kembali menjadi cipherteks yang utuh:

OLN TOGPRMTSEUAIANPSK EA IIYNN A

Bila jumlah karakter dalam plainteks bukan kelipatan dari panjang II, maka pada akhir pesan dapat ditambahkan *(padding)* karakterkarakter *dummy*. Selain itu, terdapat alternative lain dalam metode ini, diantaranya dengan membuang spasi.

### II.5.2. Transposisi Serial

Metode ini mengelompokkan seluruh karakter plainteks ke dalam beberapa grup dengan aturan tertentu, kemudian cipherteks disusun dengan menyatukan gnxp-grup tersebut secara berurutan (serial). Misalkan sebuah plainteks P terdiri atas 20 karakter, yakni

plp2p3p4p5p6p7p8p9pl0pllpl2pl3pl

4pl5pl6pl7pl8pl9p20

Kemudian didefmisikan tiga grup secara berturut-turut: grup bilangan kelipatan 4, grup bilangan ganjil, dan grup sisa sebagai berikut

Gl = p4p8pl2pl6p20

G2 = plp3p5p7p9pllpl3pl5pl7pl9

G3 = p2p6pl0pl4pl8

Maka, cipherteks C akan memiliki susunan

C = G1G2G3

= p4p8pl2pl6p20plp3p5p7p9pll

pl3pl5pl7pl9p2p6pl0pl4pl8

### II.5.3. Transposisi Kolom / Baris

Dasar dari metode ini ialah menuliskan plainteks dalam beberapa baris, kemudian cipherteks diperoleh dengan cara membacanya kolom per kolom (karakter). Berikut ialah ilustrasi dari teknik ini.

Plainteks:

INI MIRIP OPERASI TRANSPOSE

PADA MATRIKS

ditulis dalam 4 bans dan spasi dihilangkan

INIMIRIPO

PERASITRA

NSPOSEPAD

AMATRIKS

kemudian dibaca kolom per kolom menjadi

IPNA NESM IRPA MAOT ISSR RIEI

ITPK PRAS OAD

Dari metode dasar tersebut, banyak variasi yang dapat dikembangkan. Salah satunya ialah melakukan pertukaran kolom dengan memanfaatkan kunci. Misalkan teknik ini akan dilakukan pada contoh sebelumnya. Karena ada sembilan kolom, maka kunci yang digunakan panjangnya sembilan karakter.

Misalkan kuncinya ialah TRANSPOSE, maka

Kunci: T R A N S P O S E

Teks : I N I M I R I P O

P E R A S I T R A

N S P O S E P A D

A M A T R I K S

Pertukaran kolom dilakukan dengan cara mengurutkan karakter-karakter pada kunci menjadi

Kunci: A E N O P R S S T

Teks : I O M I R N I P I

R A A T I E S R P

P D O P E S S A N

A T K I M R S A

kemudian dibaca kolom per kolom menjadi

IRPA OAD MAOT ITPK RIEI NESM

ISSR PRAS IPNA

Teknik-teknik di atas juga dapat dilakukan secara terbalik: mulai dengan plainteks yang menurun dalam kolom-kolom, kemudian membuat cipherteks dengan membacanya baris per baris. Selain itu, struktur transposisi juga tidak terbatas pada matriks (baris, kolom). Berikut ini ialah contoh transposisi yang memiliki struktur 'zig-zag'.

Plainteks: SULIT SEKALI MEMBACA

TEKS INI

Disusun menjadi

S T A E C K I

U I S K L M M A A E S N

L E I B T I

Dibaca per baris menjadi

STAECKI UISKLMMAAESN

LEIBTI

## II.6. *Vigenere Cipher*

*Vigenere Cipher* adalah salah satu algoritma kriptografi klasik yang tergolong ke dalam algoritma substitusi. Secara lebih spesifik, *Vigenere Cipher* termasuk *pofyalphabetical substitution cipher* (cipher abjad-majemuk). Secara praktis hal ini berarti sebuah karakter di dalam plainteks dapat dienkripsi menjadi karakter yang berbeda pada setiap kemunculannya. Lawan dari jenis cipher ini ialah *monoalphabetical substitution cipher,* dimana suatu karakter plainteks pasti dienkripsi menjadi suatu karakter yang sama pada setiap kemunculannya. Lebih lanjut, *Vigenere Cipher* adalah cipher yang bersifat periodik. Artinya, proses enkripsi terhadap keseluruhan plainteks mengikuti periode tertentu, yang besarnya sama dengan panjang kunci yang digunakan. Dengan kata lain, terjadi periodisasi kunci terhadap plainteks.

Sifat *polyalphabetic* yang dimiliki oleh *Vigenere Cipher* diimplementasikan dengan menggunakan Bujursangkar *Vigenere,* sedangkan sifat periodik diwujudkan dengan cara menuliskan kunci yang digunakan secara berulang-ulang sampai sepanjang plainteks, kemudian memadankan setiap karakter ke-n dari plainteks dengan karakter ke-n *di* rangkaian perulangan kunci, dengan bernilai dari 1 sampai panjang plainteks.

Prosedur enkripsi pada *Vigenere Cipher* dapat dijelaskan melalui contoh sebagai berikut.

Plainteks: CONTOH ENKRIPSI VIGENERE

Kunci: coba

Langkah 1 : Hilangkan spasi dari plainteks

CONTOHENKRIPSIVIGENERE

Langkah 2 : Tuliskan kunci secara periodik

CONTOHENKRIPSIVIGENERE

cobacobacobacobacobaco

Langkah 3 : Enkripsikan setiap karakter plainteks dengan karakter kunci yang berpadanan, menggunakan Bujursangkar *Vigenere*. Caranya, cari perpotongan antara baris karakter kunci dengan kolom karakter plainteks. Jadi, untuk karakter keempat misalnya, cari perpotongan antara baris a dan kolom T. Karakter yang merupakan perpotongan baris dan kolom menjadi substitusi dari karakter plainteks yang bersangkutan. Dengan mengulangi langkah ini untuk setiap karakter plainteks, maka didapatkan cipherteks ECOTQVFNMFJPUWWIISOETS

Selain menggunakan Bujursangkar *Vigenere*, langkah ketiga dapat dilakukan dengan menggunakan rumus

|Cn|=(|Pn| + |Kn|) mod 26

Dengan

|Cn|: representasi numerik dari karakter

cipherteks ke-n

|Pn|: representasi numerik dari karakter

plainteks ke-n

|Kn|: representasi numerik dari karakter

kunci (yang berulang) ke-n

n : (1..jumlah karakter plainteks)

**II.7 Definisi Kriptografi**

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan *(Cryptography is the art and science of keeping messages secure)* selain itu ada pengertian tentang kriptografi yaitu kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kata "seni" di dalam definisi *di* atas maksudnya adalah mempunyai cara yang unik untuk merahasiakan pesan.

Defenisi lainnya adalah kriptografi berasal dari bahasa yunani, yaitu dari kata *crypto* dan *graphia* yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yan disebut cryptology. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung di dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yag tidak sah. (Janner, 2006).

Saat ini, kriptografi memainkan peranan yang sangat penting di dunia, khususnya dalam bidang teknologi informasi. Ketika komputerisasi merambah hampir semua bidang kehidupan, kriptografi turut serta. Namun demikian, sejarah kriptografi ternyata jauh lebih panjang daripada sejarah komputer. Dengan kata

lain, peradaban lebih dahulu mengenal kriptografi daripada komputer.

Berdasarkan fakta ini, secara umum kriptografi, atau secara lebih khusus algoritma kriptografi, dibagi ke dalam dua golongan besar : klasik dan modern. Algoritma kriptografi klasik merupakan kumpulan berbagai teknik kriptografi yang ditemukan manusia sebelum ditemukannya komputer. Aplikasi teknik kriptografi ini secara umum dilakukan dengan pena dan kertas, serta menyandikan suatu dokumen huruf demi huruf (berbasis karakter). Setelah computer diciptakan, kriptografi mulai diaplikasikan menggunakan komputer. Kumpulan teknik kriptografi baru ini yang dinamakan algoritma kriptografi modern. Karena berbasis komputer, maka ia bekerja mengikuti mekanisme kerja komputer, yakni (umumnya) melakukan penyandian bit per bit. Meski terdapat perbedaan yang cukup signifikan di antara kedua golongan itu, temyata algoritma kriptografi modern tetap memiliki landasan konsep yang berasal dari algoritma kriptografi klasik.

Algoritma kriptografi klasik dibagi menjadi dua jenis yakni algoritma substitusi dan algoritma transposisi. Sesuai namanya, algoritma substitusi menyembunyikan isi pesan/dokumen dengan cara mengganti karakter-karakter yang menyusun pesan/dokumen tersebut, menurut aturan tertentu. Variasi aturan substitusi ini melahirkan berbagai jenis algoritma spesifik, yang biasanya dinamai menurut penemunya. Beberapa contoh algoritma substitusi diantaranya Algoritma Caesar, Algoritma Vigenere, dan Algoritma Affine. Namun, biasanya yang lebihsering dipakai sebagai sebutan bukanlah algoritmanya melainkan hasil dari algoritma kriptografi tersebut yakni *cipher* (pesan yang telah tersandikan).

Jadi, contoh-contoh sebelumnya akan diacu sebagai *Caesar Cipher, Vigenere Cipher,* dan *Affine Cipher.*

Jenis algoritma kriptografi klasik yang kedua ialah algoritma berbasis transposisi. Cara kerja algoritma ini ialah dengan mengubah susunan/urutan karakter-karakter di dalam dokumen. Pada umumnya hal ini dilakukan dengan cara menuliskan plainteks dengan pola tertentu, kemudian dibaca menggunakan pola / aturan yang berbeda sehingga dihasilkan suatu cipherteks. Contoh teknik transposisi yang cukup populer dalam sejarah kriptografi adalah *scytale* yang berasal dari zaman Romawi Kuno. *Scytale* ialah sebuah silinder dengan diameter tertentu. Sebuah pita kertas dililitkan ke silinder tersebut, kemudian pesan ditulis ke pita dalam arah sejajar poros silinder. Pita kemudian diurai dari silinder sehingga huruf-huruf dalam pesan mengalami transposisi.

## II.8. Sejarah Kriptografi

Kriptografi mempunyai sejarah yang panjang. Informasi yang lengkap mengenai sejarah kriptografi dapat di temukan di dalam buku David Kahn yang berjudul *The Codebreakers.* Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari penggunakaan kriptografi oleh bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* yang tidak standar pada piramid) hingga penggunaan kriptografi pada abat ke-20.secara historis ada empat kelompok orang yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelejen dan mata-mata), kalangan

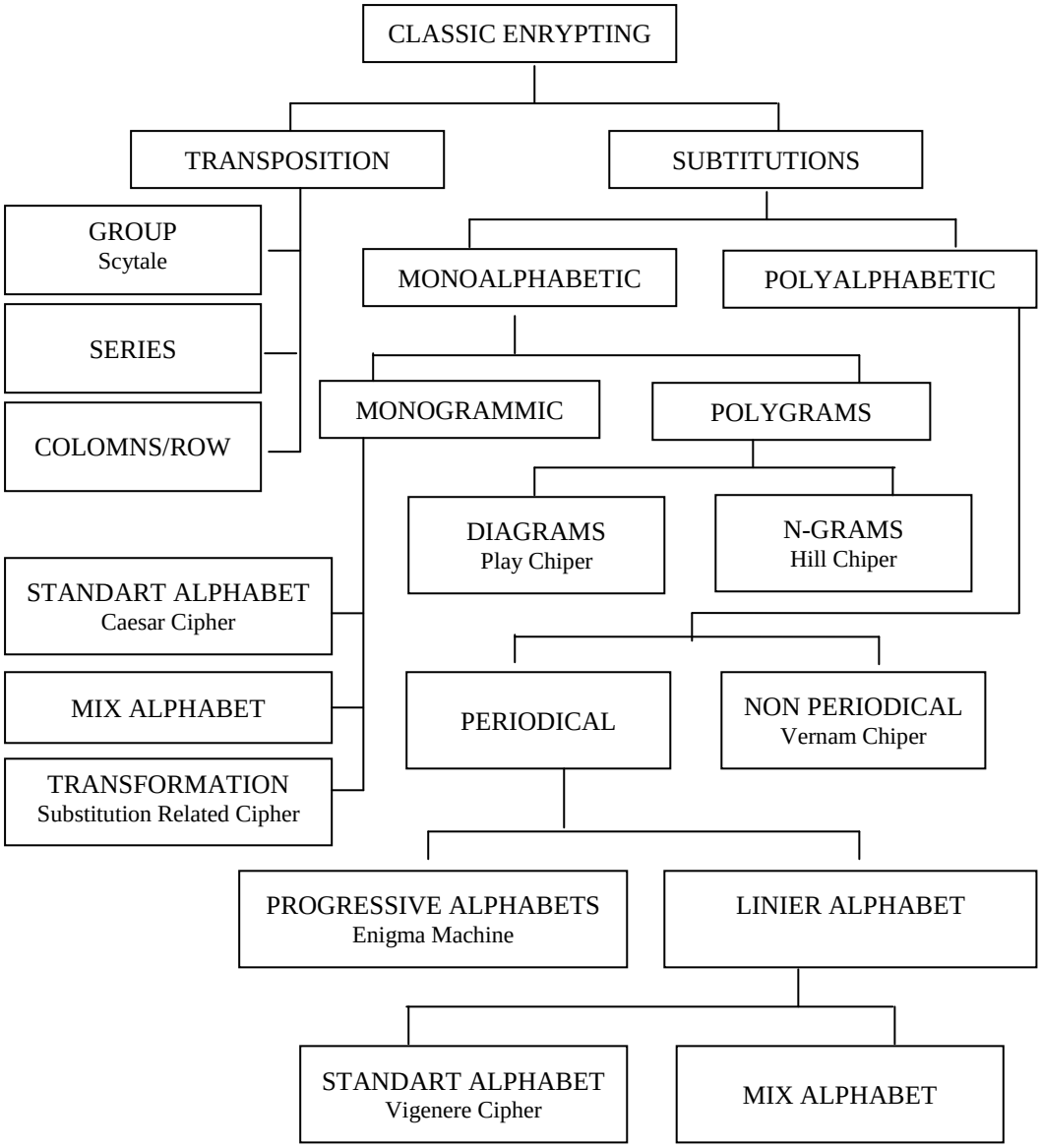
*diplomatic*, penulis buku harian, dan pencinta *(lovers).* Diantara ke-empat kelompok ini, kalangan militer yang memberikan kontribusi paling penting karena pengiriman pesan didalam suasana perang membutuhkan teknik enkripsi dan deskripsi yang rumit. Kriptografi juga digunakan Untuk tujuan keamanan.

Kalangan gereja pada masa awal agama Kristen menggunakan kriptografi untuk menjaga tulisan *religious* dan gangguan otoritas politik atau budaya yang dominan saat itu. Mungkin yang sangat terkenal adalah "Angka si Buruk Rupa" *(Number of the beast)* di dalam kitab perjanjian baru. Angka "666" menyatakan cara kriptografi (yaitu dienskripsi) untuk menyembunyikan pesan berbahaya; para ahli percaya bahwa pesan tersebut mengacu pada kerajaan Romawi.

Kriptografi modern dipicu oleh perkembangan peralatan komputer digital. Dengan komputer *digital, cipher* yg lebih kompleks menjadi sangat mungkin untuk dapat dihasilkan. Tidak seperti kriptografi klasik yang mengenskripsi karakter per karakter (dengan menggunakan *alphabet* tradisionil), kriptografi *modern* beroperasi pada *string biner. Cipher* yang kompleks seperti *DES (Data Encryption Standard)* dan penemuan algoritma *RSA* adalah algoritma kriptografi *modern* yang paling dikenal di dalam sejarah kriptografi *modern.* Kriptografi *modern* tidak hanya berkaitan dengan teknik menjaga kerahasiaan pesan, tetapi juga melahirkan konsep seperti tanda -tangan *digital* dan sertifikasi *digital.* Dengan kata lain, kriptografi modern tidak hanya memberikan aspek keamanan *confidentiality*, tetapi juga aspek keamanan lain seperti otentikasi, integritas data, dan penyangkalan (Munir, 2006).

Skema yang cukup lengkap mengenai klasifikasi algoritma kriptografi

klasik dapat dilihat pada Gambar II.1.




Gambar II.1 Klasifikasi Algoritma Kriptografi klasik

## II.9. Tujuan Kriptografi

Menurut (Janner, 2006) Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi, yaitu:

a. *Convidentiality* (kerahasiaan), yaitu memberikan kerahasiaan pesan

dan menyimpan data dengan menyembunyikan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi.

b. *Message intergrity* (integritas data), yaitu memberikan jaminan bahwa dari setiap bagian tidak mengalami perubahan dari saat data dibuat/ dikirim sampai dengan saat data tersebut di buka.
c. *Non-repudiation* (nirpenyangkalan), yang memberikan cara untuk membuktikan bahwa suatu dokumen dating dari setiap seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.
d. *Auntentication* (autentikasi), yang memberikan dua layanan. Yang pertama mengidentifikasi keaslian dari suatu pesan dan memberikan jaminan keotentikannya. Kedua, untuk menguji identitas seseorang apabila ia akan memasuki sebuah sistem.

## II.10 Kriptografi Klasik Dan Kriptografi *Modern*

### II.10.1.Kriptografi Klasik

Sebelum komputer ada kriptografi dilakukan dengan algoritma berbasis karakter. Algoritma yang digunakan termasuk ke dalam sistem kriptografi simetri dan digunakan jauh sebelum sistem kriptografi kunci *public* ditemukan. Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi (sehingga dinamakan algoritma kriptografi klasik), namun sekarang algoritma tersebut sudah usang karena sangat mudah dipecahkan (Munir, 2006).

Tiga alasan mempelajari algoritma kriptografi klasik, yaitu:

1) Untuk memberikan pemahaman konsep dasar kriptografi.
2) Dasar dari algoritma kriptografi *modern.* 14
3) Dapat memahami potensi-potensi kelemahan sistem *chiper.*

**II.10.2. Kriptografi Modern**

Algoritma kriptografi *modern* umumnya beroperasi dalam *mode bit* ketimbang *mode* karakter (seperti yang dilakukan pada *cipher* substitusi atau *cipher* transposisi dari algoritma kriptografi klasik) (Munir, 2006). Operasi dalam *mode bit* berarti semua data dan informasi (baik kunci, *plainteks*, maupun *cipherteks)* dinyatakan dalam rangkaian *(string) bit biner*, 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian *bit.* Rangkaian *bit* yang menyatakan *plainteks* dienkripsi menjadi *cipherteks* dalam bentuk rangkaian *bit,* demikian sebaliknya Enkripsi *modern* berbeda dengan enkripsi konvensional. Karena enkripsi *modern* sudah menggunkan komputer untuk pengoperasiannya. Berfungsi untuk mengamankan data baik yang di *transfer* melalui jaringan komputer maupun yang bukan. Hal ini sangat berguna untuk melindungi *privacy data, integrity, authentication* dan *non-repudiation.* Perkembangan algoritma kriptografi *modern* berbasis *bit* didorong oleh penggunaan komputer *digital* yang merepresentasikan data dalam bentuk *biner* Kriptografi *modern* merapakan 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* terdiri dari dua jenis

1) Algoritma Simetris

Algoritma simetris adalah 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 relatif cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi *digital* secara *real time* seperti *GSM.*

2) 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* (merupakan singkatan dari nama penemunya, yakni *Rivest, Shamir* dan *Adleman).*

## II.11 Algoritma Kriptografi dengan Teknik Transposisi

Algoritma Kriptografi transposisi ini merupakan algoritma yang cukup sederhana dalam dunia enkripsi data dan merupakan salah satu algoritma yang belum modern (klasik). Algoritma transposisi ini kalau gak salah ceritanya dulu ada seorang yang mau menuliskan pesan rahasia ke raja. Pesan rahasia itu akan dikirim lewat telik sandi (jaman dahulu belum ada komputer, apalagi Internet :hammer:). Akhirnya sang pengirim itu mempunyai akal yaitu dia menuliskan pesan rahasia tersebut dengan cara menggulung terlebih dahulu dengan menggunakan bambu sebagai porosnya. Kertasnya lalu ditulisi pesan rahasia secara vertikal. Setelah selesai menulis pesan tersebut, maka kertas tadi dicopot lagi gulungannya, dan terjadilah tulisan yang acak-acakkan. Tulisan inilah yang nantinya akan dikirim oleh telik sandi.

## II.12 Metode Penyandian Transposisi

Kriptografi klasik adalah kriptografi yang dipakai pada jaman dulu. Bentuk penyandiannya berupa teks (huruf) dengan menggunakan alat tulis berupa kertas dan pensil, namun bila menggunakan mesin sandi, biasanya mesin tersebut masih sangat sederhana.

Kriptografi klasik terbagi menjadi dua kategori utama, yaitu metode penyandian transposisi dan metode penvandian substitusi.

Metode penyandian transposisi adalah metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Dan untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut

berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati.

Terdapat beberapa algoritma dalam metode penyandian transposisi yaitu :

1. **Penyandian Transposisi *Rail Fence***

*Rail Fence* atau bias disebut alur pagar adalah bentuk penyandian transposisi dengan cara menuliskan huruf-huruf teks asli secara turun naik dalam sebuah pagar imajiner. Teks sandinya dibaca secara baris per baris.

Teks pesan asli :

TENTUKAN PRIORITAS ANDA SEBAB KITA TIDAK DAPAT MENGERJAKAN SEMUANYA X.

Proses :

T - - - - - - - P - - - - - - - S - - - - - - A - - - -

- E - - - - - N – R - - - - - A – A - - - - - B – B - - -

- -N - - -A - - -I - - -T - - -N - - -E - - - K - -

- - - T – K - - - - - O – I - - - - - D – S - - - - - - I –

- - - - U - - - - - - - R - - - - - - - A - - - - - - - T – DST

Hasil penyandian (teks sandi):

TPSAD MKNEN RAABB IATEA AAYNA ITNEK TKANJ NUATK

OIDSI ADPGR SMXUR ATAEE

2. **Penyandian Transposisi *Route***

Penyandian transposisi dengan metode *route* hamper sama dengan metode *Rail Fence*. Penyandian Transposisi Route dilakukan dengan cara menuliskan teks asli secara kolom dari atas ke bawah dalam sebuah kisi-kisi imajiner dengan ukuran yang telah disepakati. Teks sandinya dibaca dengan dengan arah (route)

sesuai perjanjian, misalnya dibaca secara (1) spiral dengan arah jarum jam, mulai dari kiri atas atau (2) secara ular tangga, mulai dari kanan bawah dan lain-lain cara pembacaannya.

Penyandian *route* memiliki banyak sekali variasi algoritma pembacaan teks-nya. Namun tidak semua algoritma tersebut memberikan hasil teks sandi yang memenuhi standar "aman". Beberapa algoritma tidak mengacak teks asli dengan sempurna, sehingga akan memberikan celah yang dapat dengan mudah dipecahkan oleh seorang kriptoanalisa. Penyandian transposisi *route* yang terkenal adalah *Union Route* yang digunakan oleh tentara Amerika selama perang sipil.

Contoh penyandian transposisi *route* :

Teks pesan asli :

TENTUKAN PRIORITAS ANDA SEBAB KITA TIDAK DAPAT

MENGERJAKAN SEMUANYA X.

Algoritma : 5 baris, spiral arah jarum jam mulai dari kanan bawah.

Proses:

T K I A A B T D M R N A

E A O S S K I A E J S N

N N R A E I D P N A E Y

T P I N B T A A G K M A

URTDAAKTEAUX

Hasil penyandian (teks sandi):

XUAET KAADT RUTNE TKIAA BTDMR NANYA MKGAA TBNIP

NAOSS KIAEJ SEANP DIEAR

### 3. Penyandian Transposisi Kolom

Penyandian Transposisi Kolom dituliskan secara baris (biasa) dengan panjang yang telah ditentukan sebagai kunci-nya. Teks sandi-nya dibaca secara kolom demi kolom dengan pengacakan melaiui permutasian angka kuncinya. Panjang baris dan permutasian kolomnya disebut sebagai "kata kunci".

Dalam prosesnya, kata kunci tersebut didefmisikan dahulu dengan angka sesuai urutan abjad. Sedangkan proses untuk mengembalikan ke teks sandi ke teks aslinya dilakukan langkah kebalikan darinya. Lebih mudahnya dapat dilihat dalam contoh berikut :

Teks pesan asli:

TENTUKAN PRIORITAS ANDA SEBAB KITA TIDAK DAPAT

MENGERJAKAN SEMUANYA X.

Kata kunci: PELIKAN yang berarti 7 kolom

Proses :

PELIKAN didefinisikan sesuai urutan abjad menjadi 7 2 5 3 4 1 6

7 2 5 3 4 1 6

T E N T U K A

N P R I O R I

T A S A N D A

S E B A B K I

T A T I D A K

D A P A T M E

N G E R J A K

A N S E M U A

N Y A X

Hasil penyandian (teks sandi):

KRDKA MAUEP AEAAG NYTIA AIARE XUONB DTJMN RSBTP

ESAAI AIKEK ATNTS TDNAN

**4. Penyandian Transposisi Ganda**

Penyandian transposisi ganda adalah metode penyandian transposisi kolom yang dilakukan dua kali. Dua kali proses penyandian ini dilakukan untuk mempersulit upaya pemecahan teks sandi transposisi kolom yang biasanya dapat dengan mudah dilakukan dengan metode anagram. Proses penyandian yang kedua ini bisa menggunakan kunci yang sama atau dua kunci yang berbeda.

Sebagai contoh ditetapkan kunci kedua yang berbeda yaitu GERHANA; terhadap teks sandi pertama : KRDKA MAUEP AEAAG NYTIA AIARE

XUONB DTJMN RSBTP ESAAI AIKEK ATNTS TDNAN

Proses:

GERHANA didefinisikan sesuai urutan abjad menjadi 4 3 7 5 1 6 2

4 3 7 5 1 6 2

K R D K A M A

U E P A E A A

G N Y T I A A

I A R E X U O

N B D T J M N

R S B T P E S

A A I A I K E

K A T N T S T

D N A N

Hasil penyandian (teks sandi):

AEIXJ PITAA AONSE TRENA BSAAN KUGIN RAKDK ATETT

ANNMA AUMEK SDPYR  DBITA

Selama perang dunia I dan II, metode penyandian transposisi ganda ini digunakan oleh beberapa negara sebagai metode penyandian terhadap pesan-pesan rahasia yang dikomunikasikan.

**5. Penyandian Transposisi Myszkows**

Emile Victor Theodore Myszkowski di tahun 1902 memperkenalkan variasi dari metode penyandian transposisi kolom, yang dibedakan dalam pendefinisian dan permutasian kata kunci-nya.

Dalam metode penyandian transposisi kolom, kata kunci misalnya BOROBUDUR di definisikan menjadi 1 4 6 5 2 8 3 9 7; sedangkan dalam metode Myszkowski menjadi 1 3 4 3 1 5 2 5 4

Teks sandinya dibaca secara urutan nomor kolom, bila nomor urut kolomnya sama dibaca secara bersamaan dimulai dari sebelah kiri.

Lebih mudahnya dapat dilihat dalam contoh berikut:

Teks pesan asli:

TENTUKAN PRIORITAS ANDA  SEBAB  KITA  TIDAK  DAPAT

MENGERJAKAN SEMUANYA X.

Kata kunci: BOROBUDUR yang berarti 9 kolom

Proses:

BOROBUDUR didefinisikan sesuai urutan abjad menjadi 1 3 4 3 1 5 2 5 4

1 3 4 3 1 5 2 5 4

T E N T U K A N P

R I O R I T A S A

N D A S E B A B K

I T A T I D A K D

A P A T M E N G E

R J A K A N S E M

U A N Y A X

Hasil penyandian (teks sandi):

TURIN EIIAM RAUAA AAANS ETERD STTPT JKNYN POAAK

ADAEA MNKNT SBBDK EGNEX

Untuk mempersulit pemecahan sandi oleh para kriptoanalisa, maka biasanya metode penyandian transposisi dikombinasikan dengan metode penyandian substitusi.

## II.13 Penelitian Sebelumnya

Agar penelitian ini dapat di pertanggung jawabkan secara akademis, maka penelitian akan menampilkan penelitian yang telah dilakukan oleh penelitian terdahulu sebagai berikut: Pada penelitian I Putu Herryawan yang berjudul

"Analisa Dan Penerapan Algoritma DES Untuk Pengamanan Data Gambar Dan Vidio" dijelaskan bahwa Sistem pada keamanan data dan kerahasiaan data merupakan salah satu aspekpenting dalam perkembangan kemajuan teknologi informasi namun yang cukup disayangkan adalah ketidakseimbangan antara setiap perkembangan suatu teknologi yang tidak diiringi dengan perkembangan pada sistem keamanannya itu sendiri, dengan demikian cukup banyak sistem-sistem yang masih lemah dan haras ditingkatkan keamanannya. Oleh karena itu pengamanan data yang sifatnya rahasia haruslah benar-benar diperhatikan.Untuk mengatasi masalah tersebut maka diperlukan suatu aplikasi pengamanan data yang dapat mencegah dan mengamankan data-data yang kita miliki dari orang-orang yang tidak berhak mengaksesnya. Salah satunya adalah metode algoritma kriptografi simteris, karena algoritma ini menggunakan kunci yang sama pada saat melakukan proses enkripsi dan dekripsi sehingga data yang kita miliki akan sulit untuk dimengerti maknanya dan untuk proses enkripsi data yang sangat besar akan sangat cepat. Algoritma kriptografi (cipher) yang digunakan adalah DES.

Sedangkan pada penelitian Deni Mustopa "Perancangan Program Keamanan Data Dengan Menggabungkan Algoritma Kriptografi DES dan Mars" dijelaskan Kriptografi merupakan bidang pengetahuan yang mengunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu, untuk tujuan agar informasi yang disimpan tidak dapat terbaca oleh siapa pun kecuali orang-orang yang berhak.Dalam tugas akhir ini akan disajikan analisis algoritma kriptografi DES dan MARS yang mana kedua algoritma tersebut merupakan

algoritma kriptografi simetris. Tugas akhir ini pula menampilkan implementasi program dan menampilkan bagaimana cara mengenkripsi dan mendekripsi dengan kedua algoritma tersebut.