PENERAPAN MATRIX PERSEGI PANJANG (4X2) DALAM PENGEMBANGAN ALGORITMA HILL CHIPER

Disusun dan Diajukan untuk Memenuhi Persyaratan Ujian Akhir Memperoleh
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH

NAMA	: ALI WARDHANA
NPM	: 1524370969
PROGRAM STUDI	: SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

Ali Wardhana

**PENERAPAN MATRIX PERSEGI PANJANG (4x2)
DALAM PENGEMBANGAN ALGORITMA HILL CHIPER
2019**

Kriptografi sebagai salah satu cabang ilmu yang dapat digunakan untuk mengamankan data hingga saat ini terus dikembangkan melalui berbagai algoritma. Beberapa penelitian terkait mengenai kriptografi masih mengguankan media berupa teks saja, image saja, maupun file tertentu saja. Pada penelitian ini akan digunakan media berupa seluruh jenis file sebagai media inputan. Adapun algoritma yang digunakan yaitu Hill cipher dan Bit shiffting. Kedua algoritma ini dikenal cepat, mudah dan aman untuk digunakan. Percobaan yang dilakukan menggunakan file notepad serta telah diuji melalui aplikasi yang dibangun dengan Visual Studio 2010 telah menghasilkan proses enkripsi dan dekripsi data yang berjalan dengan baik. File hasil enkripsi dapat dibuka dengan kunci yang telah ditetapkan dan tidak mengalami kerusakan, dan sebaliknya untuk proses dekripsi data juga demikian.

Kata Kunci: File, Hill Cipher, Kriptografi

KATA PENGANTAR

Puji dan syukur kehadirat Allah SWT, atas limpahan rahmat, karunia, taufik serta hidayah-Nya, sehingga penulis dapat menyelesikan skripsi dengan judul : **"PENERAPAN MATRIX PERSEGI PANJANG (4X2) DALAM PENGEMBANGAN ALGORITMA HILL CHIPER"**.

Skripsi ini disusun dan diajukan sebagai salah satu syarat untuk menempuh ujian akhir memperoleh gelar Sarjana Komputer Pada Fakultas Ilmu Komputer Universitas Pembangunan Panca Budi. Penulis menyadari bahwa dalam penulisan skripsi ini banyak menemukan kesulitan-kesulitan dan kekurangan pada penulisan. Namun berkat bantuan dan bimbingan, petunjuk serta nasehat dari berbagai pihak akhirnya penulis dapat menyelesaikan dengan baik.

Oleh karena itu dengan segenap kerendahan hati pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Allah SWT yang selalu melancarkan segala aktivitas yang penulis lakukan.
2. Istri dan putra putri penulis yang selalu memberikan motivasi dalam menyelesaikan skripsi ini tepat waktu.
3. Bapak Firdaus, SE selaku Kepala Dinas Penanaman Modal Pelayanan Perijinan Terpadu Satu Pintu Kota Subulussalam dan seluruh staff di jajaran DPMP2TSP yang tidak dapat penulis sebutkan satu persatu yang telah memberikan kesempatan untuk melanjutkan pendidikan dengan memberikan ijin kepada penulis untuk menyelesaikan pendidikan S1 Komputer dan memberikan keluangan waktu kepada penulis dengan ijin dijam dinas kantor.

4. Bapak Dr. H. Muhammad Isa Indrawan, S.E., M.M, selaku Rektor Universitas Pembangunan Panca Budi Medan.
5. Ibu Sri Shindy Indira. ST, M.S.C selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Panca Budi Medan.
6. Bapak DR Muhammad Iqbal, S.Kom., M.Kom selaku Ketua Program Studi Sistem Komputer Fakultas Ilmu Komputer Universitas Pembangunan Panca Budi Medan.
7. Bapak Hafni, S.Kom.,M.Kom selaku pembimbing I dan Bapak Khairul, S.Kom.,M.Kom selaku pembimbing II yang telah meluangkan waktu dan pemikirannya dalam membimbing penulis menyelesaikan skripsi ini.
8. Semua pihak yang telah membantu dalam penyelesaian skripsi ini yang tidak bisa saya sebutkan satu persatu.

Semoga segala bantuan yang telah diberikan kepada penulis menjadi amalan yang akan mendapatkan balasan dari Allah SWT.

Meskipun telah disusun, namun penulis menyadari bahwa isi dan tehnik penulisan skripsi ini masih jauh dari sempurna baik dari segi tata bahasa maupun materi yang terkandung di dalamnya. Untuk itu penulis berharap kritik dan saran yang bersifat membangun dari semua pihak demi kesempurnaan Skripsi ini. Semoga Skripsi ini bermanfaat bagi kita semua.

Medan, September 2018
Penulis,

Ali Wardhana
NPM. 1524370969

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

Judul Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan data dan informasi merupakan hal yang sangat penting di era informasi saat ini. Umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh diakses oleh orang tertentu. Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasian dokumen-dokumen tersebut. Namun kendalanya bahwa media-media yang digunakan sering kali dapat disadap oleh pihak lain. Oleh karena itu, diperlukan metode untuk mengamankannya, salah satunya dengan menggunakan metode *kriptografi*.

Oleh karena itu *kriptografi* muncul sebagai ilmu atau seni untuk menjaga keamanan pesan-pesan tersebut saat dikirimkan ke tujuan. Dengan harapan pesan-pesan tersebut dapat sampai ke tujuan tanpa ada yang dapat membuka atau memecahkan pesan-pesan tersebut kecuali si pengirim dan penerima.

Kriptografi digunakan sebagai alat untuk menjamin keamanan dan kerahasiaan informasi. Kriptografi adalah suatu ilmu dan seni untuk mengubah pesan yang dapat dimengerti menjadi bahasa yang tidak dapat dipahami dan kemudian mengubah kembali pesan itu kembali ke bentuk aslinya (Acharya, 2009). Salah satu algoritma kriptografi adalah algoritma Hill Cipher yaitu

penerapan aritmatika modulo kriptografi yang menggunakan sebuah matriks persegi sebagai kunci. Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja (Munir, 2006).

Pada penelitian yang terdahulu meyimpulkan pada enkripsi file dengan Algoritma Hill Cipher terdapat perbedaan ukuran file asli dengan file yang terenkripsi, dimana file yang terenkripsi akan lebih besar ukuran file-nya dibandingkan dengan ukuran file aslinya (Widodo, 2016). Hal ini disebabkan karena teknik enkripsi Hill Cipher ini menggunakan teknik dengan membagi setiap karakter yang akan dienkripsi sesuai dengan jumlah matriks kunci yang digunakan. Jika terjadi pengurangan karakter ataupun bit, akan dilakukan penambahan karakter sembarang sampai sesuai dengan jumlah matriks kunci tersebut (Sihombing, 2014).

Adanya penambahan ukuran file setelah dilakukan penyandian dengan Hill Cipher dapat menghambat pengiriman data dan membutuhkan ruang penyimpanan yang lebih besar. Oleh karena itu, dilakukan kompresi data yaitu teknik untuk mengurangi ukuran data agar penyimpanannya jauh lebih padat dan juga untuk mengurangi waktu pengiriman data tersebut (Budiman & Rachmawati, 2017). Kompresi data bertujuan untuk mengurangi jumlah bit yang digunakan untuk menyimpan atau mengirimkan informasi (Gailly, 1995).

Dari pemaparan di atas, maka dilakukan penelitian dengan judul "**Penerapan Matrix Persegi Panjang Dalam Pengembangan Algoritma Hill Chiper**".

1.2 Rumusan Masalah

Sesuai dengan latar belakang yang dipaparkan, maka masalah yang akan dibahas adalah sebagai berikut:

a. Bagaimana menerapkan algoritma *Hill cipher* yang di implementasikan pada *Three-pass protocol?*
b. Bagaimana menerapkan algoritma *Three-pass protocol* dalam penyandian pesan?

1.3 Batasan Masalah

Adapun batasan masalah yang dibatasi dari penulisan skripsi ini adalah sebagai berikut:

a. Pada proses penyandian pesan, pesan yang dikirimkan hanya berupa teks tidak angka, simbol.
b. Pada proses penyandian pesan yang menggunakan file dengan ekstensi *.*txt* atau notepad.
c. Pada proses penyandian pesan, kunci yang digunakan hanya berupa angka.
d. Aplikasi yang digunakan dalam pembuatan program adalah Visual Basic .Net 2010
e. Implementasi berupa *Enkripsi* dan *Deskripsi* pesan saja.

1.4 Tujuan Penelitian

Adapun manfaat yang dapat diambil dari penulisan skripsi ini adalah sebagai berikut:

a. Dapat menerapkankan algoritma *Hill cipher*.
b. Dapat menerapkan algoritma *Hill cipher* dalam penyandian pesan.
c. Menambah pengetahuan di bidang *kriptografi*.
d. Mengetahui proses enkripsi dan deskripsi.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diambil dari penulisan skripsi ini adalah sebagai berikut:

a. Memudahkan pengguna dalam penyimpanan data pada media penyimpanan yang relatif rendahdan memberikan pengamanan data untuk pengguna.
b. Memberikan penjelasan tentang *Hill cipher* dalam proses penyandian pesan.
c. Menjadi bahan referensi bagi penelitian lain yang memiliki keterkaitan topik

BAB II

LANDASAN TEORI

2.1 Aplikasi

Aplikasi adalah alat bantu untuk mempermudah dan mempercepat proses pekerjaan dan bukan merupakan beban bagi para penggunanya, atau aplikasi adalah satu unit perangkat lunak yang dibuat untuk melayani kebutuhan akan beberapa aktivitas seperti sistem perniagaan, *game*, pelayanan masyarakat, periklanan, atau semua proses yang hampir dilakukan manusia. Aplikasi berguna untuk melakukan pengolahan data maupun kegiatan-kegiatan seperti pembuatan dokumen atau pengolahan data Aplikasi adalah bagian PC yang berinteraksi langsung dengan *user*. Aplikasi berjalan di atas sistem operasi, sehingga agar aplikasi bisa diaktifkan perlu melakukan instalasi sistem operasi terlebih dahulu.

2.2 Kriptografi

a. Pengertian kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti secret (rahasia) dan *graphia* berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Dalam perkembangannya, *kriptografi* juga digunakan untuk mengidentifikasi pengiriman pesan dan tanda tangan digital dan keaslian pesan dengan sidik jari digital. (*Dony Ariyus, 2005*)

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau terminology. Beberapa istilah yang harus diketahui yaitu :

1. Pesan, plaintext, dan cipherteks

   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas (*cleartext*). 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 cipherteks atau kriptogram. Cipherteks harus dapat ditransformasikan kembali menjadi plaintext semula agar dapat diterima dan bisa dibaca.

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. 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 cipherteks.

3. Enkripsi dan dekripsi

   Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan

cipherteks menjadi plainteks disebut dekripsi (*decryption*) atau *deciphering*.

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 *enciphering* dan *deciphering*.

   Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen – elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen- elemen antara dua himpunan tersebut. Misalkan P menyatakan plainteks dan C menyatakan cipherteks, maka fungsi enkripsi E memetakan P ke C.

   $E(P) = C$

   Dan fungsi dekripsi D memetakan C ke P

   $D(C) = P$

   Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan semula, maka kesamaan berikut harus benar,

   $D(E(P)) = P$

   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 *enciphering* dan *deciphering*.

Kunci biasanya berupa string atau deretan bilangan. Dengan menggunakan K, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai :

$E_K(P)=C$ *dan* $D_K(C)=P$

Dan kedua fungsi ini memenuhi

$D_K(E_K(P))=P$

Keterangan :

P = plainteks

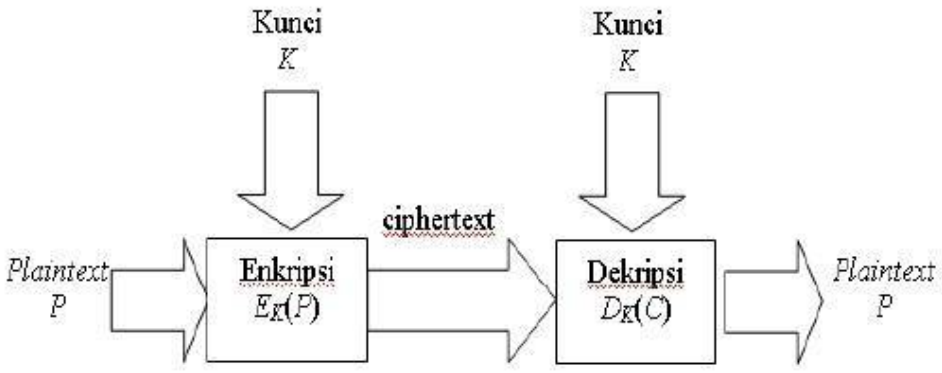
C = cipherteks

K = kunci

EK = proses enkripsi menggunakan kunci *K*

DK = proses dekripsi menggunakan kunci *K*

Skema enkripsi dengan menggunakan kunci diperlihatkan pada gambar dibawah ini :



Gambar 1. Skema enkripsi dan dekripsi dengan menggunakan kunci

Gambar di atas menjelaskan bahwa Plaintext (tulisan asli) disandikan menggunakan kunci sehingga muncul sebagai ciphertext. Kemudian tulisan dideskripsikan untuk mendapatkan tulisan asli atau Plaintext.

5. Sistem kriptografi

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

6. Penyadap

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

7. Kriptanalisis dan kriptologi

   Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. *Kriptanalisis* (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Jika seorang kriptografer (*cryptographer*) mentransformasikan plainteks menjadi cipherteks dengan suatu

algoritma dan kunci maka sebaliknya seorang kriptanalis berusaha untuk memecahkan cipherteks tersebut untuk menemukan plainteks atau kunci. Kriptologi (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis.

b. Tujuan kriptografi

Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk memberi layanan keamanan. Yang dinamakan aspek – aspek keamanan sebagai berikut :

1. Kerahasiaan (*confidentiality*)

   Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak – pihak yang tidak berhak. Di dalam kriptografi layanan ini direalisasikan dengan menyandikan plainteks menjadi cipherteks. Misalnya pesan “harap datang pukul 8” disandikan menjadi “trxC#45motyptre!%”. istilah lain yang senada dengan confidentiality adalah *secrecy* dan *privacy*.

2. Integritas data (*data integrity*)

   Adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: “ apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?”.

3. Otentikasi (*authentication*)

Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak – pihak yang berkomunikasi (*user autehentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sember pesan.

4. *Non-Repudiation*

   Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

c. Hill Cipher

Hil Cipher termasuk dalam salah satu kripto sistem polialfabetik, artinya setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter alfabet. Cipher tersebut ditemukan pada tahun 1929 oleh Lester S. Hill. Ide dari Hill Cipher adalah misalkan m adalah bilangan bulat positif, Dengan cara mengambil m kombinasi linier dari m karakter alfabet dalam satu elemen plaintext.

Misalkan m=2, maka dapat ditulis suatu elemen plaintext sebagai x = (x1, x2) dan suatu elemen ciphertext sebagai y = (y1, y2). Disini (y1, y2) adalah kombinasi linier dari x1 dan x2. Misalkan:

y1 = 11x1 + 3X2

y2 = 8x1 + 7X2

Sehingga dapat dituliskan kedalam bentuk matrik sebagai berikut:

$$(y_1, y_2) = (x_1, x_2)\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

Secara umum, algoritma Hill Cipher akan menggunakan matrik K m x m sebagai kunci untuk mengacak pesannya. Jika elemen pada baris i dan kolom j dari matriks Kij, maka dapat dituliskan sebagai berikut:

$$(y_1, y_2, \ldots\ldots, y_m) = (x_1, x_2, \ldots\ldots, x_m)\begin{bmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{bmatrix}$$

Dikatakan bahwa ciphertext diperoleh dari plaintext dengan cara transformasi linier. Untuk melakukan dekripsi, akan digunakan matrik invers K-1. Jadi, dekripsi dilakukan jika matrik tersebut memiliki nilai invers dengan rumus:

x = yK-1

1. Perkalian matrik memiliki sifat asosiatif, yaitu (AB)C = A(BC).

2. Matriks invers dari A adalah A-1 dimana AA-1 = A-1A = Im.

3. Matrik identitas m x m yang ditulis dengan Im , adalah matrik yang berisi 1 pada diagonal utama dan berisi 0 pada elemen lainnya.

Contoh matrik identitas 2 x 2:

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Im disebut dengan matrik identitas karena: AIm = A untuk sembarang matrik I x m dan ImB = B untuk sembarang matrik m x n.

Dengan menggunakan sifat-sifat matrik diatas, maka

$$y = xK$$
$$yK^{-1} = (xK)K^{-1} = x(KK^{-1}) = x\,\mathrm{Im} = x$$

Sebagai contoh gambaran dari enkripsi Hill Cipher adalah sebagai berikut:

Misalkan kunci yang dipakai adalah matrik dengan ordo 2 x 2 dengan nilai

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

dari perhitungan diatas diperoleh:

$$K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

misalkan ingin mengenkripsi plaintext JULY, disini akan memiliki 2 elemen plaintext untuk dienkripsi:

-(9,20) JU

-(11,24) LY

dimana nilai tersebut diperoleh dari tabel penyandian 2.1.

Tabel Penyandian 2.1

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Kemudian dilakukan perhitungan sebagai berikut:

$$(9,20)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99-60,\ 72+140) = (3,4) \rightarrow DE$$
$$(11,24)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (121-72,\ 88+168) = (11,22) \rightarrow LW$$

hasil tersebut didapat dari perkalian dengan kunci matriks, yang kemudian di modulus 26, karena enkripsi ini bekerja pada modulus 26 agar bisa

diperoleh nilai dari 0 sampai dengan 25. Sehingga enkripsi untuk JULY adalah DELW. (Dony Ariyus:34,2006).

Sedangkan untuk dekripsi adalah dengan mengembalikan nilai dari hasil enkripsi di kalikan dengan nilai invers key matrik. Sebagai contohnya adalah sebagai berikut:

-(3,4) DE

-(11,22) LW

kemudian dilakukan perhitungan sebagai berikut:

$$(3,4)\begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}=(21+92,54+44)=(113,98)\rightarrow JU$$

$$(11,22)\begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}=(77\ \ 506,198\ \ 242)=(583,440)\ \rightarrow LY$$

Sehingga dari dekripsi dari DELW akan kembali lagi ke bentuk semula yaitu JULY.

2.3 Serangan terhadap kriptografi

a. Jenis – jenis serangan

Serangan (“serangan kriptanalisis”) terhadap kriptografi dapat dikelompokkan dengan beberapa cara :

1. Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi atas dua macam, yaitu :
   a. Serangan pasif (*passive attack*)

      Pada serangan ini, penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima, namun penyerang menyadap semua pertukaran pesan antara kedua entitas tersebut. Tujuannya adalah

untuk mendapatkan sebanyak mungkin informasi yang digunakan untuk kriptanalisis. Beberapa metode penyadapan antara lain :

- *Wiretapping* : penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambunganperangkat keras.
- *Electromagnetic Eavesdropping* : penyadap mencegat data yang ditrasnmisikan melalui saluran wireless, misalnya radio dan microwave.
- *Acoustic Eavesdropping* : menangkap gelombang suara yang dihasilkan oleh suara manusia.

b. 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 cipherteks, mengubah cipherteks, menyisipkan potongan cipherteks palsu, me-replay pesan lama, mengubah informasi yang tersimpan, dan sebagainya.

2. Berdasarkan banyaknya informasi yang diketahui oleh kriptanalis, maka serangan dapat dikelompokkan menjadi lima jenis, yaitu:

1. *Ciphertext-only attack*

Ini adalah jenis serangan yang paling umum namun paling sulit, karena informasi yang tersedia hanyalah cipherteks saja.

Kriptanalis memiliki beberapa cipherteks dari beberapa pesan, semuanya dienkripsi dengan algoritma yang sama. Untuk itu kriptanalis menggunakan beberapa cara, seperti mencoba semua kemungkinan kunci secara *exhaustive search*. Menggunkan analis frekuensi, membuat terkaan berdasarkan informasi yang diketahui,dan sebagainya.

2. *Known-plaintext attack*

   Ini adalah jenis serangan dimana kriptanalis memiliki pasangan plainteks dan cipherteks yang berkoresponden.

3. *Chosen-plaintext attack*

   Serangan jenis ini lebih hebat dari pada *known-plaintext attack*, karena kriptanalis dapat memilih plainteks yang dimilikinya untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.

4. *Chosen-ciphertext attack*

   Ini adalah jenis serangan dimana kriptanalis memilih ciphertext untuk dideskripsikan dan memiliki akses ke plaintext hasil deskripsi.

5. *Chosen text attack*

   Ini adalah jenis serangan yang merupakan kombinasi *chosen-plaintext attack* dan *chosen-chiphertext attack*.

3. Berdasarkan teknik yang digunakan dalam menemukan kunci, maka serangan dapat dibagi menjadi dua, yaitu :

1. *Exhaustive attack* atau *brute force attack*

   Ini adalah serangan untuk mengungkap plainteks atau kunci dengan menggunakan semua kemungkinan kunci. Diasumsikan kriptanalis mengetahui algoritma kriptografi yang digunakan oleh pengirim pesan. Selain itu kriptanalis memiliki sejumlah cipherteks dan plainteks yang bersesuaian.

2. *Analytical attack*

   Pada jenis serangan ini, kriptanalis tidak mencoba-coba semua kemungkinan kunci tetapi menganalisis kelemahan algoirtma kriptografi untuk mengurangi kemungkinan kunci yang tidak ada. Diasumsikan kriptanalis mengetahui algoritma kriptografi yang digunakan oleh pengirim pesan. Analisis dapat menggunakan pendekatan matematik dan statistik dalam rangka menemukan kunci.

3. *Related-key attack*

   Kriptanalis memiliki cipherteks yang dienkripsi dengan dua kunci berbeda. Kriptanalis tidak mengetahui kedua kunci tersebut namun ia mengetahui hubungan antara kedua kunci, misalnya mengetahui kedua kunci hanya berbeda 1 bit.

4. *Rubber-hose cryptanalysis*

   Ini mungkin jenis serangan yang paling ekstrim dan paling efektif. Penyerang mengancam, mengirim surat gelap, atau melakukan

penyiksaan sampai orang yang memegang kunci memberinya kunci untuk mendekripsi pesan.

b. Kompleksitas serangan

Kompleksitas serangan dapat diukur dengan beberapa cara, yaitu :

1. Kompleksitas data (*data complexity*)

   Jumlah data (plainteks dan cipherteks) yang dibutuhkan sebagai masukan untuk serangan. Semakin banyak data yang dibutuhkan untuk melakukan serangan, semakin kompleks serangan tersebut, yang berarti semakin bagus sistem kriptografi tersebut.

2. Kompleksitas waktu (*time complexity*)

   Waktu yang dibutuhkan untuk melakukan serangan. Semakin lama waktu yang dibutuhkn untuk melakukan serangan, berarti semakin bagus kriptografi tersebut.

3. Kompleksitas ruang memori (*space/storage complexity*)

   Jumlah memori yang dibutuhkan untuk melakukan serangan. Semakin banyak memori yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem kriptografi tersebut.

2.4 Keamanan Algoritma Kriptografi

Menurut Doni Ariyus (2005) Menuliskan Lard Knudsen mengelompokkan hasil kriptanalis ke dalam beberapa kategori berdasarkan jumlah dan kualitas informasi yang berhasil ditemukan :

- Pemecahan total (*total break*). Kriptanalis menemukan kunci *K*

- Deduksi (*penarikan kesimpulan*) global (*global deduction*). Kriptanalis menemukan algoritma alternatif, A, yang ekivalen dengan tetapi tidak mengetahui kunci *K*.)
- Deduksi lokal (*instance*/*local deduction*). Kriptanalis menemukan plainteks dari cipherteks yang disadap.

Deduksi informasi (*information deduction*). Kriptanalis menemukan beberapa informasi perihal kunci atau plainteks. Misalnya kriptanalis mengetahui beberapa kunci, kriptanalis mengetahui bahasa yang digunakan untuk menulis plainteks, kriptanalis mengetahui format plainteks, dan sebagainya. Sebuah algoritma dikatakan aman mutlak tanpa syarat (*unconditionally secure*) bila cipherteks yang dihasilkan oleh algoritma tersebut tidak mengandung cukup informasi untuk menentukan plainteks.

2.5 Algortima Kriptografi Klasik

Sebelum komputer ada, kriptografi dilakukan dengan menggunakan pensil dan kertas. Algoritma kriptografi (*cipher*) yang digunakan saat itu, dinamakan juga algoritma klasik, adalah berbasis karakter, yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Semua algoritma klasik termasuk ke dalam sistrm kriptografi simetris dan digunakan jauh sebelum kriptografi kunci publik ditemukan.

Kriptografi klasik memiliki beberapa ciri :

1. Berbasis karakter
2. Menggunakan pena dan kertas saja, belum ada komputer

3. Termasuk ke dalam kriptografi kunci simetris.

Tiga alasan mempelajari algoritma klasik :

1. Memahami konsep dasar kriptografi
2. Dasar algoritma kriptografi modern
3. Memahami kelemahan sistem kode.

(*Ariyus, Dony. 2005*)

Pada dasarnya, algoritma kriptografi klasik dapat dikelompokkan ke dalam dua macam cipher, yaitu :

1. Cipher substitusi (*substitution cipher*)

   Di dalam cipher substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu "unit" di isini berarti satu huruf, pasanga huruf, atau dikelompokkan lebih dari dua huruf. Algoritma substitusi tertua yang diketahui adalah *Caesar cipher* yang digunakan oleh kaisar Romawi , Julius Caesar (sehingga dinamakan juga *casear cipher*), untuk mengirimakan pesan yang dikirimkan kepada gubernurnya.

2. Cipher transposisi (*transposition cipher*)

   Pada cipher transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (*scrambling*) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karkater tersebut.

2.6 Visual Basic Net 2010

Merupakan sebuah bahasa pemograman dan sebagai sarana (tool) untuk menghasilkan program-program aplikasi berbasiskan windows. Beberapa kemampuan atau manfaat dari Visual Basic diantaranya:

a. Untuk membuat program aplikasi berbasiskan windows.
b. Untuk membuat obyek-obyek pembantu program, seperti Control Active X, File Help, Aplikasi Internet dan sebagainya.
c. Menguji program (debugging) dan menghasilkan program akhir berakhiran ”EXE” yang bersifat executable atau dapat langsung dijalankan.

   Keistimewaan utama dari Visual Basic adalah:

d. Menggunakan platform pembuatan program yang diberi nama developer studio, yang memiliki tampilan seperti C++ dan visual J++.
e. Memiliki kompiler handal yang dapat menghasilkan File Executable yang lebih cepat dan efisien.
f. Memiliki tambahan saran wizard yang baru. Tambahan kontrol-kontrol baru dan lebih canggih serta peningkatan kaidah struktur bahasa Visual Basic.
g. Kemampuan membuat Active X dan fasilitas internet yang lebih banyak.
h. Sarana akses yang lebih cepat dan andal untuk membuat aplikasi database yang berkemampuan tinggi.
i. Visual Basic.net memiliki beberapa versi baru edisi yang disesuaikan dengan kebutuhan pemakainya.

Dalam pemograman berbasiskan OOP (Object Oriented Programming), sebuah program dibagi menjadi bagian-bagian kecil yang disebut dengan obyek. Setiap obyek memiliki entiti terpisah dengan entiti-entiti lain dalam lingkungannya. Obyek-obyek yang terpisah ini dapat diolah sendiri-sendiri, dan setiap obyek memiliki sekumpulan sifat dan metode yang melakukan fungsi tertentu sesuai dengan yang telah diprogramkan kepadanya.

Adapun obyek-obyek yang dipergunakan dalam program ini adalah:

1. Project

   Project adalah sekumpulan modul. Jadi project merupakan aplikasi itu sendiri. Project disimpan dalam file yang berakhiran VBP. Jika kita akan melaksanakan pembuatan program aplikasi, akan terdapat jendela project yang berisi semua file yang dibutuhkan menjalankan program aplikasi Visual Basic.net pada saat pembuatan program aplikasi baru maka jendela project otomatis akan berisi object form1. Pada jendela project terdapat tiga icon yaitu View Code, View Object, dan Toggle Folders. Icon View Code dipakai untuk menampilkan jendela editor kode program. Icon View Object dipakai untuk menampilkan bentuk formulir (form) dan icon Toggle Folders digunakan untuk menampilkan folder

2. Form

   Form adalah jendela yang dipakai untuk membuat user interface/tampilan. Secara otomatis akan tersedia form yang baru jika membuat suatu program aplikasi yang baru, dengan nama Form1. pada umumnya dalam suatu form

terdapat garis titik-titik yang disebut dengan Grid. Untuk lebih memahami form ini maka di bawah ini terdapat gambar jendela form.

3. Toolbox

   Toolbox adalah kumpulan dari obyek yang digunakan untuk membuat user interface (tampilan) serta control bagi program aplikasi. Untuk menempatkan control pada suatu form dapat dilakukan dengan klik ganda control dalam toolbox, kemudian mengubah besar dan ukurannya serta memindahkannya dengan metode Drag and Drop atau dengan cara mengklik kontrol toolbox, kemudian pindahkan pointer mouse jendela form. Kursor berubah menjadi Crosshair lalu tempatkan pada sudut kiri atas dimana kita inginkan kontrol tersebut diletakkan, tekan tombol mouse kiri dan tahan ketika menyeret kursor ke arah sudut kanan bawah.

4. Properties

   Properties berisikan daftar struktur setting properti yang digunakan pada sebuah object terpilih. Kotak drop-down pada bagian atas jendela berisi daftar semua object pada form yang aktif. Ada tab tampilan, yaitu alphabetic (urut abjad) dan categorized (urut berdasarkan kelompok).

5. Kode Program

   Kode program adalah serangkaian tulisan perintah yang akan dilaksanakan jika suatu obyek dijalankan. Kode program ini mengkontrol dan menentukan jalannya suatu obyek.

6. Event

Event adalah peristiwa atau kejadian yang diterima suatu obyek, misalnya klik, seret, tunjuk, dan lain sebagainya.

7. Metode (Methods)

   Metode adalah serangkaian perintah yang sudah tersedia pada suatu obyek yang dapat diminta untuk mengerjakan tugas khusus.

8. Module

   Module dapat disejajarkan dengan form, tetapi module tidak mengandung obyek. Module berisikan prosedur umum, deklarasi variabel dan definisi konstanta yang digunakan oleh aplikasi.

2.7 Pengertian UML

Unified Modelling Language (UML) adalah sebuah bahasa yang telah menjadi standar dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak. UML menawarkan sebuah standar untuk merancang model sebuah sistem. Dengan menggunakan UML dapat dibuat model untuk semua jenis aplikasi piranti lunak, di mana aplikasi tersebut dapat berjalan pada piranti keras, sistem operasi dan jaringan apapun, serta ditulis dalam bahasa pemrograman apapun. Tetapi karena UML juga menggunakan *class* dan *operation* dalam konsep dasarnya, maka lebih cocok untuk penulisan piranti lunak dalam bahasa berorientasi objek seperti C++, Java, atau VB. NET (Prastuti Sulistyorini, 2012).

Unified Modeling Language (UML) adalah kumpulan notasi grafis yang didukung oleh sebuah model tunggal, yang membantu dalam menjelaskan dan merancang sistem perangkat lunak, khususnya sistem perangkat lunak dibangun menggunakan gaya berorientasi objek. UML terdiri atas banyak elemen-elemen grafis yang digabungkan membentuk diagram. Tujuan representasi elemen-elemen grafis ke dalam diagram adalah untuk menyajikan beragam sudut pandang dari sebuah sistem berdasarkan fungsi masing-masing diagram tersebut. Kumpulan dari beragam sudut pandang inilah yang kita sebut sebuah model (Andy Prasetyo Utomo, 2013).

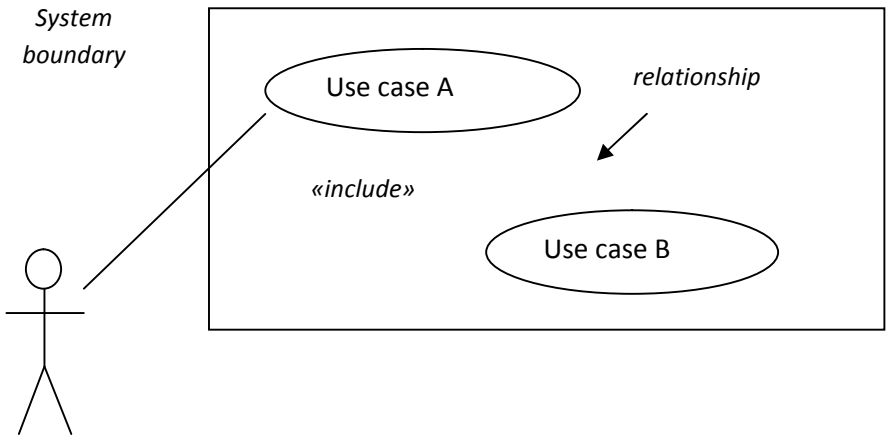
Dengan menggunakan model ini diharapkan pengembangan piranti lunak dapat memenuhi semua kebutuhan pengguna dengan lengkap dan tepat, termasuk faktor-faktor seperti *scalability*, *robustnees*, *security*, dan sebagainya. Untuk melakukan pemodelan sistem perangkat lunak secara visual digunakan UML (*Unified Modelling Language*) yang digambarkan secara elektronik lewat sarana perangkat lunak *Rational Rose*. Sebagai mana telah diterapkan oleh Gufran (2012) di mana UML diterapkan untuk mengukur kinerja mahasiswa menggunakan pendekatan berorientasi objek. Kemudian UML diterapkan juga oleh Sunguk (2012) untuk menerapkan sistem *database* dan aplikasi komputer. Selanjutnya Jakimi dan Koutbi (2009) menerapkan pendekatan UML untuk sekenario rekayasa dan kode generasi.

a. Use Case Diagram

Use case merupakan teknik menangkap kebutuhan-kebutuhan fungsional dari sistem baru atau sistem yang diubah. Setiap *use case* terdiri dari satu atau lebih skenario yang menerangkan bagaimana sistem berinteraksi dengan pengguna atau sistem yang lain untuk mencapai suatu sasaran bisnis tertentu. Dalam tehnik ini tidak diterangkan cara kerja sistem secara internal maupun implementasinya. Yang ditunjukkan adalah langkah-langkah yang dilakukan pengguna dalam menggunakan perangkat lunak (Nyimas Artina, 2006).

Diagram *Use Case* merupakan diagram yang menggambarkan fungsi berupa komponen, kelas, atau kejadian yang ada dalam *system* (Ade Sutedi *et al*, 2015). *Use case* atau diagram *use case* merupakan pemodelan untuk kelakuan (*behavior*) sistem informasi yang akan dibuat. *Use case* mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Secara kasar, *use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu (Rosa A.S dan M. Shalahuddin, 2014).

Syarat penamaan pada *use case* adalah nama didefinisikan sesimpel mungkin dan dapat dipahami. Ada dua hal utama pada *use case* yaitu pendefinisian apa yang disebut aktor dan *use case*.

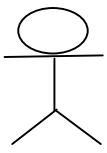


Gambar 2. ***Use Case Diagram***

Terdapat 2 bagian utama dalam *use case modeling* sebagaimana dijelaskan sebagai berikut:

- Aktor

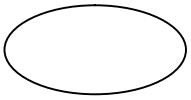
  Aktor merupakan orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi yang akan dibuat itu sendiri, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang.



Gambar 3. Aktor

- *Use Case*

  Use case merupakan fungsional yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor.



Gambar 4. *Use Case*

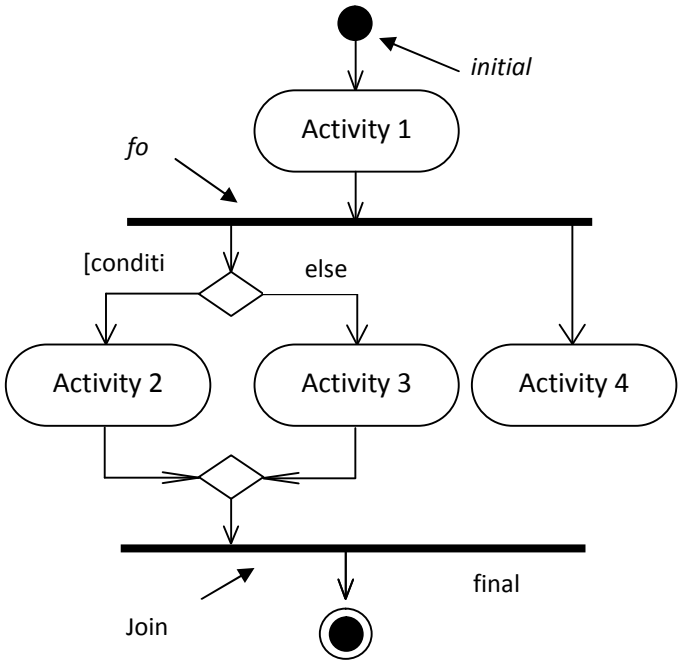
b. Activity Diagram

Activity diagrams menggambarkan *workflow* (aliran kerja) atau aktivitas sari sebuah sistem atau proses bisnis. Yang perlu diperhatikan di sini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem (Rosa A.S dan M. Shalahuddin, 2014).

Diagram aktivitas juga banyak digunakan untuk mendefinisikan hal-hal berikut :

1. Rancangan proses bisnis dimana setiap urutan aktivitas yang digambarkan merupakan proses bisnis sistem yang didefinisikan.
2. Urutan atau pengelompokkan tampilan dari sistem/*user interface* di mana setiap aktivitas dianggap memiliki antarmuka tampilan.

3. Rancangan pengujian di mana setiap aktivitas dianggap memerlukan sebuah pengujian yang perlu didefinisikan kasus ujinya.

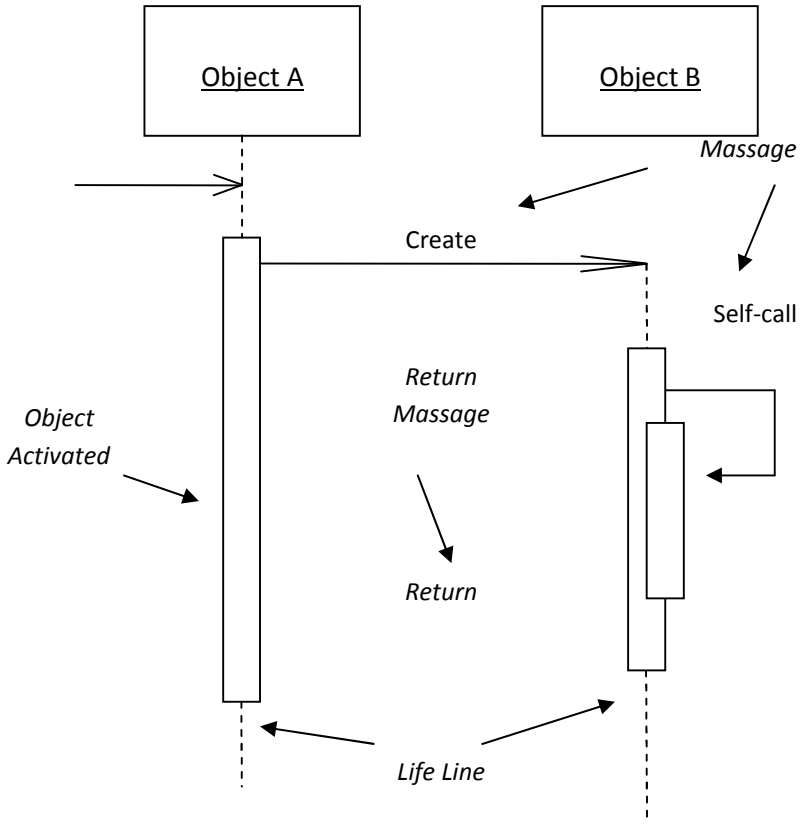


Gambar 5. ***Activity Diagram***

c. Sequence Diagram

Sequence diagram menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima antar objek. Oleh karena itu untuk menggambarkan diagram sekuen maka harus diketahui objek-objek yang terlibat dalam sebuah *use case* beserta metode-metode

yang dimiliki kelas yang diinstansiasi menjadi objek itu (Rosa A.S dan M. Shalahuddin, 2014).



Gambar 6. *Sequence Diagram*

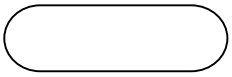
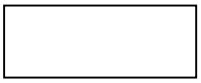
2.8 Pengertian Flowchat

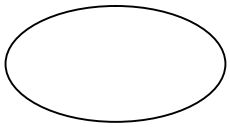
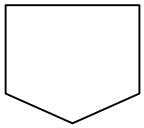
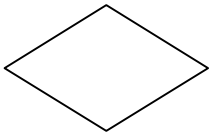
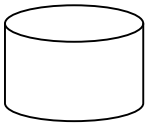
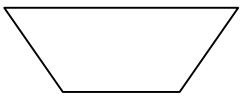
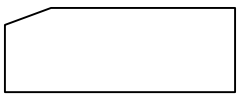
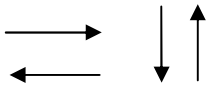
Menurut (Sariadin Siallagan, 2013), Flowchart adalah suatu diagram alir yang mempergunakan simbol atau tanda untuk menyelesaikan masalah. Dalam hal ini, penyelesaian masalah menggunakan simbol-simbol yang telah disepakati.

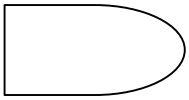
Menurut (Abdillah Baraja, 2012) Flowchart adalah representasi grafik yang menggambarkan setiap langkah yang akan dilakukan dalam suatu proses, yang merupakan alat bantu yang banyak digunakan untuk menggambarkan sistem secara pisikal.

Bagan alir (flowchart) adalah bagan (chart) yang menunjukkan alir (flow) di dalam program atau prosedur system secara logika. Digunakan terutama untuk alat bantu komunikasi dan untuk dokumentasi.

Tabel 2.3. Simbol-Simbol Flowchart

NO	SIMBOL	FUNGSI
1.		Terminal menyatakan awal atau akhir dari suatu logaritma.
2.		Menyatakan proses.
3.		Proses yang terdefenisi atau sub program.
4.		Persiapan yang digunakan untuk memberi nilai awal suatu besaran.

5.		Menyatakan masukan dan keluaran (input/output).
6.		Menyatakan penyambung ke simbol lain dalam satu halaman.
7.		Menyatakan penyambung ke halaman lainnya.
8.		Menyatakan pencetakan (dokumen) pada kertas.
9.		Menyatakan *decision* (keputusan) yang digunakan untuk penyeleksian kondisi didalam program.
10.		Menyatakan media prnyimpanan drum magnetik.
11.		Menyatakan input/output menggunakan disket.
12.		Menyatakan operasi yang dilakakukan secara manual.
13.		Menyatakan input/output dari kartu plong.
14.		Menyatakan aliran pekerjaan (proses).

15.		Multidocument (banyak dokumen).
16.		Delay (penundaan atau kelambatan).

Sumber : Abdillah Baraja, 2012

2.9. Perbedaan Penelitian dari Peneliti Yang Lain.

NO	NAMA PENELITI	JUDUL	URAIAN
1	Akik Hidayat1, Tuty Alawiyah2	Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang	Hill Cipher merupakan salah satu algoritma kriptografi yang memanfaatkan matriks sebagai kunci untuk melakukan enkripsi dan Dekripsi dan aritmatika modulo. Setiap karakter pada plaintext ataupun ciphertext dikonversikan kedalam bentuk angka. Enkripsi dilakukan dengan mengalikan matriks kunci dengan matriks plaintext, sedangkan Dekripsi dilakukan dengan mengalikan invers matriks kunci dengan matriks ciphertext. Karena itulah, Hill Cipher hanya bisa menggunakan matriks persegi sebagai matriks kuncinya. Invers semu atau pseudo invers dapat dimanfaatkan pada algoritma Hill Cipher, sehingga matriks kunci yang digunakan tidak terbatas pada matriks persegi saja. Penggunaan matriks persegi panjang menjadikan ciphertext lebih panjang dari plaintext.

			Hal ini tentunya membuat pesan menjadi lebih tersamarkan. Pada tulisan ini, penulis menggunakan modulo 95 artinya inputan data ada 95 simbol. Untuk mempermudah penghitungan pada saat inisialisasi matriks kunci, proses enkripsi dan proses Dekripsi menggunakan program aplikasi C++.
2	Abdul Halim Hasugian	Implementasi Algoritma Hill Cipher Dalam Penyandian 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, di mana 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.Data dapat berupa sebuah filedan berbentuk string. Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Karena Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. Kata Kunci : Hill Cipher, Enkripsi, Dekripsi *(PDF) IMPLEMENTASI ALGORITMA HILL CIPHER DALAM PENYANDIAN DATA*. Available from:

			https://www.researchgate.net/publication/318947312_IMPLEMENTASI_ALGORITMA_HILL_CIPHER_DALAM_PENYANDIAN_DATA [accessed Nov 02 2018].
3	Nikken Prima Puspita dan Nurdin Bahtiar	Kriptografi Hill Cipher Dengan Menggunakan Operasi Matriks	Diberikan matriks A berukuran 2× 2 dengan determinan 1 atau -1. Setiap karakter pada plainteks dikonversikan kedalam angka berdasarkan kode ASCII. Proses enkripsi dilakukan dengan cara mengalikan matriks plainteks dengan matriks A. Hasil elemen matriks perkaliannya harus merupakan bilangan bulat modulo 95 yang kemudian ditambahkan dengan bilangan 32. Sedangkan proses dekripsi hill cipher dilakukan dengan cara yang sejalan tetapi matriks cipherteks dioperasikan dengan matriks $1A$.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem

Tahap implementasi sistem merupakan tahap dimana aplikasi yang telah dirancang dijalankan. Tahap ini menunjukkan apakah setiap proses dapat berjalan dengan baik dan mampu memberikan hasil yang diharapkan. Proses perancangan aplikasi menggunakan *visual basic NET 2010* ditampilkan dalam bentuk form-form yang menjadi sarana bagi pengguna untuk melakukan proses implementasi.

4.2 Pengujian Sistem

Pengujian sistem dilakukan untuk menunjukkan apakah sistem yang telah dirancang dapat berjalan sesuai harapan. Selain itu tujuan pengujian adalah untuk dapat menemukan kesalahan fungsi pada aplikasi yang dibangun dan memperbaikinya.

Pengujian dilakukan dengan memasukkan karakter atau huruf dari file berformat .txt selanjutnya diproses oleh aplikasi apakah aplikasi tersebut dapat memberikan hasil yang sesuai. Proses yang akan dilakukan pengujian dalam aplikasi ini adalah simulasi pengiriman pesan dengan menggunakan metode algoritma *Hill Chiper* antara pengirim kepada penerima dengan kunci yang dimiliki masing-masing pihak tanpa perlu bertukar kunci tunggal hingga pada akhirnya pesan asli yang dikirimkan oleh pengirim dapat dibaca oleh penerima .

4.2.1 Tampilan Awal/ Home

Tampilan pada gambar dibawah merupakan tampilan awal ketika aplikasi dijalankan. Pada form ini pengguna dapat memilih untuk membuka beberapa form lainnya seperti tombol tentang yang akan mengarahkan pengguna menuju form yang menjelaskan profil aplikasi ini, tombol materi dan tombol pengaturan yang akan mengarahkan pengguna ke form yang menjelaskan tata cara penggunaan dari aplikasi ini.

Gambar 18. Tampilan Awal/ Home

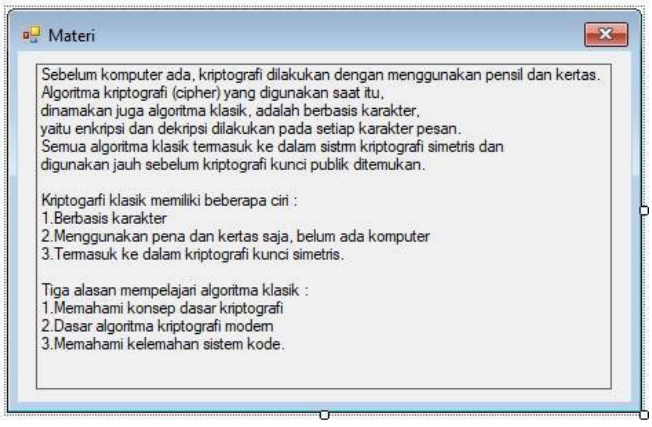
4.2.2 Tampilan Halaman Judul

Tampilan berikut ini menampilakan halaman atau form yang berisi tentang profil dari aplikasi ini. Di dalamnya terdapat judul dari aplikasi beserta maksud dari pembuatannya beserta nama dan nomor pokok mahasiswa penulis.

Gambar 19. Tampilan Halaman Judul

4.2.3 Tampilan Materi

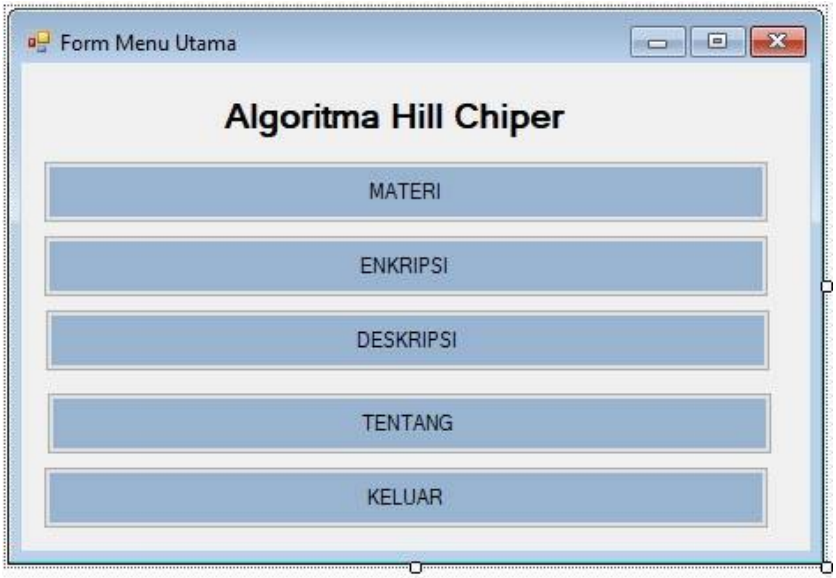
Tampilan materi merupakan tampilan halaman atau form yang berisi tentang materi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma *Hill Chiper*.



Gambar 20. Tampilan Materi

4.2.4 Tampilan Halaman Utama Algoritma *Hill Chiper*

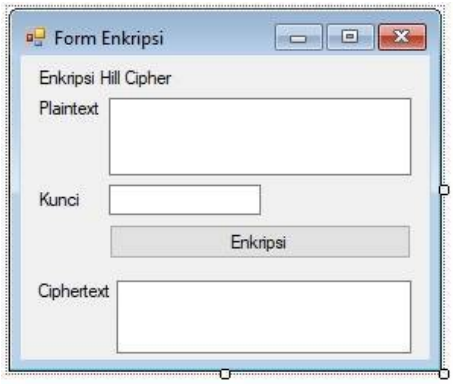
Tampilan berikut merupakan tampilan utama pada aplikasi ini. Algoritma *Hill Chiper* merupakan protokol yang menjamin tidak adanya pertukaran kunci antara pihak-pihak yang melakukan enkripsi dan dekripsi. Kedua belah pihak menggunakan kunci mereka masing-masing untuk mengenkripsi pesan dan kemudian untuk mendekripsi pesan tanpa perlu mengetahui kunci yang lainnya



Gambar 22. Tampilan Halaman Utama Algoritma *Hill Chiper*

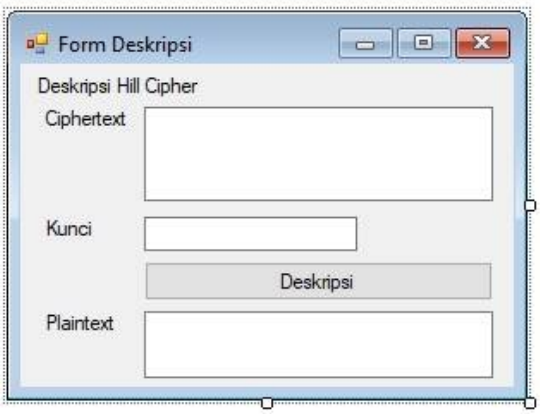
Uji coba pada system aplikasi ini dilakukan dengan memasukkan input teks yang bersumber dari file berekstensi *txt ,dengan menggunakan tombol pencarian yang berada disisi kanan atas.

Pada tahap awal rangkaian karakter akan berada di sisi bagian pengirim yang akan mengeksekusi rangkaian karakter tersebut untuk diubah menjadi ciphertext menggunakan Algoritma *Hill Chiper* Cipher. Untuk dapat mengeksekusi dibutuhkan kunci yang hanya dapat diisi karakter angka dari 0 sampai 9.



Gambar 26. Tampilan Enkripsi dengan Algoritma *Hill Chiper*

Tombol enkripsi yang ditekan setelah memasukkan kunci berupa karakter angka selanjutnya akan mengeksekusi rangkaian karakter pesan asli yang selanjutnya akan dipanggil plaintext. Hasil enkripsi didapatkan pada textbox dibawahnya.Tombol kirim yang ditekan oleh penerima berfungsi untuk meneruskan pesan kembali pada pengirim. Selanjutnya ciphertext yang merupakan enkripsi dari ciphertext yang diterima dari pengirim akan diteruskan ke pengirim.



Gambar 27. Tampilan Deskripsi Hill Cipher

4.3 Pengujian Sistem

Perangkat lunak adalah elemen kritis dari jaminan kualitas perangkat lunak dan merepresentasikan kajian pokok dari spesifikasi, perancangan, dan pengkodean. Pengujian yang digunakan untuk menguji sistem ini adalah metode pengujian *black-box*. Pengujian *black-box* berfokus pada persyaratan fungsional perangkat lunak.

4.3.1 Rencana Pengujian

Pengujian fungsi Penerapan Matrix Persegi Pancajang Dalam Pengembangan Algoritma Hill Chiper dilakukan dengan menggunakan metode Black Box. Pengujian dilakukan pada fungsi-fungsi sistem untuk menentukan apakah fungsi tersebut telah berjalan sesuai dengan yang diharapkan.

1) Bangkitkan Kunci

Tabel . Rencana Pengujian Tombol Cari

Menu yang diuji	**Detail pengujian**	**Kesimpulan**
Bangkitkan Kunci	Melakukan random kunci pada proses hill chiper.	*Diterima*

2) Proses Enkripsi

Tabel . Rencana Pengujian Pengguna (*User*)

Menu yang diuji	**Detail pengujian**	**Jenis uji**
Proses	Melakukan proses enkripsi	*Diterima*
Kirim	Proses pengiriman file enkripsi	*Diterima*
Clear All	Menghapus seluruh text yang ada pada text box	*Diterima*

3) Proses Deskripsi

Tabel . Rencana Pengujian Pengguna (*User*)

Menu yang diuji	**Detai pengujian**	**Jenis uji**
Dekripsi	Melakukan proses deskripsi atau pengembalian pesan asli	*Diterima*
Close	Menutup semua program	*Diterima*
Clear All	Menghapus seluruh text yang ada pada text box	*Diterima*

4.3.2 Pengujian Proses

Pengujian proses yang telah disusun, maka dapat dilakukan pengujian sebagai berikut :

Tabel . Proses Pengujian Enkripsi dan Deskripsi (*User*)

Data Pengujian Proses					**Hasil**
Nomor	**Isi Pesan**	**Kunci**	**Enkripsi**	**Deskripsi**	
1	PANCA BUDI	119 24 91 251	H+ k7{¦Ít¿	PANCA BUDI	Berhasil

4.3.3 Kesimpulan Dan Hasil Pengujian Sistem

Hasil pengujian dari pengujian alpha telah selesai, menunjukkan bahwa sistem sudah memenuhi syarat fungsional. Secara fungsional sistem yang sudah dibangun sudah dapat menghasilkan keluaran sesuai yang diharapkan.

Tabel . Kesimpulan Pengujian Alpha

Nama fungsi	**Hasil**
Tombol Cari	Fungsi berjalan dengan baik
Proses	Fungsi berjalan dengan baik
Enrkipsi	Fungsi berjalan dengan baik
Deskripsi	Fungsi berjalan dengan baik
Clear All	Fungsi berjalan dengan baik

BAB V

PENUTUP

1. Kesimpulan

Berdasarkan pembahasan dalam perancangan Penerapan Matrix Persegi Panjang Dalam Pengembangan Algoritma Hill Chiper, maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk menampilkan simulasi pengiriman pesan berekstensi *txt antara pengirim dan penerima.
2. Penggunaan Algoritma Hill Chiper memiliki manfaat bagi pengirim dan penerima pesan tanpa harus menukar kunci matrix.
3. Tidak ada lagi kesalahan pemahaman atau salah tafsir kunci tunggal karena pengirim dan penerima memiliki kunci yang dapat ditetapkan masing-masing pihak.
4. Kemungkinan bocornya kunci saat proses pertukaran informasi kunci tunggal dapat dihindari.

2. Saran

Adapun saran-saran yang dapat dilakukan penelitian ataupun pengembangan selanjutnya adalah sebagai berikut:

1. Perangkat lunak ini dapat dikembangkan dengan menggunakan kombinasi metode-metode lain.
2. Perangkat lunak ini dapat dikembangkan dan terhubung ke jaringan sehingga dapat dijalankan di lebih dari satu computer.

3. Perangkat lunak ini dapat dikembangkan menggunakan algoritma-algoritma lain yang lebih kompleks.

DAFTAR PUSTAKA

Anonim, E. H. Rachmawanto and C. A. Sari, "Keamanan File Menggunakan Teknik Kriptografi Shift Cipher," Jurnal Techno. Com, vol. 14, no. 2, pp. 329-335, 2014.

Azanudin, " *Penyandian Short Message Service (SMS) Pada Telepon Sesular Dengan Menggunakan Algoritma Gronsfeld Cipher,* " Jurnal Pelita Informatika Budi Darma, Vol. 4, Nomor 1, 2013.

Andrian, Yudhi, and Purwa Hasan Putra. "Analisis Penambahan Momentum Pada Proses Prediksi Curah Hujan Kota Medan Menggunakan Metode Backpropagation Neural Network." Seminar Nasional Informatika (SNIf). Vol. 1. No. 1. 2017.

Azmi, Fadhillah, and Winda Erika. "Analisis keamanan data pada block cipher algoritma Kriptografi RSA." CESS (Journal of Computer Engineering, System and Science) 2.1: 27-29.

Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (WASPAS). Jurnal Media Informatika Budidarma, 2(2).

Bishop, Rosdiana, "*Sekuritas Sistem Dengan Kriptografi*," in Prosiding Sendi_U 2013, Semarang, 2013.

Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." IT Journal Research and Development 2.1 (2017): 1-11.

Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2017, October). Encryption and decryption using password based encryption, MD5, and DES. In International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017) (pp. 278-283). Atlantis Press.

Erika, Winda, Heni Rachmawati, and Ibnu Surya. "Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)." Jurnal Aksara Komputer Terapan 1.2 (2012).

Fachri, B. (2018). Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif. Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika), 3, 98-102.

Fresly, Faizal Zuli1, Ari Irawan, "*Implementasi Kriptografi Dengan Algoritma Blowfish dan Riverst Shamir Adleman (RSA) Untuk Proteksi File*," Jurnal Format Volume 6 nomor 2 Tahun 2016

Fuad, R. N., & Winata, H. N. (2017). Aplikasi keamanan file audio wav (waveform) dengan terapan algoritma RSA. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 1(2), 113-119.

Ginting, G., Fadlina, M., Siahaan, A. P. U., & Rahim, R. (2017). Technical approach of TOPSIS in decision making. Int. J. Recent Trends Eng. Res, 3(8), 58-64.

Gede Angga Pradipta " *Penerepan Kombinasi metode Enkripsi Vigenere Cipher Dan Trasposisi Pada Aplikasi Client Server Chatting*, " Jurnal Sistem Dan Informatika Vol. 10, Nomor 2, 2016.

Hafni, Layla, and Rismawati Rismawati. "Analisis faktor-faktor internal yang mempengaruhi nilai perusahaan pada perusahaan manufaktur yang terdaftar di BEI 2011-2015." Bilancia: Jurnal Ilmiah Akuntansi 1.3 (2017): 371-382.

Hamdi, Muhammad Nurul, Evi Nurjanah, and Latifah Safitri Handayani. "Community development based onibnu khaldun thought, sebuah interpretasi program pemberdayaan umkm di bank zakat el-zawa." EL MUHASABA: Jurnal Akuntansi (e-journal) 5.2 (2014): 158-180.

Hariyanto, E., & Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. International Journal of Science and Research (IJSR), 5(10), 1363-1365.

Hartanto, S. (2017). Implementasi fuzzy rule based system untuk klasifikasi buah mangga. TECHSI-Jurnal Teknik Informatika, 9(2), 103-122.

Harumy, T. H. F., & Sulistianingsih, I. (2016). Sistem penunjang keputusan penentuan jabatan manager menggunakan metode mfep pada cv. Sapo durin. In Seminar Nasional Teknologi Informasi dan Multimedia (pp. 6-7).

Havena, M., & Marlina, L. (2018). The Technology of Corn Processing as an Effort to Increase The Income of Kelambir V Village. Journal of Saintech Transfer, 1(1), 27-32.

Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana, " *Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard*," Jurnal Informatika Mulawarman Vol. 10. Nomor 1, 2015.

Rhee, C. A. Sari, E. H. Rachmawanto, Y. P. Astuti and L. Umaroh, "Optimasi Penyandian File Kriptografi Shift Cipher," in Prosiding Sendi_U 2013, Semarang, 2013.

Renddy, Teady Matius, Surya Mulyana, Fresly, " *Steganografi Dengan Deret Untuk Mengacak Pola Penempatan Pada Rgb*," Jurnal Teknologi Informasi, 2015.

Suriski Sitinjak, Yuli Fauziah, Juwairiah, " *Aplikasi Kriptografi File Menggunakan Algoritma Blowfish*," Jurnal Informatika Mulawarman Vol. 10. Nomor 1, 2015.