Jurnal Online Universitas Budi Luhur

# SKANIKA

Sistem Komputer dan Teknik Informatika

Vol. 1, No. 1, Mei 2018

**Diterbitkan oleh:**
Universitas Budi Luhur
Jl. Raya Ciledug Petukangan Utara, Jakarta Selatan

download PDF Abstract views: 1142 times. Downloaded: 746 times.

**APLIKASI EMAIL (ELECTRONIC MAIL) MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-128) DAN ALGORITMA RIVEST CIPHER 4 (RC4) BERBASIS WEB**

Ryfan Aditya Indra , Wahyu Pramusinto 704-710

download PDF Abstract views: 996 times. Downloaded: 759 times.

**APLIKASI KEAMANAN EMAIL DENGAN METODE RC4 (RIVEST CODE 4) DAN DES (DATA ENCRYPTION STANDARD) BERBASIS MOBILE ANDROID PADA PT. TIRTA ABADI GEMILANG**

Diki Firmansyah, Rizky Tahara Shita 528-533

download PDF Abstract views: 1409 times. Downloaded: 688 times.

**IMPLEMENTASI ALGORITMA APRIORI UNTUK MEMPREDIKSI PENJUALAN TIKET BERBASIS DEKSTOP PADA PT. NADIA TRAVEL**

Thisa Tri Utami , Mohammad Syafrullah 739-744

download PDF Abstract views: 1461 times. Downloaded: 1222 times.

**APLIKASI PENGAMANAN SMS (SHORT MESSAGE SERVICE) DENGAN MENGGUNAKAN ALGORITMA AES-128 BERBASIS ANDROID PADA KANTOR NOTARIS RINA ADRIANI S.H**

Anita Fauziah, Dewi Kusumaningsih 558-564

download PDF Abstract views: 1379 times. Downloaded: 604 times.

**APLIKASI KRIPTOGRAFI PENGAMANAN DATABASE MENGGUNAKAN METODE AES DAN VIGENERE BERBASIS DESKTOP PADA PADA DIVISI PENCEGAHAN DAN PENANGGULANGAN HIV AIDS YAYASAN KAPETA**

Denny Eka Erlianto , Painem Painem 773-779

download pdf Abstract views: 1525 times. Downloaded: 644 times.

**APLIKASI PENCARIAN INFORMASI KONTEN MENGGUNAKAN ALGORITMA KNUTH MORRIS PRATT PADA APLIKASI LIBRO PUSTAKA DIGITAL**

# Aplikasi Kriptografi Pengamanan *Database* Menggunakan Metode AES Dan Vigenere Berbasis *Desktop* Pada Pada Divisi Pencegahan Dan Penanggulangan Hiv Aids Yayasan Kapeta

**Denny Eka Erlianto[1)], Painem[2)]**
*Program Studi Tehnik Informatika, Fakultas Teknologi Informasi, Univ Budi Luhur*
*Jl. Raya Ciledug Raya, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260*
*Telp. (021) 5853753, Fax. (021) 5866369*
*E - mail :* erliandenny@gmail.com

**ABSTRAK**

*Teknologi informasi saat ini telah banyak mempengaruhi segala bidang, diantaranya pada bidang keamanan komputer, terutama kerahasiaan data. Hal ini merupakan suatu tanda bahwa informasi merupakan elemen yang sangat penting untuk diamankan. Kriptografi merupakan salah satu komponen yang tidak dapat diabaikan dalam membangun keamanan komputer. Kriptografi terus dikembangkan seiring berjalannya waktu untuk memberikan keamanan dan kenyamanan pengguna. Kriptografi bertujuan agar basis data yang dikirim tidak dibaca oleh orang yang tidak berhak. Keamanan basis data sangat dibutuhkan seperti di Yayasan KAPETA, yayasan KAPETA sebagai Sub Recipient (SR) dibawah koordinasi Principle Recipient (PR) yaitu Yayasan Spiritia, basis data dikirimkan secara berkala setiap bulan oleh yayasan KAPETA atau Sub Recipient lainnya secara berkala sebagai laporan melalui surat elektronik dengan mengirimkan basis data yang berbentuk file berformat .mdb ke Yayasan Spiritia sebagai Principle Recipient (PR), hal tersebut memiliki celah keamanan yang sangat besar karena data yang dikirim setiap bulan melalui surat elektronik dengan masih berbentuk basis data dengan format .mbd yang sangat mudah di buka dan di salah gunakan. Algoritma yang digunakan pada penelitian ini adalah algoritma AES 128bit (Advanced Encryption Standard) dan algoritma Vigenere yang merupakan bagian dari algoritma enkripsi dalam kriptografi. Algoritma Vigenere merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu plaintext dengan menggunakan teknik substitusi. Tabel dengan jumlah field 45 dan record 13279 membutuhkan waktu proses enkripsi selama 30 menit dan 28 menit 20 detik untuk mendekripsi kembali tabel tersebut. Sedangkan untuk tabel dengan jumlah field sebanyak 3 dan record sebanyak 531 membutuhkan waktu proses enkripsi selama 2 detik. Hal ini menunjukan bahwa waktu proses enkripsi dan dekripsi tergantung banyaknya jumlah record dan jumlah field dari tabel database yang diproses.*

**Kata kunci :** kriptografi, *database*, *desktop*, aes, 128, vigenere,

## 1. PENDAHULUAN

Keamanan *database* sangat dibutuhkan seperti di Yayasan KAPETA. Yayasan KAPETA sebagai Sub Recipient (SR) dibawah koordinasi Principle Recipient (PR) Yayasan Spiritia melalui dukungan pendanaan program penanggulangan TB-HIV dari the GF-ATM New Funding Model tahun 2016-2017 untuk komponen HIV dan AIDS. Data dikirim yayasan KAPETA atau Sub Recipient lainnya secara berkala sebagai laporan melalui surat elektronik dengan mengirimkan *database* yang berbentuk file berformat .mdb ke Yayasan Spiritia sebagai Principle Recipient (PR). Hal tersebut memiliki celah keamanan yang sangat besar karena data yang dikumpulkan di sistem SIS (Sistem Informasi Spritia) dan dikirim setiap bulan melalui surat elektronik dengan masih berbentuk *database* dengan format .mbd . Untuk mengamankan data tabel *database* kita dapat menggunakan kriptografi, penerapan kriptografi pada yayasan KAPETA akan di fokuskan bagaimana sampai dengan *database* dibuka oleh pihak yang berhak untuk melihatnya. Algoritma yang digunakan adalah Advanced Encryption Standard (AES) 128 bit dan algoritma Vigenere. Maka dapat di rumuskan bahwa dapat dengan mudah diubah atau dibaca oleh pihak yang tidak berhak dan tidak bertanggung jawab karena kurangnya keamanan *database* di yayasan KAPETA. Rentannya akan keamanan *database* di yayasan KAPETA, karena setiap bulan file *database* (*mdb) tersebut dikirimkan secara berkala melalui e-mail (sebagai laporan bulanan) tanpa pengamanan berarti. Secara umum tujuan untuk mengamankan sebuah data dalam bentuk table *database* agar tidak bisa di baca oleh orang lain selain pemilik atau orang yang berhak atas *database* tersebut serta

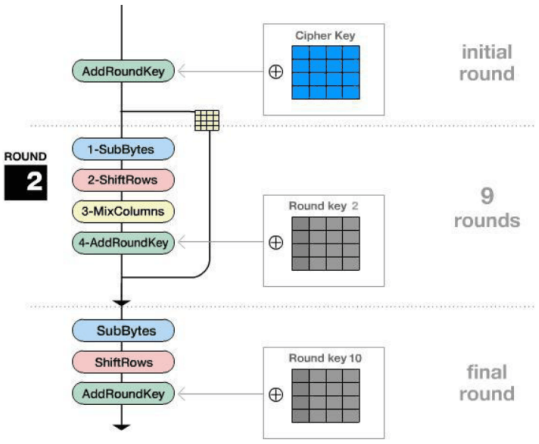
menghasilkan aplikasi pengamanan *database* berbasis vb.net yang mudah digunakan oleh pengguna dan mengimplementasikan algoritma AES dan algoritma VIGNERE.

## 2. LANDASAN TEORI

Dalam menjaga kerahasiaan data menggunakan kriptografi, data sederhana yang dikirim (plaintext) diubah ke dalam bentuk data sandi (*cipher*text), kemudian data sandi tersebut dapat hanya dikembalikan ke dalam bentuk data asli hanya dengan menggunakan kunci (key) tertentu yang dimiliki oleh pihak yang berhak saja. [1], Untuk menjamin keamanan data dilakukan proses penyandian dengan tujuan agar data yang akan diberikan sesuai dengan penerima, dan tidak ada yang bisa membuka kecuali penerima langsung.Proses penyandian terdiri atas dua tahap, yaitu enkripsi dan dekripsi. Enkripsi adalah proses untuk mengubah *plain*teks menjadi *cipher*teks yang tidak akan bisa dimengerti. Sebelum mengirim data, data tersebut akan dilakukan enkripsi terlebih dahulu, untuk meningkatkan keamanan enkripsi pesan, pada proses enkripsi ditambahkan kunci yang juga akan diperlukan untuk proses dekripsi. Algoritma kriptografi merupakan suatu urutan langkah logis untuk penyelesaian masalah yang telah disusun secara sistematis. Sehingga 8 algoritma kriptografi adalah langkah-langkah logis dalam menyembunyikan pesan dari orang yang tidak memiliki hak akan pesan tersebut.

### 2.1. Algoritma AES

AES menjadi salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik. Secara garis besar algoritma enkripsi Rijndael diperlihatkan pada gambar dibawah ini.




*Gambar 1. Proses enkripsi AES*

Algoritma Rijndael yang berjalan pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut :

1. AddRoundKey : melakukan operasi XOR antara state awal dengan *cipher* key. Tahap ini disebut dengan initial round.
2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada persetiap putaran adalah :
   a) *SubBytes* : proses subtitusi byte dengan menggunakan tabel subtitusi (S-box).
   b) *ShiftRows* : proses pergeseran baris-baris *array state* (secara *wrapping*).
   c) *MixColumns* : proses mengacak data dimasing-masing kolom *array state*.
   d) *AddRoundKey* : operasi XOR antara *state* sekarang *round key*
3. *Final round* : proses pada putaran yang terakhir.
   *a) SubBytes*
   *b) ShiftRows*
   *c) AddRoundKey*

### 2.2. Algoritma Vigenere

Vigenere *cipher* mungkin adalah merupakan contoh yang terbaik dari *cipher* alfabet-majemuk. Algoritma ini telah dipublikasikan oleh seorang diplomat Perancis, bernama *Blase de Vigenere* di abad 16. Algoritma enkripsi jenis ini terkenal karena sangat mudah dipahami dan diimplementasikan. Teknik yang menghasilkan *ciphertext* bisa dilakukan menggunakan proses subtitusi angka maupun bujur sangkar vigenere.

*Tabel 1. Vigenere Cipher*

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Rumus operasi enkripsi vigenere *cipher* :

$Ci \equiv (Pi+Ki) mod\ 26$

Atau

Ci = (Pi + Ki) – 26 kalau hasil penjumlahan Pi dan Ki lebih dari 26

Rumus operasi dekripsi vigener *cipher* :

$Pi \equiv Ci-Ki\ mod\ 26$

Atau

Pi = (Ci – Ki) + 26 kalau hasil pengurangan Ci dengan Ki minus.

### 2.3. Studi literatur

Penelitian ini mengacu pada beberapa penulisan terkait penelitian yang telah dilakukan sebelumnya, yaitu sebagai berikut:

1) Rantika Dwi Amaliasari dan Ahmad Rosyadi [2] membuat penelitian tentang Implementasi Algoritma Enkripsi Aes Dan Vigenere Cipher

Pada Aplikasi Sms Berbasis Android. Diambil kesimpulan yaitu Aplikasi mengirimkan pesan terenkripsi dan dapat melakukan dekripsi kembali apabila kunci yang dimasukkan telah sesuai. Dua belah pihak pengguna harus sama-sama menginstal aplikasi ini untuk bisa bertukar pesan rahasia.

2) Prade Septo Negroho, dkk [3] membuat penelitian tentang Pengembangan Modul Enkripsi Dan Dekripsi Pada Php Dengan Modifikasi Metode Kriptografi Vigenere Cipher Dan Cipher Block Chaining. Dari penelitian dihasilkan modul enkripsi dan dekripsi pada PHP dengan metode modifikasi kriptografi Vigenere Cipher dan Cipher Block Chaining (CBC), Modul dapat melakukan generate panjang terhadap hasil enkripsi atau cipher teks berdasarkan panjang yang telah ditentukan, Modul melakukan enkripsi pada karakter ASCII dengan kode desimal 48 – 122, Modul dapat digunakan pada PHP dengan metode structural atau Object Oriented Programming (OOP).
3) Rika Rahmawati, Dani Raharjo [4] membuat penelitian tentang Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform Dan Kriptografi Aes 128 Bit Pada Smk Pgri 15 Jakarta. Metode Steganografi DCT (*Transform*) dan teknik Kriptografi AES 128 Bit sangat membantu dalam menjaga kerahasiaan pesan agar tidak mudah dibaca oleh orang yang tidak memiliki kepentingan. Proses *Embedded File* rata waktu penyelesaian sebesar 432,3 detik, serta berhasil mendapatkan mutu Steganografi yang baik dengan rata-rata nilai MSE yang relatif kecil sebesar 1,38 dB dan rata-rata nilai PSNR sebesar 47,66 dB. Proses Extract File memiliki waktu penyelesaian selama 139,6 detik, serta tingkat keberhasilan sebesar 100%
4) Aji Fitrah Marisman [5] melakukan penelitian tentang Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher Dan (AES) Untuk File Teksimplementasi Algoritma Kriptografi AES Untuk Enkripsi Dan Dekripsi Email. metode AES lebih aman dari metode Caesar Cipher karena *cipher*teks tidak dapat dipecahkan dengan metode *Brute Force Attack*. Hal ini terjadi karena metode AES menggunakan *bit/round* sehingga lebih aman. Dalam hal efisiensi waktu, metode AES lebih unggul dari metode Caesar Cipher dengan rata– rata perbedaan waktu sebesar 3000 ms. Dalam hal efisiensi ukuran, metode Caesar Cipher unggul dengan perubahan ukuran sebesar 0% sedangkan metode Advance Encryption Standard terjadi perubahan ukuran sebesar 33%. Hal ini terjadi karena pada Caesar Cipher, jumlah karakter output sama dengan jumlah karakter input sedangkan pada Advance Encryption Standard, jumlah karakter output lebih banyak dari jumlah karakter input. Aplikasi ini dirancang untuk membandingkan dua metode kriptografi.
5) Efrandi dkk [6] melakukan penelitian tentang Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher. merancang aplikasi kripto sistem ini melalui beberapa tahap yaitu tahap perancangan *diagram*, *flowchart*, layout/tampilan program, dan pengkodean algoritma Vigenere cipher yang diimplementasikan pada visual basic 6.0. Pada saat penulisan coding enkripsi dan dekripsi harus melakukan pengulangan yang sama tetapi dengan objek yang berbeda. Spesifikasi program aplikasi ini dapat dijalankan sesuai dengan spesifikasi teknis yang telah dirancang. Program aplikasi sistem kripto ini dapat menyembunyikan pesan yang penting terbaca menjadi tak terbaca dan mencari arti dari pesan yang rahasia menjadi bisa terbaca.

## 3. ANALISA MASALAH DAN PERANCANGAN PROGRAM

### 3.1 Metodologi Penelitian

Beberapa metode penelitian dan pengembangan yang digunakan dalam membangun aplikasi ini yaitu meliputi:

1. Metode kepustakaan dilakukan untuk mengumpulkan data dengan mencari dan membaca buku refrensi yang dapat menunjang penyusunan tugas akhir ini. Melihat dan membaca jurnal yang terkait.
2. Analisis Data, menganalisis Algoritma kriptografi yang digunakan yaitu algoritma AES dan algoritma VIGNERE, serta teknik – teknik yang digunakan. Membuat rancangan aplikasi sesuai hasil analisa yang telah dilakukan dengan membuat rancangan layar, arsitektur software, dan rincian prosedur.
3. Perancangan Sistem, merancang sistem aplikasi untuk mengimplementasikan algoritma AES dan algoritma VIGNERE dengan menggunakan bahasaa pemrograman vb.net dengan berbasis dekstop.
4. Uji Coba Aplikasi, setelah aplikasi dibuat, maka dilakukan uji coba terhadap aplikasi untuk evaluasi program.

### 3.2 Analisis dan Pemecahan Masalah

Yayasan KAPETA yang memiliki masalah dengan mengamankan data penting, data yang dikumpulkan seperti identitas para populasi kunci (komunitas

LGBT yaitu Gay, Waria, Transgender, dan lelaki suka lelaki) dan hasil dari pemeriksaan virus HIV AIDS. Data tersimpan di database dan dikirim setiap bulan ke Yayasan Spiritia sebagai Principle Recipient (PR) melalui surat elektronik begitu saja tanpa pengamanan berarti. Keamanan data kepada suatu database untuk menyimpan data dan informasi penting lainnya juga belum dilakukan dengan maksimal. Oleh karena itu, kemungkinan pencurian data sangat mudah dilakukan. Oleh karena itu membutuhkan sebuah aplikasi pengamanan database. Aplikasi berbasis dekstop sangat berguna karena database dapat diamankan sesudah menginput data di aplikasi SIS (Sistem Informasi Spritia) yang dibuat oleh Yayasan Spiritia sebagai Principle Recipient (PR) dan langsung dikirim kan sebagai laporan bulanan secara aman.

### 3.2.1 Pemecahan Masalah

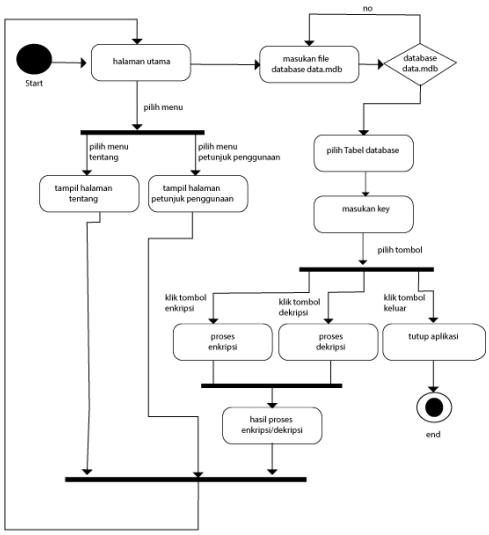
Pada Tugas Akhir ini menggunakan teknik enkripsi algoritma AES dan algoritma Vignere. AES 128 bit (*Advanced Encryption Standard*) merupakan modifukasi dari algoritma enkripsi standar DES (*Data Encryption Standard*) yang masa berlakunya dianggap usang karena faktor keamanan. Perkembangan komputer yang sangat cepat dianggap sangat membahayakan DES, sehingga pada tanggal 2 Maret tahun 2001 ditetapkan standar algoritma baru Rijndael sebagai AES. Kriteria pemilihan AES didasarkan 3 kriteria utama yaitu: harga, keamanan, dan karakteristik algoritma serta implementasinya. Algoritma AES mengunakan kunci kriptografi 128 bit untuk proses enkripsi dan dekripsi data pada blok 128 bit. Vigenere adalah salah satu algoritma kriptografi klasik untuk menyandikan suatu *plaintext* dengan teknik substitusi. Sandi Vigenere merupakan pengembangan dari sandi Caesar. Vigenere *cipher* pada dasarnya sangat rumit untuk dipecahkan. Meskipun begitu, Vigenere *cipher* tetap memiliki beberapa kelemahan. Salah satunya adalah mengetahui panjang kunci dengan menggunakan metode kasiski. Hal ini disebabkan karena umumnya terdapat frasa huruf yang berulang-ulang pada *ciphertext* yang akan dihasilkan.

### 3.3 Rancangan Desain Sistem

Perancangan merupakan proses yang dilakukan untuk merancang aplikasi terebut. Perancangan sistem yang dibuat secara umum adalah enkripsi dan dekripsi mengunakan metode AES 128 bit dan Vigenere berbasis desktop, adapun beberapa tahap dalam perancangan aplikasi adalah sebagai berikut

### 3.3.1 *Statechart Diagram*

*Statechart diagram* menggambarkan perubahan keadaan dan transisi (dari antara satu *state* ke *state* lainnya) suatu objek pada sistem sebagai akibat dari proses yang diterima.



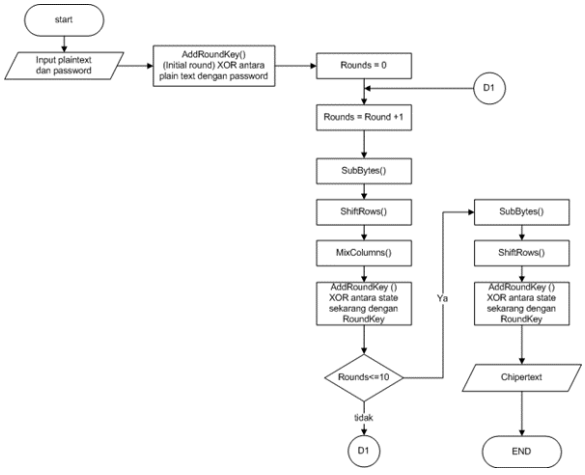

*Gambar 2 : Gambar Statechart Diagram Aplikasi Keamanan Database*

### 3.4 *Flowchart* Aplikasi

Inti dari aplikasi ini terdapat pada halaman utama, panduan penggunaan aplikasi, tentang aplikasi. Pada halaman tersebut terdapat fasilitas pengamanan *database* dengan teknik enkripsi dan dekripsi menggunakan algoritma AES 128 bit dan algoritma Vigenere.

### 3.5 *Flowchart* Enkirpsi AES-128

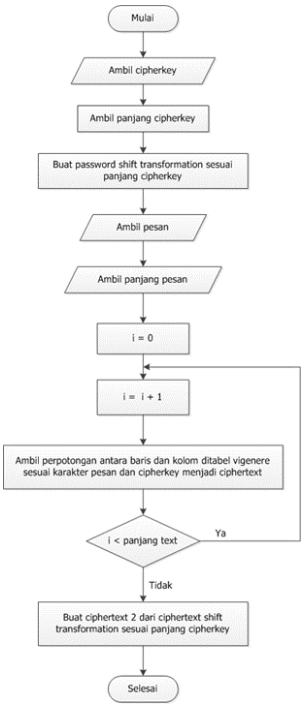
Berikut adalah flowchart proses Enkripsi AES 128



*Gambar 7 : Flowchart Enkripsi AES-128*

### 3.6 *Flowchart* Enkirpsi Vigenere

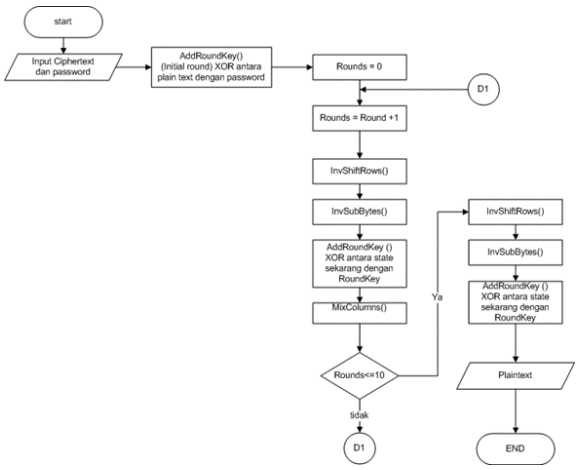
Berikut flowchart alur enkripsi algoritma Vigenere.




*Gambar 8 : Flowchart Enkripsi Vigenere*

### 3.7 *Flowchart* Dekirpsi AES 128

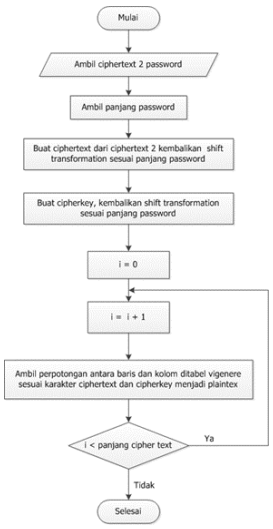
Berikut merupakan flowchart Dekirpsi AES 128.




*Gambar 9 : Flowchart Dekripsi AES 128*

### 3.8 *Flowchart* Dekirpsi Vigenere

Berikut merupakan flowchart Dekirpsi Vigenere.




*Gambar 10 : Flowchart Dekripsi Vigenere*

### 3.9 Algoritma Halaman Utama

Alur algoritma berikut akan menjelaskan proses yang terjadi pada halaman utama. Pada halaman ini proses enkripsi dan dekripsi akan dilakukan.

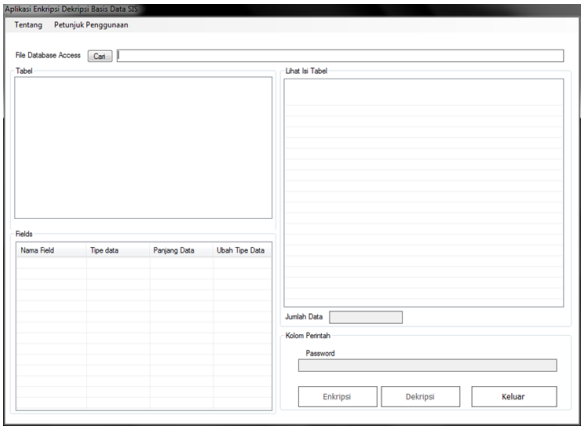
1. Tampilkan halaman *home*
2. *Input* Pilih Menu
3. If pilih = "Tentang" *Then*
4. Tampilkan halaman Tentang
5. *Else* if pilih = "Panduan Penggunaan" *Then*
6. Tampilkan halaman Panduan Penggunaan
7. Pilih *file database*
8. Pilih Tabel

```
9.  Pilih tombol
10. Masukan Key
11. If pilih tombol = “enkripsi” then
12.   If key = null then
13.       Peringatan “Key belum isi”
14.       Kembali ke baris 10
15.   Else
16.       Proses enkripsi
17.       Munculkan tabel yang sudah di enkripsi di
          kolom tabel
18.       Kembali ke baris 8
19.   End if
20. If pilih tombol = “dekripsi ” then
21.   If key = null then
22.       Peringatan “Key belum isi”
23.       Kembali ke baris 10
24.   Else
25.       Proses Dekripsi
26.       Munculkan tabel yang sudah di dekripsi di
          kolom tabel
27.       Kembali ke baris 8
28.   End if
29. Else If pilih tombol = “keluar’’ then
30.       Keluar aplikasi
31. End if
```

## 4. HASIL DAN PEMBAHASAN

### 4.1 Tampilan Layar Utama

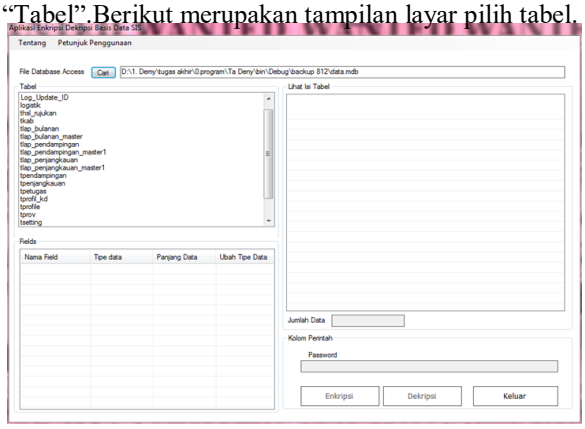
Saat pengguna memulai aplikasi ini maka akan muncul halaman utama pada aplikasi kriptografi ini. Pada layar utama ini terdapat pula *menu bar*, kolom yang berisi tabel-tabel, kolom field isi tabel, dan kolom tombol kontrol. Berikut tampilan saat pengguna memulai aplikasi.




*Gambar 11 : Halaman Utama Pilih Tabel*

### 4.2 Tampilan Layar Pilih Tabel

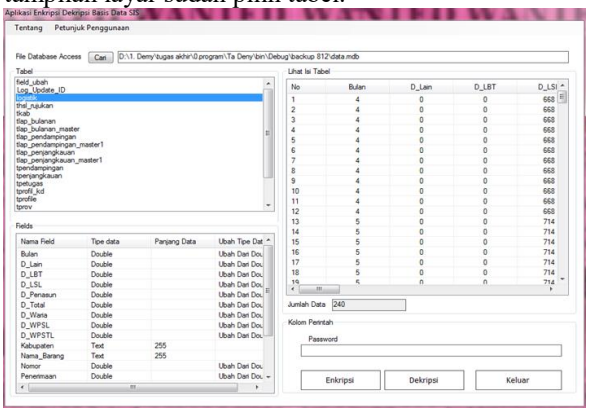
Selanjutnya pengguna dapat memilih tabel mana yang akan di enkripsi atau didekripsi dengan cara memilih salah satu tabel yang muncul di list box “Tabel”.Berikut merupakan tampilan layar pilih tabel.




*Gambar 12 : Halaman Utama Pilih Tabel*

### 4.4 Tampilan Layar Sudah Pilih Tabel

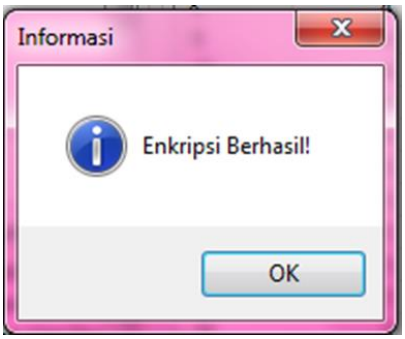
Data akan muncul juga dikolom field (kiri bawah) dimana berisi nama field tabel database yang dipilih, jumlah ukuran field tabel database yang dipilih, tipe data field database, dan tipe data field yang diubah sesuai aturan enkripsi atau dekripsi dan memasukan key yang akan digunakan. Berikut merupakan tampilan layar sudah pilih tabel.




*Gambar 13 : Halaman Utama Sudah Pilih Tabel*

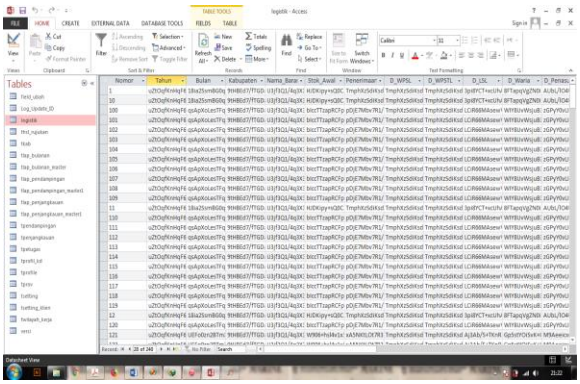
### 4.5 Tampilan Kotak Dialog Proses Berhasil

Bila user sudah memilih tabel yang mana akan dienkripsi dan telah memasukkan password pada form yang sudah tersedia, pengguna dapat menekan tombol enkripsi. Tunggu beberapa saat karena proses ekripsi sedang berjalan (lama proses tergantung jumlah data yang terdapat di tabel database yang sedang dienkripsi). Bila proses enkripsi selesai dan berhasil, maka otomatis akan muncul notifikasi Enkripsi Berhasil yang berada di tengah aplikasi.




*Gambar 14 : Tampilan Kotak Dialog Proses Berhasil*

Maka data yg disimpan tadi akan tersimpan di dalam database, berikut adalah tampilan data yang disimpan di database.



*Gambar 15 : Tampilan Hasil Enkripsi pada Database*

### 4.6 Tabel Pengujian

Dalam tabel pengujian kali ini, akan dibahas beberapa tabel yang telah diuji pada aplikasi keamanan *database* yang telah dibuat dengan mengimplementasikan metode AES dan Vignere sebagai enkripsi dan dekripsi *database*.

#### 4.6.1 Tabel Pengujian Enkripsi

*Tabel 2 : Hasil Pengujian Enkirpsi*

| NO | Nama Tabel | Jumlah *Row* | Jumlah *Field* | password | Waktu Proses | Status | Keterangan |
|---|---|---|---|---|---|---|---|
| 1 | logistik | 240 | 18 | kapeta | 00:00:02.861 | berhasil | |
| 2 | thsl_rujukan | 4286 | 38 | kapeta | 00:19:52.124 | berhasil | |
| 3 | tkab | 531 | 3 | kapeta | 00:00:01.708 | Berhasil | |
| 4 | tlap_penjangkauan | 2094 | 29 | kapeta | 00:00:35.066 | Berhasil | |
| 5 | tpenjangkauan | 13279 | 45 | kapeta | 00:27:57.253 | berhasil | |
| 6 | tpetugas | 31 | 4 | kapeta | 00:00:00.801 | berhasil | |
| 7 | tprofil_kd | 8774 | 10 | kapeta | 00:00:52.212 | berhasil | |
| 8 | tprofile | 1 | 10 | kapeta | 00:00:00.187 | berhasil | |
| 9 | tprov | 34 | 2 | kapeta | 00:00:00.401 | Berhasil | |
| 10 | tsetting | 1 | 4 | kapeta | 00:00:00.249 | Berhasil | |
| 11 | versi | 1 | 4 | kapeta | 00:00:00.307 | Berhasil | |
| 12 | twilayah_kerja | 2 | 5 | kapeta | 00:00:00.480 | berhasil | |

Berdasarkan tabel pengujian proses enkripsi diatas didapatkan rata-rata waktu proses enkripsi adalah 00.04:06.982.

#### 4.7.2 Tabel Pengujian Dekripsi

*Tabel 3 : Hasil Pengujian Dekirpsi*

| NO | Nama Tabel | Jumlah *Row* | Jumlah *Field* | Password | Waktu Proses | Status | Keterangan |
|---|---|---|---|---|---|---|---|
| 1 | logistik | 240 | 18 | kapeta | 00:00:02.737 | berhasil | |
| 2 | thsl_rujukan | 4286 | 38 | kapeta | 00:19:01.224 | berhasil | |
| 3 | tkab | 531 | 3 | kapeta | 00:00:01.708 | Berhasil | |
| 4 | tlap_penjangkauan | 2094 | 29 | kapeta | 00:00:34.980 | Berhasil | |
| 5 | tpenjangkauan | 13279 | 45 | kapeta | 00:28:01.332 | berhasil | |
| 6 | tpetugas | 31 | 4 | kapeta | 00:00:00.507 | berhasil | |
| 7 | tprofil_kd | 8774 | 10 | kapeta | 00:00:47.654 | berhasil | |
| 8 | tprofile | 1 | 10 | kapeta | 00:00:00.349 | berhasil | |
| 9 | tprov | 34 | 2 | kapeta | 00:00:00.428 | Berhasil | |
| 10 | tsetting | 1 | 4 | kapeta | 00:00:00.258 | Berhasil | |
| 11 | versi | 1 | 4 | kapeta | 00:00:00.350 | Berhasil | |
| 12 | twilayah_kerja | 2 | 5 | kapeta | 00:00:00.320 | berhasil | |

Berdasarkan tabel pengujian proses dekripsi diatas didapatkan rata-rata waktu proses dekripsi adalah 00:04:02.654

### 4.8 Analisa Program

Setelah dilakukan analisa dari hasil pengujian aplikasi kriptografi dengan cara membandingkan hasil fungsi enkripsi dan dekripsi, dapat ditemukan beberapa kelebihan dan kekurangan, yaitu sebagai berikut :

#### 4.8.1 Kelebihan

*1)* Dapat dioperasikan di semua komputer dimana aplikasi ini berada, sehingga lebih fleksibel untuk segala jenis operating sistem.
2) Proses enkripsi dan dekripsi berjalan lancar untuk file *mdb yang dijalankan dengan MS Access.
3) Pengguna bisa memilih salah satu atau lebih tabel yang akan dienkripsi atau didekripsi.
4) Aplikasi ini sangat mirip akan aplikasi penginputan data (Aplikasi SIS), sehingga pengguna akan tidak merasa kesulitan.
5) Kolom password tidak di sembunyikan saat memasukan password sehingga pengguna dapat mengecek ulang atau mencatat sehingga dapat di enkripsi kembali.
6) Pengguna dapat mengecek setiap isi tabel *database* sehingga tidak perlu lagi mengecek ulang melalui aplikasi MS Access.
7) Ukuran aplikasi tidak terlalu besar
8) Tidak banyak menu yang dapat membingungkan pengguna
9) Dapat digunakan tanpa sambungan internet.
10) Aplikasi ini dikhususkan untuk mengamankan *database* *mdb dari yayasan kapeta

#### 4.8.2 Kekurangan

1) Aplikasi ini tidak dapat mendeteksi apakah tabel sudah di-enkripsi/dekripsi sebelumnya.
2) Lama proses enkripsi atau dekripsi tergantung banyak jumlah data yg terdapat di tabel yang dienkripsi atau didekripsi.
3) Aplikasi ini tidak dapat mendeteksi saat password pada tabel yang sudah di enkripsi salah atau tidak.
4) Ukuran file sebelum dan setelah melakukan meng-enkripsi/dekripsi tedapat pertambahan ukuran file.

## 5. KESIMPULAN

Berdasarkan pembahasan diatas maka ditarik kesimpulan sebagai berikut :

a. Kriptografi algoritma *Advanced Encription Standart 128 bit* (AES) dan algoritma vigenere dapat diimplementasikan untuk aplikasi keamanan dokumen.
b. Aplikasi kriptografi ini dapat melakukan proses enkripsi-dekripsi tabel *file database* yang berformat *mdb dengan lancar. Dengan demikian permasalahan yang ada dapat diselesaikan dalam hal pengamanan data.
c. Aplikasi ini hanya dikhususkan untuk pengamanan basis data dari aplikasi Sistem Informasi Spirtia saja.
d. Adanya program aplikasi kriptografi, proses penyimpanan dan pertukaran informasi menjadi lebih aman.
e. Tanpa *key* yang tepat, maka siapapun tidak dapat membuka file yang telah di enkripsi. Aplikasi ini tidak dapat memeriksa dan memproses key salah saat proses dekripsi dilakukan.
f. Tabel dengan jumlah *fields* 45 dan *rows* 13279 membutuhkan waktu proses enkripsi selama 27 menit 57 detik 252 milidetik dan 28 menit 1 detik 332 mii detik untuk mendekripsi kembali tabel tersebut. Sedangkan untuk tabel dengan jumlah *field* sebanyak 3 dan *rows* sebanyak 531 membutuhkan waktu proses enkripsi selama 1 detik, 708 mili detik. Hal ini menunjukan bahwa waktu proses enkripsi dan dekripsi, tergantung banyaknya jumlah *row* dan jumlah *field* dari tabel *database* yang diproses.

## 6. DAFTAR PUSTAKA


[1] Munir, Rinaldi. 2006. Kriptografi. Bandung: Informatika Bandung.

[2] Amaliasari, Rantika Dwi, dan Ahmad Rosyadi,. 2015, Implementasi Algoritma Enkripsi Aes Dan Vigenere Cipher Pada Aplikasi Sms Berbasis Android, Jurnal Ilmiah, Universitas Dian Nuswantoro, Semarang.

[3] Negroho, Prade Septo, Dkk. 2014, Pengembangan Modul Enkripsi Dan Dekripsi Pada Php Dengan Modifikasi Metode Kriptografi Vigenere Cipher Dan Cipher Block Chaining, Jurnal, Universitas Ahmad Dahlan. Vol 2, Nomor 1 / Februari 2014.

[4] Rahmawati, Rika, dan Dani Raharjo. 2016, Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform Dan Kriptografi Aes 128 Bit Pada Smk Pgri 15 Jakarta, Jurnal, Universitas Budi Luhur, Vol 2, Nomor 1 / April 2016.

[5] Marisman, Aji Fitrah, 2015, *Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher Dan Advance Encryption Standard (Aes) Untuk File Teksimplementasi Algoritma Kriptografi Aes Untuk Enkripsi Dan Dekripsi Email*, Jurnal, Politeknik Negeri Jakarta. Vol 19, Nomer 3 / Desember 2015.

[6] Efrandy, dkk. 2014, *Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher*, Jurnal, Universitas Dehasen Bengkulu. Vol 10, No. 2 / September 2014