ISSN : 2548-6985

Aplikasi Kriptografi Database MySQLMenggunakan Metode Markel Helman

[1)] Ahmad Rifai
STMIK Budi Darma Medan, Jl. Sisingamangaraja No. 338 Medan, Sumatera Utara, Indonesia
E-Mail : ahmadrifailbs@yahoo.co.id

[2)] Hery Sunandar
STMIK Budi Darma Medan, Jl. Sisingamangaraja No. 338 Medan, Sumatera Utara, Indonesia
E-Mail : hery_nandar@gmail.com

ABSTRAK

Keamanan merupakan salah satu hal yang sangat penting dalam penyimpanan data, khususnya penyimpanan data pada Database yang didalamnya terdapat banyak ancaman dari pihak yang tidak bertanggungjawab.

Kriptografi merupakan metode dengan menyandikan isi informasi (plaintext) menjadi isi yang sulit atau bahkan tidak dipahami melalui proses enkripsi. Untuk memperoleh kembali informasi yang asli dapat dilakukan dengan proses dekripsi, yang tentunya dengan menggunakan kunci yang benar.

Untuk melindungi akses data dari pihak-pihak yang tidak berkepentingan tersebut maka sangat diperlukan enkripsi dan dekripsi. Agar dapat dilakukan dengan baik, dibutuhkan suatu algoritma untuk enkripsi dan dekripsi. Metode yang digunakan disini adalah Metode Merkle Hellman.

Kata Kunci : **Pengamanan, Merkle Hellman, Kriptografi.**

PENDAHULUAN

Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Hal tersebut tentu saja akan menimbulkan resiko bila informasi yang sensitif dan berharga tersebut di buka oleh orang-orang yang tidak berhak. Keamanan data dari sistem informasi sangat berperan penting, untuk menunjang keaslian dari data tersebut agar tidak mudah dirubah oleh orang yang tidak bertanggung jawab. Banyak sekali permasalahan pada komputer seperti data asli hilang, meskipun telah menggunakan pengamanan data seperti *password* tetap saja ada yang sanggup menembusnya.

Oleh karena itu, untuk menghindari agar hal tersebut tidak terjadi, maka lebih baik jika menggunakan sistem pengamanan data yang sulit ditembus, seperti enkripsi dan dekripsi data pada kriptografi. Kriptografi secara umum digunakan dalam bidang keamanan data, teknik yang digunakan adalah merubah data ke dalam bentuk yang tidak dapat dimengerti dengan menggunakan kunci *asimetris* dalam proses enkripsi dan dekripsinya.

Kriptografi *(cryptography)* berasal dari Bahasa Yunani: *"cryptos"* artinya *"secret"* (rahasia), sedangkan *"graphein"* artinya *"writing"* (tulisan). Jadi, kriptografi berarti *"secret writing"* (tulisan rahasia). Ada beberapa defenisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Defenisi yang dipakai dalam buku-buku lama (sebelum tahun 1980-an) menyatakan kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Maka data tersebut besar kemungkinan terjamin keamanannya. Dalam hal ini penulis tertarik untuk menjaga kerahasian data yang berada dalam *database* yang berupa data text[1].

Database merupakan kumpulan informasi yang disimpan didalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer, *Database* digunakan untuk menyimpan data atau informasi yang terintegrasi dengan baik didalam komputer dan *Software* yang digunakan untuk membuat *database* tersebut adalah *mysq l*[2].

Mysql adalah sebuah perangkat lunak sistem manajemen basis data SQL (bahasa inggris: *database management system*). *Mysql* dimiliki dan disponsori oleh sebuah perusahaan komersial Swedia yaitu *MYSQL AB*. Mysql *merupakan software database open sourse* yang paling populer didunia dimana saat ini digunakan lebih dari 100 juta pengguna diseluruh dunia. Mysql pertama kali dibuat dan dikembangkan di Swedia, yaitu oleh David Axmark, Allan Larsson dan Michael "Monty" Widenius. Mereka mengembangkan Mysql sejak tahun 1980-an.

Salah satu cara untuk melindungi terjadinya pencurian *database* tersebut sangat diperlukan enkripsi dan deskripsi pada *database* yang disimpan dalam basis data tersebut. Dalam hal ini maka metode yang

ISSN : 2548-6985

tepat untuk mengamankan *database* tersebut adalah metode *Markel Helman*.

Martin Hellman adalah seorang profesor teknik listrik di Stanford University dan *Ralph Merkel* dari *University of California* di Berkley. Pada tahun 1975 Whitefield mengembangkan konsep kunci *Asimetris* yang dibuka kemungkinan operasi *Kripto-sistem* dengan kunci publik dan swasta. Pada tahun 1976, menggunakan fungsi satu arah dan aritmatika modular, *Hellman* telah mengembangkan strategi untuk memecahkan masalah pertukaran kunci.

Metode *Merkel Helman* menggunakan kunci *Asimetris* dalam prose enkripsi dan dekripsi data menjadi bentuk lain akan tetapi menjadi tidak dapat dimengerti pihak lain walaupun data telah dimiliki atau dicuri.

Enkripsi adalah proses transformasi informasi dengan bantuan sebuah algoritma (disebut *cipher*) untuk membuatnya terbaca kepada siapa pun kecuali mereka yang memiliki pengetahuan khusus biasanya disebut sebagai kunci

Berdasarkan uraian pada latar belakang masalah di atas, maka yang menjadi rumusan masalah adalah Bagaimana menetukan spesifikasi *database* yang akan dienkripsi ? Bagaimana menerapkan metode *Markel Helman* pada proses enkripsi dan dekripsi *record-record* dalam tabel ? Bagaimana merancang aplikasi enkripsi dan dekripsi *database mysql* ?

Adapun tujuan dari penelitian yang akan diberikan dalam perancangan aplikasi yaitu Untuk mengetahui proses enkripsi dan dekripsi *database mysql* dengan metode *Markel Helman.*

Adapun manfaat yang didapatkan dalam penelitian ini adalah sebagai berikut: Dapat membantu pengguna dalam mengenkripsi *database* miliknya sehingga orang lain tidak mengerti apa isi dari *database* tersebut. Dapat menghasilkan sebuah aplikasi yang dapat digunakan untuk enkripsi dan dekripsi *database* menggunakan algoritma *markel helman*.

Aplikasi adalah sistem program komputer untuk pemakai tertentu yang dapat memecahkan masalah tertentu atau melakukan kegiatan tertentu. Contoh: menghasilakn kuitansi, bon, mencetak laporan ataupun memasukkan data-data baru ke dalam *file*[6].

Contoh-contoh aplikasi ialah program pemroses kata dan *Web Browser*. Aplikasi akan menggunakan sistem operasi (OS) komputer dan aplikasi yang lainnya yang mendukung. Secara historis, aplikasi adalah *Software* yang dikembangkan oleh sebuah perusahaan. Contoh utama aplikasi adalah pengolahan kata, lembar kerja dan pemutar media. Beberapa aplikasi yang digabung bersama menjadi suatu paket kadang atau disebut juga sebagai suite aplikasi (*Application Suite*). Contohnya adalah *Microsoft Office* dan *Open Office.org*, yang menggabungkan suatu aplikasi pengolahan kata, lembar kerja, serta beberapa aplikasi lainnya. Berdasarkan uraian defenisi aplikasi diatas dapat ditarik kesimpulan bahwa aplikasi adalah suatu perangkat lunak komputer yang memanfaatkan keamanan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna.

Cryptography (kriptografi) berasal dari bahasa Yunani yaitu dari kata crypto yang berarti penulisan *secret* (rahasia), sedangkan graphein artinya *writing* (tulisan). Jadi secara sederhana dapat diartikan *secret writing* (tulisan rahasia). Definisi lain dari kriptografi adalah sebuah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Menurut terminologinya, kriptogrofi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu:

Pada prinsipnya, Kriptografi memiliki 4 komponen utama yaitu:

1. *Plaintext*, yaitu pesan yang dapat dibaca
2. *Ciphertext*, yaitu pesan acak yang tidak dapat dibaca
3. *Key*, yaitu kunci untuk melakukan teknik kriptografi
4. *Algorithm*, yaitu metode untuk melakukan enkripsi dan dekripsi[1].

Metode kriptografi *Merkel Hellman* atau umumnya dikenal dengan sebutan merupakan *cipher* yang ide awalnya dari metode kriptografi *One Time Pad*, yaitu kunci yang dibangkitkan secara *random* dan panjang kunci sepanjang plainteks yang akan dienkripsi. Tetapi pada algoritma kriptogarfi pembangkitan kunci-kunci tersebut secara otomatis dengan teknik berantai.

Metode ini memiliki aturan substitusi berdasar pada caesar *cipher* yaitu dengan pergeseran huruf-huruf. Kekuatan *cipher* ini terletak pada kunci yaitu nilai integer yang menunjukkan pergeseran karakter-karakter sesuai dengan operasi pada caesar *cipher*. Kekuatan kedua terletak pada barisan bilangan-bilangan yang berfungsi sebagai pengali dengan kunci. Barisan bilangan tersebut dapat berupa bilangan tertentu seperti deret bilangan ganjil, deret bilangan genap, deret *fibonancci*, deret bilangan prima, serta deret bilangan yang dapat dibuat sendiri.

ISSN : 2548-6985

Matriks dilambangkan dengan s_i atau *super increasing* {s1, s2,s3,….sn}.

Proses Enkripsi

Proses enkripsi diawali dengan menentukan kunci umum yang didapatkan dari kunci rahasia dengan ketentuan misalnya:

s_i = (1,6,13,27,60,135,280,567)
a = 600
p = 1093

keterangan :
s = bilangan super *increasing*
a = kunci *private*
p = bilangan pembagi

untuk mendapatkan kunci publik maka digunakan rumus

$t_i = a * s_i \bmod p$

dimana
t_i = kunci publik
a = kunci rahasia
s = bilangan super increasing
p = bilangan pembagi

dan dihitung seperti cara dibawah ini :

Tabel 1 Proses Pencarian Kunci Publik

A		s_i		p		t_i
980	*	1	mod	1089	=	600
980	*	6	mod	1089	=	333
980	*	13	mod	1089	=	177
980	*	27	mod	1089	=	954
980	*	60	mod	1089	=	63
980	*	135	mod	1089	=	414
980	*	280	mod	1089	=	294
980	*	567	mod	1089	=	432

Dari tabel di atas didapatkan hasil kunci publik sebagai berikut:

t_i =(980,435,761,324,1083,531,1061,270)

Untuk proses enkripsi setiap karakter diubah kedalam bentuk bilangan ASCII kemudian dikonversikan lagi kedalm bentuk bilangan biner. Misalkan karakter yang akan dienkripsikan adalah huruf “S” sebagai contoh. Huruf “S” diubah ke dalam bentuk ASCII (S = 83) agar dapat dipecah menjadi bilangan biner. Biner dari huruf “S” adalah 1010011. Setelah mendapatkan bilangan biner dari karakter yang dimaksud maka proses enkripsi dilakukan dengan rumus:

$t_i * x = \sum y$

dimana
t_i = kunci publik
x = bilngan biner karakter
y = hasil perkalian

Tabel 2 Proses Enkripsi

t_i		x		Y
600		0		0
333	*	1	=	333
177	*	0	=	0
954	*	1	=	954
63	*	0	=	0
414	*	0	=	0
294	*	1	=	294
432	*	1	=	432
Jumlah				2013

Maka hasil enkrip yang didapatkan dari huruf S adalah 2013

Proses Deskripsi

Setelah menerima pesan yang terenkripsi makan dilakukan proses deskripsi dengan menggunakan rumus

$z = a^{-1} y \bmod p.$

keterangan:
z = target sum / hasil perkalian
a = kunci private
a^{-1} = invers dari a
y = *chipertext* yang diterima
p = bilangan pembagi

a^{-1} belum diketahui nilainya. Untuk mendapatkan nilainya dapat digunakan algoritma extended eucidian gcd (p,a) dimana:

p = bilangan pembagi
a = kunci private

berikut adalah perhitungan invers dari a^{-1} dengan gcd(p,a) setelah diketahui (1093,600)

1093 = 1 * 600 + 493
600 = 1 * 493 + 107
493 = 4 * 107 + 65
107 = 1 * 65 + 42
64 = 1 * 42 + 23
42 = 1 * 23 + 19
23 = 1 * 19 + 4
19 = 4 * 4 + 3

Selanjutnya:

$t_0 = 0$
$t_1 = 1$
$t_2 = t_0 - q_1 t_1 = 0 - 1*1 = -1$
$t_3 = t_1 - q_2 t_2 = 1 - 1*(-1) = 2$
$t_4 = t_2 - q_3 t_3 = (-1) - 4*2 = -9$
$t_5 = t_3 - q_4 t_4 = 2 - 1*(-9) = 11$
$t_6 = t_4 - q_5 t_5 = (-9) - 1*11 = -20$
$t_7 = t_5 - q_6 t_6 = 11 - 1*(-20) = 31$
$t_8 = t_6 - q_7 t_7 = (-20) - 1*31 = -51$
$t_9 = t_7 - q_8 t_8 = 31 - 4*(-51) = 235$

Dari perhitungan tersebut didapatkan 235 sebagai invers dari a. Namun jika hasil adalah nilai negatif tidak dapat dilakukan perhitungan. Hasil yang didapatkan adalah negatif hasil ditambahkan dengan bilangan p pada gcd(p,a) agar menjadi positif. Contoh:

-286 + 1093 = 807

Jadi didapatkan hasil dari a^{-1} adalah:

600^{-1}=235

Setelah mendapatkan nilai dari a^{-1} proses deskripsi dapat dilanjutkan. Diketahui *chipertext* yang diterima adalah “750”.

ISSN : 2548-6985

Dengan rumus

$z = a^{-1} * 2013 \bmod 1093$
$z = 235 * 2013 \bmod 1093$
$= 473055 \bmod 1093$
$= 879$

Hasil 879 merupakan hasil sementara. Untuk mendapakan pesan maka dilakukan penjumlahan bilangan super *increasing* pada kunci rahasia hingga hasilnya sama atau berdekatan lebih besar dan lebih kecil dengan 879 seperti berikut.

s_i = (1,6,13,27,60,135,280,567)

total dari bilangan tersebut adalah

1+6+13+27+60+135+280+567 = 1089

dan 1089 tidak sama atau atau berdekatan lebih besar dan lebih kecil dengan 879, untuk mengatasi masalah tersebut maka dilakukan perhitungan dengan mengalikan setiap bilangan s_i dengan angka 1 atau 0 hingga didapatkan hasil penjumlahan sama atau berdekatan lebih besar dan lebih kecil 879.

0*1+1*6+0*13+1*27+0*60+0*135+1*280+1*567 = 880

Jika hasil penjumlahan yang didapatkan sama atau berdekatan lebih besar dan lebih kecil dengan 879 ambil kembali angka 1 dan 0 sesuai urutan perhitungan 0*1+1*6+0*13+1*27+0*60+0*135+1*280+1*567 . Kemudian pisahkan tanda tambah dan bilangan s_i sehingga didapatkan 01010011 berupa bilangan biner. 01010011 jika diubah ke dalam desimal adalah 83 dan karakter ASCII nya adalah “S”. maka deskripsi dari *chipertext* “750” adalah “S”

HASIL DAN PEMBAHASAN

Metode kriptografi Merkel Helman atau umumnya dikenal dengan sebutan merupakan *cipher* yang ide awalnya dari algoritma kriptografi *One Time Pad*, yaitu kunci yang dibangkitkan secara *random* dan panjang kunci sepanjang plainteks yang akan dienkripsi.

Tahap-Tahap Enkripsi dan Deskripsi

Adapun tahapan yang diperlukan untuk melakukan enkripsi dan deskripsi adalah seperti pada penjalasan di bawah ini:

a. Tentukan *plaintext*
b. Tentukan *secret key*
   s = (1,2,5,11,32,87,141)
   a = 200, p = 307
c. Hitung *public key* untuk enkripsi
   ti=a*si mod p
   s_i =(200,93,79,51,260,208,263).
d. Proses Enkripsi
   Ubah setiap huruf *plaintext* menjadi bilangan biner dan kalikan setiap angka bilangan biner dengan kunci publik s_i. Totalkan jumlah dari hasil perkkalian untuk mendapatkan *chipertext*.
e. Proses Deskripsi
   Proses deskripsi diawali dengan menghitung invers dari a. Hasil invers tersebut dikalikan dengan *chipertext* dan di*mod*kan dengan p. Hasil dari perhitungan tersebut jika hasilnya sama dengan biner plaintext dikalikan dengan s maka akan didapatkan *plaintext* awal.
f. *Output* yang dihasilkan adalah Kunci publik (s_i), Pesan terenkripsi, Pesan terdeskripsi.

Proses Enkripsi

Sebelum melakukan enkripsi terlebih dahulu menentukan *plaintext* database yang akan dienkripsikan. Untuk melihat isi *database* setelah *service* mysql-d aktif dapat dilihat dengan langkah-langkah berikut

1. Buka *command prompt*
2. Ketikkan cd\ kemudian enter
3. Ketik cd apache\mysql\bin dan enter
4. Pada sub direktori yang terbuka ketikkan kembali mysql dan enter
5. Maka akan muncul tampilan mysql>
6. Untuk menampilkan *database* ketikkan show databases; dan enter
7. Pilih database dengan *sintax use database* misalnya database mahasiswa. *Use database* mahasiswa; kemudian enter
8. Gunakan *show tables*; untuk menampilkan tabel-tabel yang ada dalam database tersebut.
9. Misalkan terdapat tabel tblmahasiswa.
10. Untuk melihat isi dari tabel login ketikkan perintah “select * from table login;” dan enter.
11. Setelah isi tabel mucul misalkan dengan field kode pengguna, nama, dan password.
12. Kita tentukan bagian field mana yang akan dienkripsikan misalkan password dengan kode pengguna “1108222”.
13. Gunakan perintah “select password from table login where kode pengguna=”1108222” kemudian enter untuk menampilkan password dari pengguna dengan kode “1108222” dengan password “123”
14. Seletah hasilnya muncul maka dilakukan proses enkripsi dengan langkah-langkah seperti berikut.

Tentukan kunci rahasia yang di dalamnya terdapat nilai bilangan super increasing s dan kata kunci a sebagai faktor pengali, p sebagai sisa hasil bagi.

s = (1,2,5,11,32,87,141)
a = 200
p = 307

Hitunglah dengan rumus s_i=a*s mod p untuk mendapatkan kunci publik

200 * 1 mod 307 = 200
200 * 2 mod 307 = 93
200 * 5 mod 307 = 79
200 * 11 mod 307 = 51
200 * 32 mod 307 = 260
200 * 87 mod 307 = 208
200 * 141 mod 307 = 263

Maka kunci publik adalah s_i =(200,93,79,51,260,208,263).

Setiap huruf dari *plaintext* diubah kebentuk ASCII agar dapat dipecah menjadi bilangan biner.

Tabel 3 Bilangan Biner Plaintext Password

Plaintext	ASCII	Biner
1	49	0110001
2	50	0110010
3	51	0110011

Setelah hasil enkripsi didapatkan maka gunakan perintah seperti dibawah ini untuk mengupdate isi tabel *database*.

"update table login set password='Èêd' where kode pengguna="1108222"

Maka isi tabel login pada field password dengan kode pengguna "1108222" akan ternkripsi.

Proses Deskripsi

Jika penerima telah menerima pesan yang terbentuk dari hasil enkripsi maka penerima memisahkan header pesan dengan pesan terenkripsi seperti pada penjelasan berikut. Pada proses pendeskripsian setiap hasil dari enkripsi tidak dapat langsung dideskripsikan. Mula-mula dilakukan perhitungan dengan rumus $z = a^{-1} y \bmod p$. Hitung dulu a^{-1} menggunakan algoritma extended eucidian gcd (a,b) dimana a adalah bilangan pembagi dan b adalah bilangan a^{-1} tanpa -1 untuk mencari invers dari a^{-1}. Maka untuk 200^{-1}:

307 = 1 * 200 + 107
200 = 1 * 107 + 93
107 = 1 * 93 + 14
93 = 6 * 14 + 9
14 = 1 * 9 + 5
9 = 1 * 5 + 4
5 = 1 * 4 + 1

Selanjutnya:

$t_0 = 0$
$t_1 = 1$
$t_2 = t_0 - q_1\ t_1 = 0 - 1*1 = -1$
$t_3 = t_1 - q_2\ t_2 = 1 - 1*(-1) = 2$
$t_4 = t_2 - q_3\ t_3 = (-1) - 1*2 = -3$
$t_5 = t_3 - q_4\ t_4 = 2 - 6*(-3) = 20$
$t_6 = t_4 - q_5\ t_5 = (-3) - 1*20 = -23$
$t_7 = t_5 - q_6\ t_6 = 20 - 1*(-23) = 43$
$t_8 = t_6 - q_7\ t_7 = (-23) - 1*43 = -66$

Jika hasil yang didapatkan adalah negatif maka hasil ditambahkan dengan bilangan a pada gcd(a,b)

Maka -66 + 307 adalah 241, jadi didapatkan hasil 200^{-1}=241

Untuk y = 435 yang tadinya adalah hasil enkripsi yang akan dideskripsikan:

Z = 241*435 mod 307
= 104835 mod 307
= 148

148 = 0*1 + 1*2 + 1*5 + 0*11 + 0*32 + 0*87 + 1*141

Maka hasilnya didapatkan biner 0110001 diubah ke dalam desimal adalah 49 dan carakter nya adalah "1".

Setelah semua hasil deskripsi didapatkan maka gunakan perintah:

"update table login set password="123" where kodepengguna='adm102'" kemudian enter. Maka isi tabel login akan terupdate dengan hasil deskripsi password tersebut.

Keterangan :
s = bilangan super *increasing*
a = kunci *private*
p = bilangan pembagi
s_i = kunci publik
x = biner *plaintext*
y = hasil perkalian x dengan s_i

Algoritma Enkripsi

Berikut ini adalah algoritma enkripsi:

```
Procedure algoritma {
        Input   : t = plaintext
                  k = bilangan super increasing
        output  : c = chipertext
}
Proses  : for (t:=0 to m-n) do
                j = 0
                while (j<n and t[i+j]=t[j]) do
                        ti = t mod (k);
                end while
                if(t>=n) then
                        c=ti
                end if;
          end for;
```

Algoritma Deskripsi

Berikut ini adalah algoritma deskripsi:

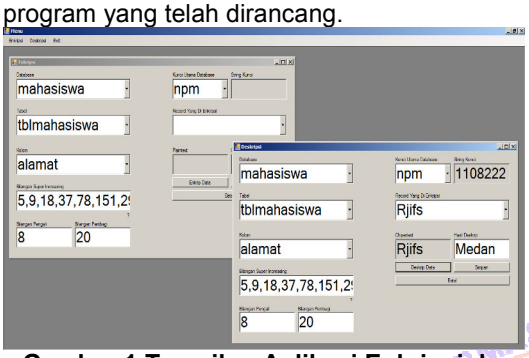
```
Procedure algoritma {
        Input   : c = chipertext
                  k = bilangan super increasing
                  x = bilangan pengali
                  y = bilangan pembagi
        output  : t = plaintext
}
Proses  : kp=(x*y)
          for (c:=0 to m-n) do
                j = 0
                while (j<n and c[i+j]=c[j]) do
                        ci = c mod (k);
```

ISSN : 2548-6985

```
        end while
        if(c>=n) then
                t=c_i
        end if;
end for;
```

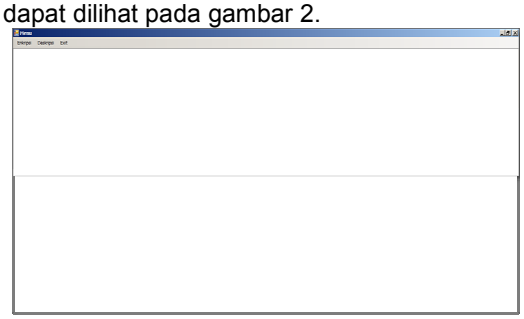
Hasil Aplikasi

Aplikasi enkripsi dan deskripsi yang telah dirancang merupakan aplikasi berbasis VB.NET 2008, dimana aplikasi ekripsi dan deskripsi tersebut dapat dijalankan sistem operasi. Berikut ini tampilan dari bentuk program yang telah dirancang.



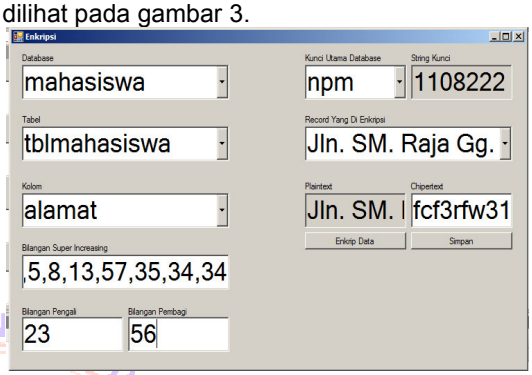
Gambar 1 Tampilan Aplikasi Enkripsi dan Deskripsi

Menu utama dapat dikatakan sebagai antar muka (*user interface*) antara *user* dan program. Menu utama menampilkan pilihan menu yang tersedia pada program. Pada menu utama aplikasi enkrip dan deskripsi tersedia 3 pilihan menu yaitu menu enkripsi untuk memenkripsi pesan yang menghubungkan ke *form* enkripsi dan menu deskripsi untuk mengubungkan ke *form* deskripsi dan menu exit untuk keluar dari program enkripsi dan deskripsi dengan metode merkle hellman. Berikut gambar untuk tampilan menu utama dapat dilihat pada gambar 2.



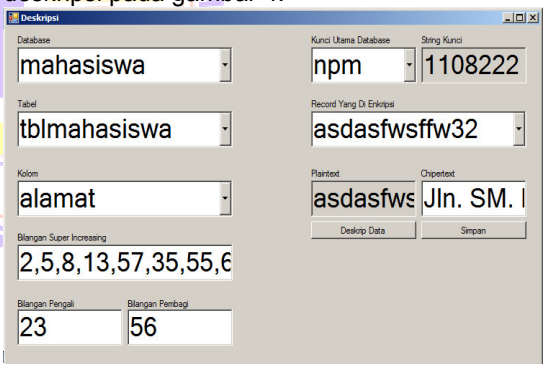
Gambar 2 Menu Utama

Form enkripsi digunakan untuk mengekripsikan text yang akan dikirim ke penerima. *Public key* didapatkan dari perhitungan bilangan super increasing. *Plaintext* adalah tempat menampilkan data yang akan dienkripsikan. Hasil enkripsi akan tampil ketika tombol enkrip data ditekan. Sebelum melakukan enkripsi terlebih dahulu ditentukan *record* apa yang akan dienkripsikan pada *database*. Kunci utama datadase adalah kunci setiap record yang akan dienkripsi atau sering disebut dengan *primary key* pada database. Kunci utama database inilah yang akan menjadi acuan untuk meng*update* isi dari database agar tidak terjadi kesalahan enkripsi. Kunci ini dapat berupa identitas yang tidak pernah sama dengan yang lain misalnya nomor KTP, nomor induk, npm atau jenis lain yang dapat dipastikan tidak sama tiap record. Berikut gambar untuk tampilan *form* enkripsi dapat dilihat pada gambar 3.



Gambar 3 Form Enkripsi

Form deskripsi digunakan untuk mendeskripsikan text yang diterima dari penerima. Berikut gambar untuk tampilan *form* deskripsi pada gambar 4.



Gambar 4 Form Deskripsi

KESIMPULAN

Setelah Melakukan analisa terhadap penerapan metode Merkle Hellman pada penyandian dalam database, maka penulis dapat menarik beberapa kesimpulan sebagai berikut :

1. Spesifikasi database yang akan dienkripsi adalah database dengan servis *mysql* dengan layanan *apache*.
2. Menerapkan mertode Herkle Hellman pada proses enkripsi dan deskripsi dilakukan dengan pembentukan kunci yang berasal dari bilangan super increasing, dimana bilangan super increasing dikalikan dengan bilangan pengali dan ambil sisa hasil

baginya dengan bilangan pembagi. Hasil dari perhitungan tersebut akan dijumlahkan dengan bilangan ascii dari setiap karakter yang terdapat pada plaintext/record tabel database yang dipilih.

3. Merancang aplikasi enkripsi dan deskripsi menggunakan Visual Basic .NET 2008 dengan menanfaatkan *tools* seperti *textbox*, *form*, *module*, *button* dan *class*.

DAFTAR PUSTAKA

1. Arius doni, “Pengantar Ilmu Kriptografi”. Penerbit Andi Publisher, Jakarta 2006.
2. Arby, “Manajemen Database Dengan Mysql”. Penerbit Andi, 2010.
3. Darmayuda Ketut, “Pemrograman Aplikasi Database Dengan Microsoft Visual Basic. Net 2008” ,Penerbit Elex Media komputindo.
4. Kadir Abdul, “Pengenalan Teknologi informasi”. Penerbit Andi, Jakarta 2006,
5. Sugiarti Y, “Analisis Dan Perancangan Unified Modeling Languange” , Penerbit Graha Ilmu, Jakarta 2014.
6. Syah Suhatman Surya, “Kamus Komputer”. Penerbit Rineka Cipta, Surabaya 2002.