Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma XOR

Andryanto A[1], Dasril[2]
[1,2]Program Studi Manajemen Informatika AMIK Ibnu Khaldun, Palopo, Sulawesi Selatan, Indonesia
[1]andryantoaman@gmail.com , [2]dasrilbachmid@gmail.com

Abstrak

Sistem penyimpanan data pada beberapa aplikasi yang dibuat saat ini, masih tergolong rendah dilihat dari kemanan data.Salah satu data pribadi guru, Sehingga tidak sedikit orang yang tidak bertanggung jawab melakukan pencurian data. Keamanan data diperlukan agar seseorang tidak dapat membaca, memindahkan, dan merusak data. Salah satu keamanan data menggunakan enkripsi, sehingga data tidak mudah untuk dibaca. Penelitian ini bertujuan untukmengimplementasikan algoritma xor sebagai aplikasi pengamanan data. metode pengujian sistem yang digunakan adalah metode pengujian white box . Hasil dari penelitian aplikasi pengamanan data menggunakan algoritma xor adalah mampu melakukan enkripsi pada data guru dan juga melakukan dekripsi agar data dapat kembali dapat terbaca, sehingga dapat memberikan kenyamanan pada pengguna aplikasi.

Kata Kunci : Dekripsi, Enkripsi, Algoritma, White Box, XOR.

1. Pendahuluan

Keamanan data adalah usaha mengamankan data dari pengubahan maupun akses yang tidak sah. Keamanan data difokuskan untuk memastikan kerahasian data[5]. Salah satu usaha penjagaan keamanan data adalah dengan mengenkripsi sebuah data agar tidak mudah untuk seseorang dapat melakukan pembacaan data[6].

Berbagai macam teknik yang telah digunakan untuk menjaga keamanan data atau melindungi informasi rahasia dari orang yang tidak berhak untuk mengetahuinya, salah satunya adalah menggunakan algoritma xor. Dalam proses pengamanan data terdapat dua proses yaitu pengubahan pesan yang dapat dibaca (plaintext) menjadi pesan yang tidak dapat dibaca (enkripsi) dan proses pengubahan dari pesan yang tidak dapat dibaca kemudian dikonversi ke pesan yang dapat dibaca (dekripsi)[2].

Dalam penelitian ini penulis bermaksud ingin mengimplementasikan algoritma xor sebagai aplikasi keamanan data, penelitian ini fokus pada keamanan data guru yang nantinya diharapkan aplikasi ini nanti dapat implementasikan pada sekolah-sekolah yang membutuhkan tingkat keamanan data yang baik.

2. Metodologi

Pembuatan aplikasi ini penulis menggunakan algoritma XOR untuk digunakan dalam pengaplikasian suatu aplikasi enkripsi dan dekripsi teks. XOR enkripsi, impelementasi algoritma XOR enkripsi dengan menggunakan fungsi aljabar boolean XOR.

Code:		
X	Y	XˆY

1	1	0
1	0	1
0	1	1
0	0	0

Gambar 1. Code 1

Pada gambar 1 terlihat bahwa jika semua masukan adalah tinggi (1), gerbang xor akan membangkit keluaran rendah(0) [8]. Namun bagaimana jika kita melakukan dua kali operasi XOR dua kali terhadap suatu bit dengan operand yang sama, maka hasilnya akan kembali seperti semula. Seperti contoh gambar 2 berikut.

Code:			
X	Y	XˆY	(XˆY)ˆY

1	1	0	1
1	0	1	1
0	1	1	0
0	0	0	0

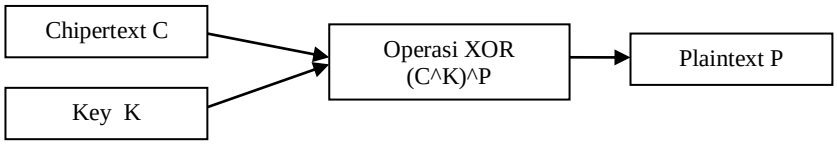
Gambar 2. Code 2

Dapat dilihat dari kedua gambar di atas, pada gambar pertama terlihat nilai pada variabel X yang di XOR kan dengan variabel Y dan menghasilkan nilai yang ada pada variabel X^Y. Namun, jika kita lihat pada gambar kedua, variabel X^Y di XOR kan lagi dengan variabel Y dan kemudian menghasilkan nilai yang sama dengan nilai yang ada pada variabel X. Sifat seperti ini yang dapat kita gunakan untuk membuat enkripsi sederhana.

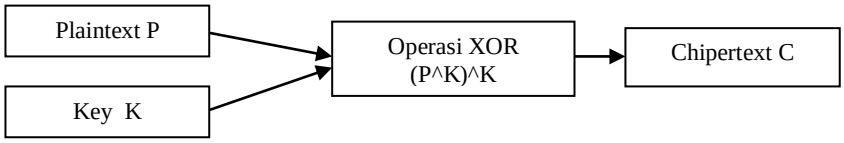
Misal terdapat karakter A = 01000001 di XOR kan dengan 10000000 maka hasilnya akan menjadi 11000001 atau karakter ⊥ dan jika di XOR kan lagi, maka akan kembali menjadi 01000001 atau A lagi.

Cara yang sebenarnya enkripsi XOR digunakan adalah untuk mengambil kunci dan mengenkripsi file dengan berulang kali dan menerapkan kunci untuk segmen berturut-turut dari file dan menyimpan output. Output akan menjadi setara dengan program acak sepenuhnya, sebagai kunci yang dihasilkan secara acak.
Skema enkripsi dan dekripsi :

Contoh sebuah plaintext yaitu P dan memiliki sebuah kunci yaitu K(ingat panjang kunci harus sama dengan plaintext dan sebaiknya tidak ada karakter yang diulang).



Gambar 3 contoh skema enkripsi teks



Gambar 4 contoh skema dekripsi teks

Pertama kita harus mendapatkan kode ASCII dari plaintext kemudian diubah ke bentuk biner. Hal yang sama juga harus dilakukan pada kunci yang dipilih. Setelah itu masing-masing karakter di XOR-kan dengan Key yaitu dengan membandingkan dua buah bit yang apabila pada salah satu bit nya bernilai Benar, maka hasil akhir operasi XOR tersebut adalah benar. Namun, bila kedua bit yang akan dibandingkan bernilai Salah atau keduanya bernilai Benar maka hasil akhir operasi adalah Salah.

Secara singkat, operasi XOR akan mengembalikan nilai 1 jika jumlah operand bernilai satu ganjil, jika tidak maka akan mengembalikan hasil 0. Berikut ini contohnya:

1 XOR 1 = 0
1 XOR 0 = 1
0 XOR 1 = 1
0 XOR 0 = 0

Pembuatan *chiper* (teks hasil enkripsi) melalui operasi XOR merupakan suatu algoritma enskripsi yang relatif sederhana. Teknik ini beroperasi sesuai dengan prinsip:

A XOR 0 = A,
A XOR A = 0,
(B XOR A) XOR A = B XOR 0 = B,

Suatu string teks dapat dienkripsi dengan menerapkan operasi XOR berbasis bit (*binary digit*) terhadap setiap karakter menggunakan *key* tertentu. Bagaimana mendekripsi outputnya untuk mendapatkan *plaintext* kembali? Dengan menerapkan operasi XOR terhadap chiper.Sebagai contoh, string "Andry" di ubah ke formar ASCII 8 bit lalu di ubah ke bentuk biner, untuk string "Andry" kode ASCIInya dapat dilihat pada tabel di bawah ini:

Tabel 5*ASCII* 8 Bit

Char	ASCCII Code	Binary	Char	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

Sumber : Teuku Taufik, 2013

Jadi stirng "Andry" jika di ubah kedalam bentuk biner menjadi 01000001 01101110 01100100 0111001001111001 dapat dienkripsi dengan suatu *key*"z" misalnya 01111010 sebagai berikut:

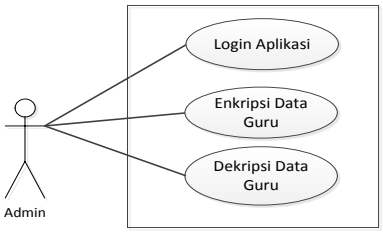
01000001 01101110 01100100 0111001001111001
01111010011110100111101001111010011111010
———————————————————————— (XOR)
0011101100010100 00011110 00001000 00000011 (Hasil)
Dan sebaliknya, untuk dekripsi adalah:
0011101100010100 00011110 00001000 00000011
01111010 01111010 01111010 0111101001111010
———————————————————————— (XOR)
01000001 01101110 01100100 0111001001111001 (Hasil)

Keterangan cara XOR biner:
Jika ada dua bilangan biner yang sama diXOR maka hasilnya tetap nol(0) tetapi jika ada dua bilangan biner yang berbeda maka hasilnya satu(1).
Keamanan algoritma XOR juga ditentukan dari panjang key yang digunakan.

3. Hasil dan Pembahasan

3.1. Rancangan Sistem

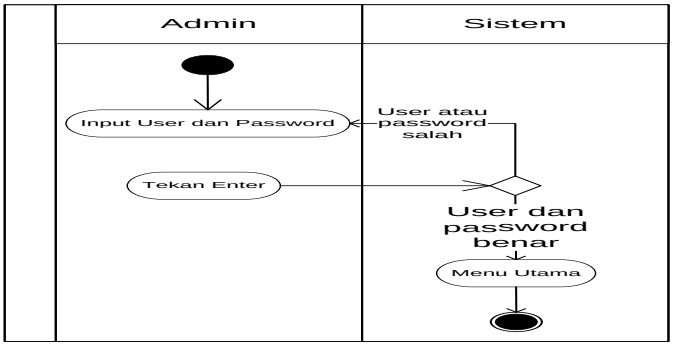
Use case merupakan rangkaian/uraian sekolompok yang saling terkait dan membentuk sistem secara teratur yang dilakukan atau diawasi oleh sebuah aktor[1]. Berikut ini use case diagram admin.



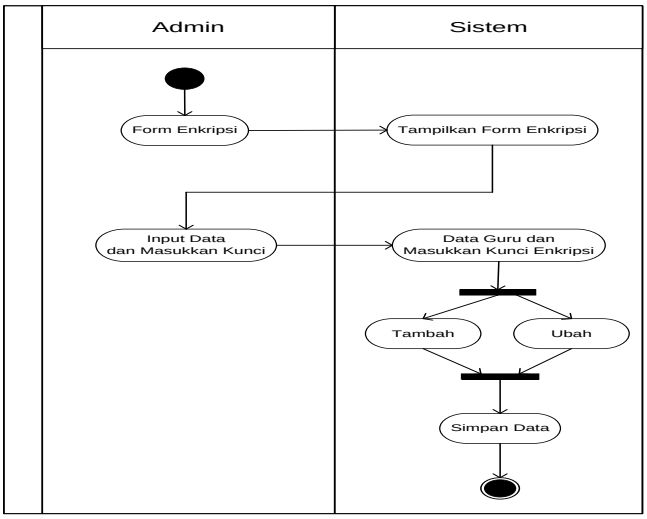
Gambar 5. Use Case Diagram

pada gambar 5, admin mengambil data pegawai dari pegawai setelah itu admin melakukan login untuk dapat mengkases sistem, setelah login admin menginput data guru dan memasukkan kunci enkripsi lalu menyimpan ke dalam database. Admin juga dapat mendekripsi data guru yang terlebih dahulu memasukkan kunci dekripsi.

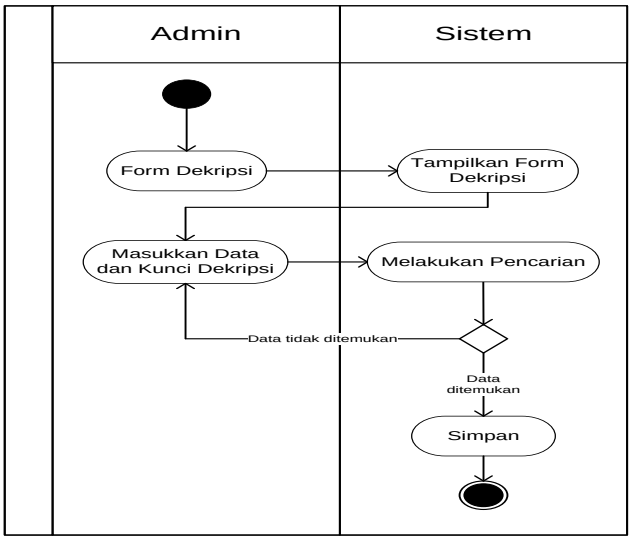
Diagram Activity menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, decision yang mungkin terjadi, dan bagaimana mereka berakhir [3]. Berikut ini diagram activity untuk login



Gambar 6. Diagram Activity Login



Gambar 7. Diagram Activity Enkripsi



Gambar 8. Diagram Activity Dekripsi

3.2. Pembahasan dan Hasil

Microsoft Visual Basic (VB) merupakan sebuah bahasa pemrograman yang menawarkan Integrated Development Environment (IDE) visual untuk membuat program perangkat lunak berbasis sistem operasi Microsoft Windows[4]. Berikut ini hasil tampilan aplikasi menggunakan program Visual Basic.

Gambar 9. Tampilan Form Login

Gambar 9 merupakan tampilan form login, dimana pengguna terlebih dahulu melakukan pengisian data User dan pasword yang telah disediakan.

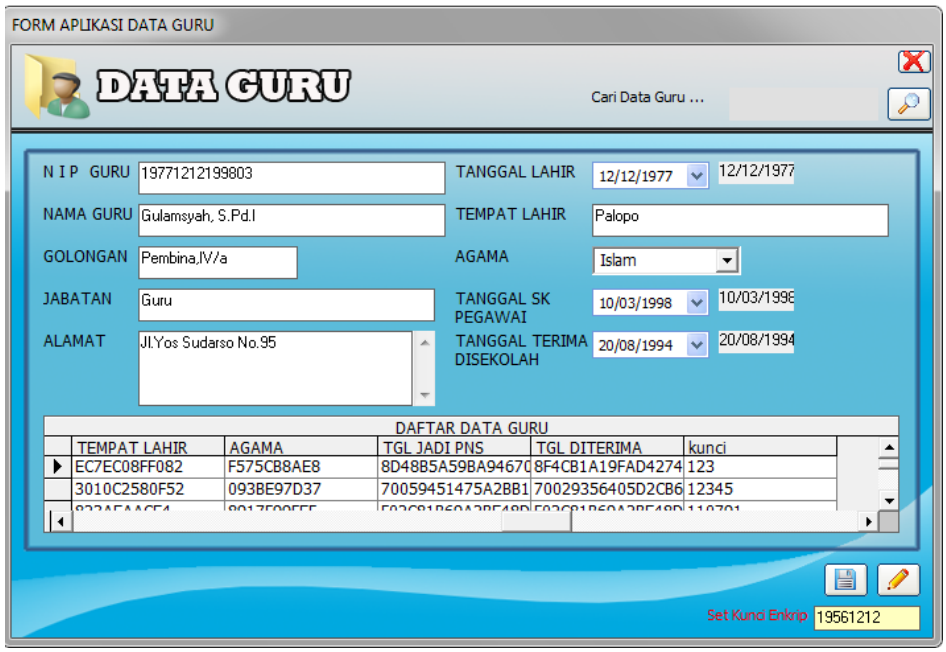
Gambar 10. Tampilan Form Menu Utama

Gambar 10 merupakan tampillan menu utama aplikasi pengamanan data guru, pilihan menu yang terdapat pada menu utama yaitu;

a. Tambah Data Guru / Enkripsi
Pada menu tambah data guru, pengguna aplikasi dapat melakukan penambahan data guru yang kemudian bisa di enkripsi atau bisa tanpa melakukan enkripsi.

b. Cari Data / Dekripsi
Untuk menu cari data, pengguna aplikasi melakukan pencarian data berdasarkan NIP, jika data ingin di dekripsi maka cantumkan password dekripsi.

c. Keluar
Menu keluar digunakan untuk menghentikan proses kerja program.

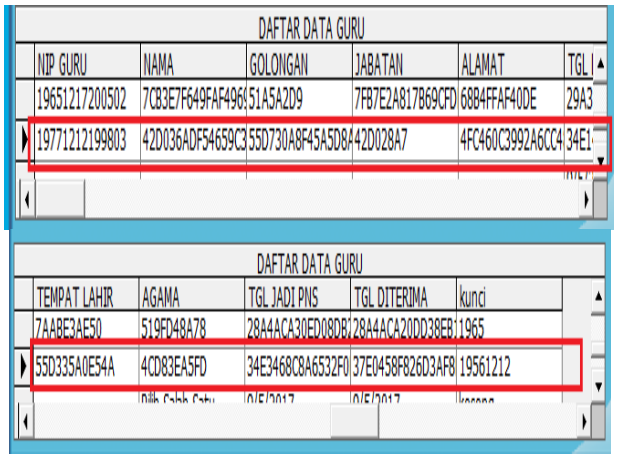


Gambar 11. Tampilan Form Enkripsi

Gambar 11 merupakan inputan data guru yang akan dienkripsi terdiri dari nama guru, golongan, jabatan, alamat, tanggal lahir, tempat lahir, agama, tanggal SK pegawai, tanggal terima disekolah, serta key untuk enkripsi. Berikut *Source Code* enkripsi algoritma xor dan hasil enkripsinya.

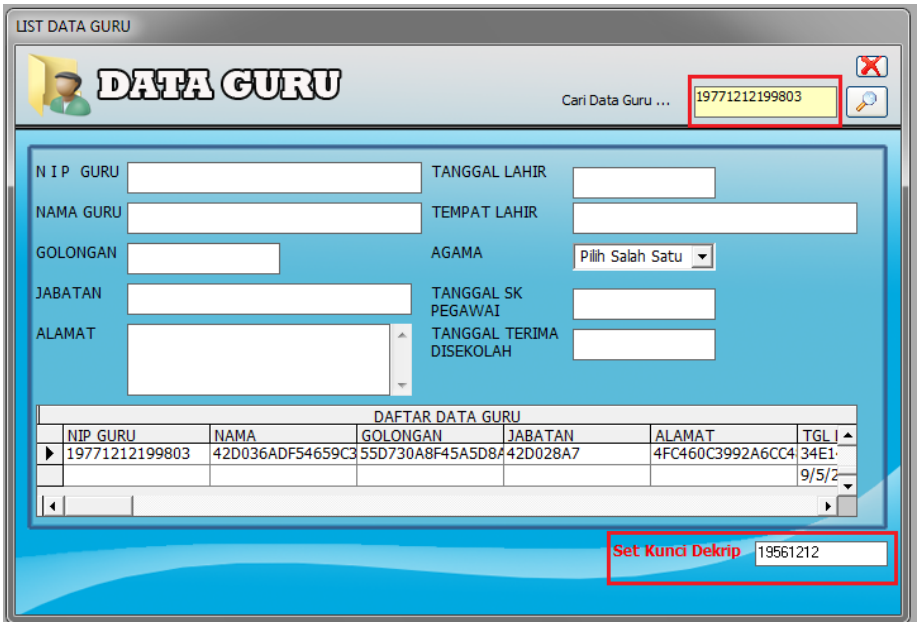
```
Sub enkrp1()
Dim x As Long
Dim eKey As Long, eChr As Byte, oChr As Byte, tmp$
Rnd -1
Randomize Len(txtPw.Text)
For i = 1 To Len(txtPw.Text)
   eKey = eKey + (Asc(Mid$(txtPw.Text, i, 1)) Xor Fix(255 * Rnd) Xor (i Mod 256))
Next
Rnd -1
Randomize eKey
oChr = Int(Rnd * 256)
For x = 1 To Len(Text2.Text)
   pp = pp + 1
   If pp > Len(txtPw.Text) Then pp = 1
   eChr = Asc(Mid$(Text2.Text, x, 1)) Xor Int(Rnd * 256) Xor Asc(Mid$(txtPw.Text, pp, 1)) Xor oChr
   tmp$ = tmp$ & Chr(eChr)
   oChr = eChr
Next
lnama.Caption = AsctoHex(tmp$)
End Sub
```

dari prosedur diatas merupakan salah satu contoh dari proses enkripsi “nama guru” , inputan nama guru dapat dilihat pada gambar 11, dan hasil enkripsi dapat dilihat pada gambar 12.



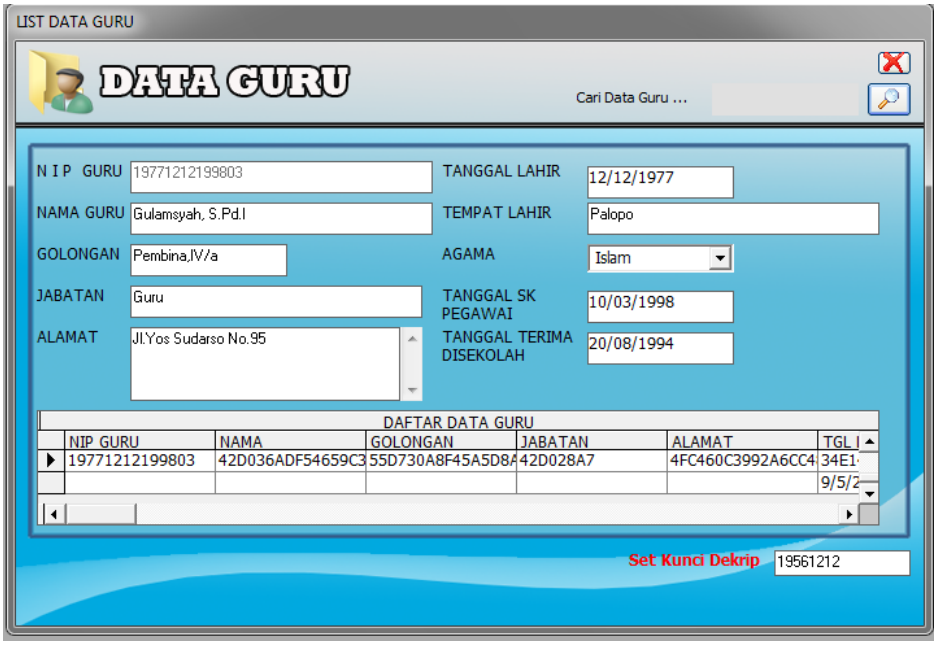
Gambar 12. Hasil Enkripsi

Pada gambar 12 merupakan data yang telah tersimpan dalam database yang dalam bentuk enkripsi. Data yang telah terenkripsi tidak dapat dilakukan perubahan data agar tidak mempengaruhi proses dekripsi. Pada pilihan pencarian data menu utama merupakan proses pencarian data yang akan di dekripsi. Berikut ini proses input pencarian data guru.



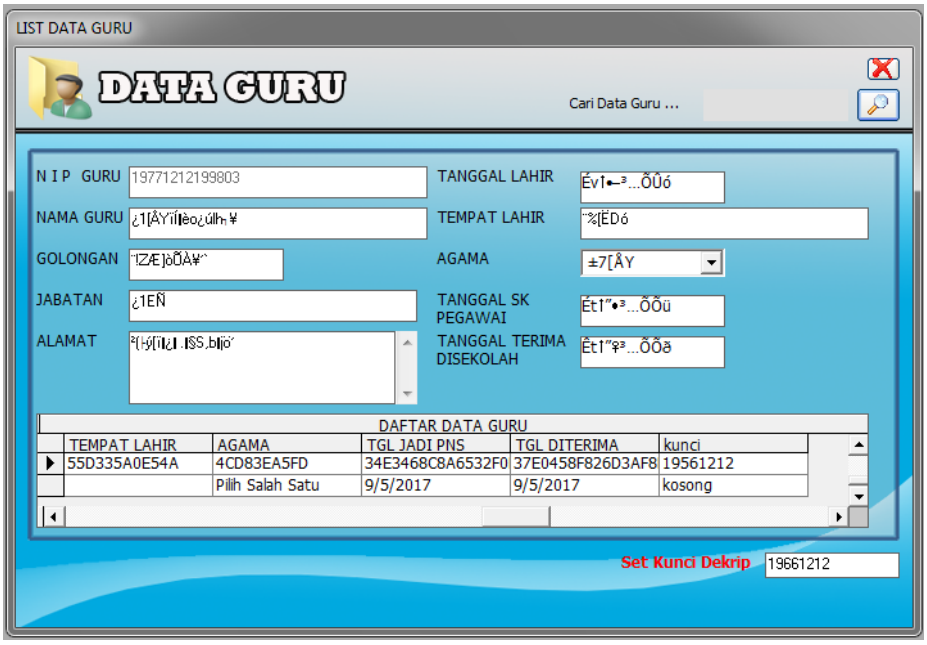
Gambar 13. Tampilan Form Dekripsi

Input NIP untuk melakukan pencarian data guru dan set kunci dekripsi, dimana kunci dekripsi sama dengan kunci enkripsi saat melakukan inputan data guru.



Gambar 14. Dekripsi

Jika data NIP dan kunci dekripsi sesuai dengan database maka akan menampilkan data guru seperti pada gambar 14.



Gambar 15. Kunci Dekripsi dan Data nip Guru tidak sesuai

Jika data nip guru dan kunci dekripsi tidak sesuai dengan database maka maka menampilkan seperti pada gambar 15. Data guru tidak dapat dibaca. Berikut ini source code untuk melakukan dekripsi.

```
Function dekrip()
Dim x As Long
Dim eKey As Long, eChr As Byte, oChr As Byte, tmp$
Rnd -1
Randomize Len(txtpsdk.Text)
For i = 1 To Len(txtpsdk.Text)
   eKey = eKey + (Asc(Mid$(txtpsdk.Text, i, 1)) Xor Fix(255 * Rnd) Xor (i Mod 256))
Next
Rnd -1
```

```
Randomize eKey
oChr = Int(Rnd * 256)
tmp$ = HexToAsc(nama.Caption) 'sumber data yang terenkrip
Text2.Text = ""  ' tujuan kolom dekrip
For x = 1 To Len(tmp$)
   pp = pp + 1
   If pp > Len(txtpsdk.Text) Then pp = 1
   If x > 1 Then oChr = Asc(Mid$(tmp$, x - 1, 1))
   eChr = Asc(Mid$(tmp$, x, 1)) Xor Int(Rnd * 256) Xor Asc(Mid$(txtpsdk.Text, pp, 1)) Xor oChr
   Text2.Text = Text2.Text & Chr$(eChr) ' tujuan kolom dekrip
Next
End Function
```

pada source code diatas merupakan salah satu function untuk melakukan dekripsi.

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulan dengan adanya aplikasi pengamanan data menggunakan algoritma xor dapat membantu pengguna aplikasi dalam pengolahan data guru serta aplikasi ini didukung enkripsi data sehingga tidak semua orang yang dapat membaca data yang telah di enkripsi. Selain itu juga dapat mendekripsi data, sehingga pengguna dapat membaca data.

Referensi :

[1] Jogiyanto. 2001. Analisis & Desain Sistem Informasi,Andi Offset, Yogyakarta.
[2] Munir, Rinaldi, 2012. Kriptografi. Bandung: Informatika.
[3] Nugroho Adi, Bunafit, 2005. MySQL dan UML untuk pemodelan Desain Program. Andi Offset. Yogyakarta.
[4] Raditya, Wibowo Herry. Dkk . 2012. Buku Pintar Vb.Net. Elex Media Komputindo. Jakarta.
[5] Sadikin, Rifki. 2012. Kriptografi untuk keamanan jaringan. Andi Offset. Yogyakarta
[6] Sianipar, RH.2016. Kompilasi Proyek Kriptografi dengan Visual Basic.Net. Andi Offset. Yogyakarta
[7] Taufik, Teuku. 2013. Kode Standar Amerika untuk Pertukaran Informasi Atau ASCII. http://www.teukutaufik.com/2013/03/tabel-ascii-8-bit_27.html. diakses pada tanggal 4 Januari 2017.
[8] University, Robotics. 2013. Gerbang logika X-OR. http://www.robotics-university.com/2013/01/gerbang-logika-x-or-exclusive-or.html. diakses pada tanggal 4 januari 2017.