IMPLEMENTASI KEAMANAN DATABASE DENGAN ENGGUNAKAN METODE *ADVANCED ENCRYPTION STANDARD (AES-256)* PADA SEKOLAH SMK ISLAM AL HIKMAH JAKARTA BERBASIS DESKTOP

Handoko[1)], Muhammad Ainur Rony, S.Kom.[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : aanhandokodoko@gmail.com[1)], ainur.rony@gmail.com[2)]

Abstrak

Seiring dengan berkembangnya Teknologi Komputer yang semakin pesat, kemampuan untuk mengakses dan menyediakan informasi data secara cepat dan akurat dalam Bidang Pendidikan. SMK Islam Al Hikmah Jakarta adalah sekolah yang berlokasi di Jakarta Selatan, data siswa,guru dan raport sering terjadi keamanan yang kurang safety. Setelah dilakukan sedikit penelusuran, terdapat data-data yang sangat penting dan tidak boleh ada orang lain yang tahu selain guru kelas lain atau pun pihak sekolah dari unit tertentu, data tersebut yaitu data siswa,guru dan raport. Penyimpanan data tersebut masih dalam pengamanan yang kurang, yaitu dengan menyimpan data pada suatu file folder tanpa pengamanan. Metode kriptografi yang digunakan pada sebuah penelitian ini yaitu Advanced Encryption Standard (AES) dengan kunci sepanjang 256 bit. AES- 256 ini menggunakan 14 Round yang memiliki urutan langkah, yaitu AddRoundKey , SubBytes , ShiftRows , MixColumns. setelah itu ulangi lagi langkah-langkah tersebut sebanyak tiga belas kali dan pada langkah ke empat belas tahap MixColumns tidak dilakukan. Dengan adanya aplikasi ini pada SMK ISLAM AL HIKMAH JAKARTA, semua data siswa,guru, dan nilai dapat di enkripsi oleh user menjadi data yang tidak dapat digunakan oleh pihak-pihak tidak berwenang, dan dapat menjaga kerahasiaan data tersebut.

Kata kunci: *Kriptografi, Enkripsi, Dekripsi*, AES-256.

1. PENDAHULUAN

Pada perkembangan teknologi saat ini, manusia banyak tergantung pada bidang teknologi informasi. Dengan semakin majunya teknologi memungkinkan manusia untuk bertukar informasi, ataupun bertukar data. Keuntungan yang diberikan ddalam teknologi juga diiringi dengan dampak negative, yaitu kejahatan dalam pencurian data.

Sangat pentingnya sebuah data menyebabkan seringkali informasi data, dapat digunakan oleh pihak tertentu. Jatuhnya informasi data kepada pihak lain yang tidak diinginkan (misalnya pihak luar atau bahkan siswa) dapat merugikan bagi pihak yang memegang informasi data. Oleh karena itu keamanan dari penyimpanan data yang digunakan haruslah terjamin dalam batas yang dapat diterima.

SMK Islam Al Hikmah Jakarta adalah Sekolah yang berlokasi di Jakarta Selatan. Dalam informasi data siswa,guru dan raport sering terjadi keamanan yang kurang safety. Setelah dilakukan sedikit penelusuran, terdapat data-data penting dan tidak boleh ada orang lain yang tahu selain Guru kelas lain atau pun pihak sekolah dari unit tertentu, data tersebut yaitu data siswa,Guru dan Raport. Penyimpanan data tersebut masih dalam pengamanan yang kurang, yaitu dengan menyimpan data pada suatu file *folder* tanpa pengamanan. Dengan penyimpanan data yang kurang aman, data bisa hilang serta bisa disalahgunakan dan dapat merugikan Sekolah.

Aplikasi ini dibuat untuk keamanan *database*. Apabila terjadi sesuatu yang tidak diinginkan, seperti bencana alam, kebakaran, duplikasi data, serta pencurian data yang digunakan oleh pihak yang tidak sebagaimana mestinya. Dalam implementasi ini data yang masuk dalam sebuah *database* sudah terenkripsi dan apabila data dipanggil kembali sudah terdekripsi.

Berdasarkan uraian di atas, pada penulisan skripsi tersebut, akan membahas bagaimana implementasi keamanan *database* menggunakan metode *AES 256 bit* pada Sekolah SMK ISLAM AL HIKMAH Jakarta berbasis desktop .

2. LANDASAN TEORI

2.1. Database

Database dapat diartikan sebagai kumpulan dari item yang saling berhubungan antara satu dengan lainnya yang dapat diorganisasikan atas dasar sebuah skema atau struktur tertentu, data tersimpan di hardware komputer. Salah satu fungsi penting database adalah menjaga kerahasiaan data dan infomasi yang ada didalamnya. [1].

2.2 Pengertian Kriptografi

Kriptografi berasal dari bahasa yunani, yang terdiri dari dua kata yaitu kata *crypto* yang berarti rahasia dan *graphia diartikan sebagai tulisan*. Menurut termologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan agar pesan yang terkirim tidak terbaca oleh pihak lain. [2]

Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi. Kriptografi mempunyai tujuan menjaga kerahasiaan sebuah informasi yang termuat dalam data sehingga informasi data tidak dapat diketahui oleh pihak yang tidak seharusnya atau pihak yang salah. Perancang algoritma kriptografi disebut kriptografer. [3]

2.3 Konsep Dasar Kriptografi

Kriptografi merupakan teknik mengacak suatu data menggunakan kunci enkripsi menjadi suatu pesan yang sulit dibaca oleh pihak yang tidak memiliki kunci dekripsi. Sedangkan dekripsi merupakan teknik mengolah data asli menggunakan kunci dekripsi. Proses enkripsi menggunakan suatu algoritma dengan beberapa parameter. Biasanya algoritma yang digunakan tidak dirahasiakan, bahkan enkripsi yang mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Kerahasiaan terletak pada parameter yang digunakan.

Dalam kriptografi klasik, kriptografi pertama ditemukan pada ukiran yang tidak layak meskipun arti atau definisi dari tulisan tersebut belum dapat diperjelas. Untuk mendapatkan pengertian bagaimana suatu akgoritma kriptografi dapat berkembang, dapat ditelusuri satu per satu algoritma klasik dari teknik subtitusi dan teknik transposisi. teknik subtitusi adalah pergantian dalam setiap karakter plaintext dengan karakter lain, sedangkan transposisi yaitu teknik mutasi karakter data, dalam artian apabila digunakan teknik ini pesan yang original atau asli tidak dapat dibaca kecuali memiliki kunci untuk membuka kunci data tersebut.

2.4 Komponen Kriptografi

Komponen kriptografi pada dasarnya terdiri dari beberapa komponen penting seperti :

a. Pesan
   Data atau informasi yang dapat dibaca dan dimengerti maknanya.
b. Pengirim dan Penerima
   Pengirim bisa diartikan sebagai entitas yang dapat mengirim pesan kepada entitas lainnya. Penerima yaitu entitas menerima pesan. Entitas disini dapat berupa orang, mesin, kartu kredit dan sebagainya.
c. Enkripsi dan Dekripsi
   Enkripsi adalah proses menyandikan plaintext menjadi cipher text . Sedangkan proses mengembalikan cipher text menjadi *plaintext* semula dinamakan dekripsi.
d. Kriptoanalisa (*cryptoanalysis*)
   Ilmu dan seni untuk memecahkan cipher text menjadi plaintext tanpa mengetahui kunci yang digunakan.
e. Kunci (*Key*)
   Kunci yang dimaksud disini adalah kunci yang dipakai untuk melakukan proses enkripsi dan dekripsi. Kunci terdiri atas dua bagian, yakni kunci pribadi (*private key*) dan kunci umum (*public key*).

2.5 Tujuan Kriptografi

Aspek-aspek keamanan didalam kriptografi adalah :

a. Kerahasiaan (*Confidentiality*)
   Layanan bertujuan menjaga pesan supaya tidak dapat dibaca oleh pihak yang tidak berhak dan tidak sebagaimana mestinya.
b. Integritas (*Data Integrity*)
   Layanan dalam menjamin bahwa setiap pesan masih orisinil asli/utuh atau belum pernah dimanipulasi selama proses pengiriman sebuah data. Dalam arti lain, aspek keamanan pesan ini dapat diartikan sebagai pertanyaan
c. Otentikasi (*Authencitacion*)
   Layanan yang saling berhubungan dengan identifikasi, dalm halnya baik mengidentifikasi kebenaran pihak yang berkomunikasi, maupun mengidentifikasi kebenaran sumber pesan
d. Nirpenyangkalan (*Non - repudiation*)
   Layanan yang berfungsi mencegah atau menentang entitas yang berkomunikasi melakukan proses, yaitu pengirim pesan tidak membenarkan melakukan pengiriman atau penerima pesan tidak mengakui atau menolak telah menerima pesan.

2.6 Macam-Macam Algoritma Kriptografi

Algoritma Kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya, yaitu Algoritma Simetri, Algoritma Asimetri, dan Hash Function.

a. Algoritma Simetri
   Algoritma Simetri adalah salah satu jenis kunci pada algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Bila mengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunvi dari pesan tersebut agar bisa mendekripsikan pesan yang dikirim. Keamanan dari pesan yang digunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan.

b. Algoritma Asimetri
Algoritma asimetri sering juga disebut dengan algoritma kunci publik. Kunci yang digunakan untuk melakukan *enkripsi* dan *dekripsi* berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu:
1) Kunci umum (*public key*): kunci yang orang lain boleh mengetahui.
2) Kunci rahasia (*private key*): kunci yang tidak boleh orang tahu dan hanya diketahui oleh satu orang saja.

c. Fungsi *Hash*
Fungsi *Hash* dapat diartikan sebagai fungsi satu arah (*one-way function*)

2.7 Algoritma AES

Advanced Encryption Standard (AES) dapat diartikan sebagai Algoritma Cryptographic yang dapat digunakan untuk menjaga keamanan sebuah data [4]. *Advanced Encryption Standard* muncul sebagai suatu kebutuhan akan adanya standar baru untuk menggantikan *Data Encryption Standard* (DES) yang semakin lama semakin mudah dibobol, terutama sejak adanya perangkat keras khusus yang mampu memecahkan algoritma *kriptografi Data Encryption Standard* (DES) dalam beberapa hari.

2.8 Perbandingan 3 Blok Cipher AES-128, AES-192, dan AES-256

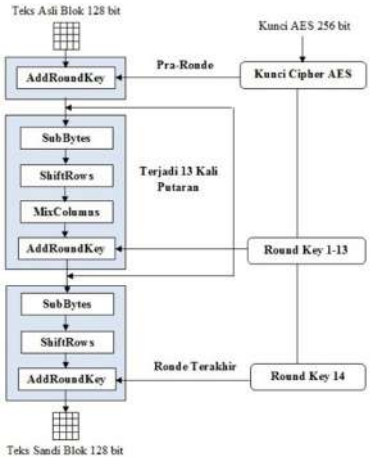
Standar *enkripsi* kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat terdiri atas 3 blok cipher, yaitu AES-128, AES-192 dan AES-256, yang diadopsi yaitu koleksi lebih besar yang awalnya telah terbit sebagai *Rijndael*. Dalam halnya setiap cipher mempunyai ukuran 128-bit, dengan ukuran kunci 128, 192, dan 256 bit. AES telah diteliti secara luas dan sekarang digunakan di seluruh dunia, seperti oleh pendahulunya, *Data Encryption Standard* (DES), [5]

Tabel 2.1 : Perbandingan Jumlah Round dan Key pada Tipe AES

Tipe	Jumlah Key (Nk)	Ukuran Blok (Nb)	Jumlah Putaran (Nr)
AES – 256	8	4	14
AES – 192	6	4	12
AES – 128	4	4	10

2.9 Proses Enkripsi AES-256 Bit

Proses *enkripsi* algoritma AES 256 terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes, ShiftRows, Mixcolumns dan* AddRoundKey . dalam sebuah awal proses enkripsi, input yang telah disamakan atau di duplikasi ke dalam state akan mengalami transformasi *SubBytes , ShiftRows , Mixcolumns* dan *AddRoundKey* secara berulang sesuai banyaknya Nr. Dalam sebuah Proses ini dapat disebut dalam algoritma AES yaitu round function . Round yang paling akhir tidak sama dan agak berbeda dengan round - round pada sebelumnya round terakhir, state tidak mengalami *MixColumns* .



Gambar 1: Proses Enkripsi AES-256 Bit

a. *AddRoundKey*
AddRoundKey adalah mengkombinasikan sebuah *Ciphertext* dan *State* dengan menggunakan operator XOR. *(Ridwan, 2016)*

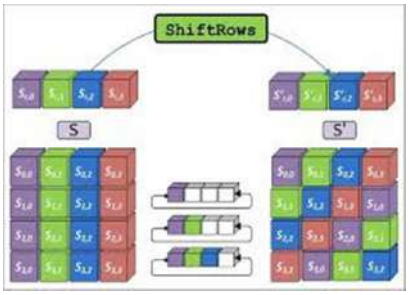
b. *SubBytes*
SubBytes adalah berganti isi matriks dengan row(baris) dan column(kolom)dalam tabel S - Box . Dibawah ini adalah contoh Tabel S - Box .

Tabel 2.2: Tabel S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

c. *ShiftRows*

Shift Rows adalah sebuah proses yang melakukan pergeseran dalam elemen blok/tabel yang harus dilakukan per barisnya, baris pertama tidak harus dilakukan pergeseran 2 byte lalu setelah itu baris yang keempat dilakukan pergeseran 3 bytes. Berikut pada gambar 2.5 proses

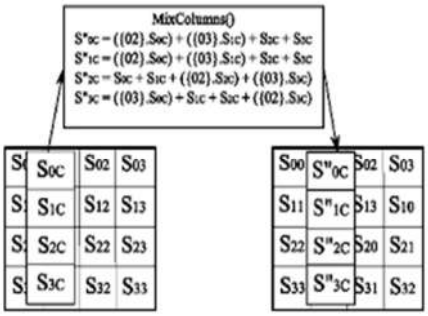


Shiftrows *(Ridwan, 2016)*

Gambar 2: Proses ShiftRows (Ridwan, 2016)

d. *MixColumns*

Mix Column adalah membuat perkalian setiap elemen dari Blok Cipher dengan matriks yang sudah ditentukan. Hitungan perkalian dilakukan seperti perkalian matriks biasa yaitu menggunakan Dot Product lalu perkalian keduanya dimasukan ke dalam sebuah Blok Cipher baru.



Gambar 3 : Proses Mix Columns (Ridwan, 2016)

e. *InvSubBytes*

InvSubBytes dapat diartikan transformasi bytes yang tidak searah atau lawan dari kebalikan transformasi SubBytes. Pada InvSubBytes, setiap elemen masing-masing state dipetakan menggunakan tabel *Inverse S-Box*.

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Tabel 2.3 : Inverse S-Box

f. *InvMixColumns*

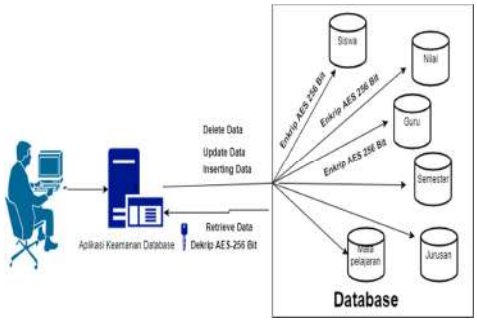
Dalam prosesnya kolom dalam state dikalikan ke matrik perkalian dalam rumusan AES. Perkalian dalam matrik dapat dituliskan :

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad \text{for } 0 \le c < Nb.$$

3. RANCANGAN SISTEM DAN APLIKASI

Pada rancangan layar system, implementasi ini akan dijelaskan dua rancangan layar yaitu sistem yang menjadi inti dari alur *Enkripsi* dan *Dekripsi.* Pada perancangan aplikasi ini membuat rancangan layar dengan menggunakan *software pencil* yang terdiri dari beberapa *Form* yaitu layar Menu Utama/Form Menu, *Form* Siswa , *Form Guru* , *Form Mata Pelajaran*, *Form* Jurusan, *Form* Penilaian Siswa, *Form Show Tables, Form PopUp Siswa, Form PopUp* Mata Pelajaran*, Form Popup* Guru, *Form Popup* Jurusan, *Form* Help dan *Form About*. Pembuatan *flowchart* menggunakan *software* Microsoft visio dilanjutkan dengan algoritma yang merupakan proses *flowchart* masing-masing *form* beserta proses metode kriptografi yang digunakan.

Untuk dapat menggunakan aplikasi ini dibagi 3 bagian hak akses form yaitu nilai,data guru dan data siswa yang terdapat pada *Form* Menu Utama. Hak akses form pada Tata Usaha dapat melakukan entry. Kemudian pada menu *form* siswa, guru & nilai terdapat sebuah keamanan untuk melakukan enkripsi ketika memilih tombol save yang akan berjalan ke database. Untuk proses dekripsi data dari database *form* siswa, *form* guru & *form* nilai dapat memilih menu *popup* siswa atau *popup* guru yang ada pada menu *form* siswa, *form* guru atau *form* nilai pada saat mencari data.

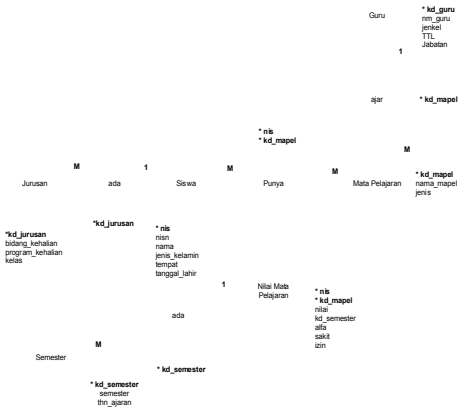


Gambar 4: Arsitektur Aplikasi

3.1 Rancangan Basis Data

a. Spesifikasi Diagram ERD(Entity Relationship Diagram)

Berikut ini adalah ERD(Entity Relationship Diagram) yang digunakan dalam pembuatan aplikasi ini:



Gambar 5: ERD(Entity Relationship Diagram)

1. Rancangan Layar

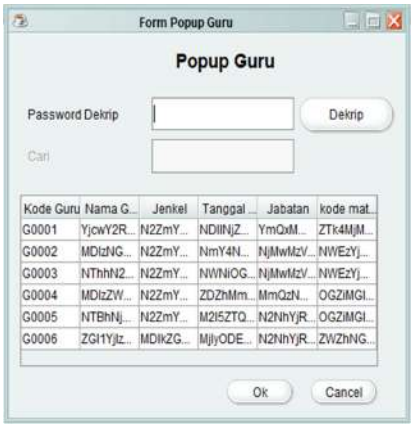
salah satu inti yang sangat penting dalam sebuah program yaitu membuat rancangan layar. Oleh sebab itu rancangan layar harus mudah dipahami dan dimengerti, supaya dalam menggunakan program user dan tidak mengalami kesulitan saat menggunakan program ini. Dalam sebuah program ini,dapat dilihat atau digambarkan rancangan layar dalam setiap form, yaitu *Rancangan layar Form Show Table*.

Gambar 6 : Rancangan Layar Form Show Table

4. HASIL DAN PEMBAHASAN

Pada bab ini akan membahas mengenai implementasi

kebutuhan yang paling utama dibutuhkan dalam sebuah syarat terpenuhinya kebutuhan spesifikasi aplikasi dan implementasi program suapaya dapat berjalan dengan baik. Pada aplikasi ini dilakukan penerapan aplikasi dan penggunaan aplikasi dan sebuah tes uji coba dalam sebuah sistem yang akan dibuat. Pada Bab ini akan membahas tentang hasil proses *Enkripsi* dan proses *Dekripsi*



Gambar 7 : Proses Enkripsi

Pada Form Guru, user juga bisa melakukan pengeditan dan penghapusan data Guru yang sudah di *encrypt* . Untuk melakukan pengeditan dan penghapusan data Guru, user terlebih dahulu melakukan proses *decrypt* . Untuk proses *decrypt*, user harus ke Form Popup Guru dengan mengklik button cari. Langkah selanjutnya user memasukan key atau password data Guru tersebut dan mengklik

button *Decrypt*.

Gambar 8 : Proses Dekripsi

5. KESIMPULAN

Atas dasar hasil analisa yang kami lakukan terhadap suatu permasalahan dan aplikasi yang dikembangkan, maka untuk mengatasinya dapat dirangkum suatu kesimpulan, sebagai berikut :

a. Aplikasi keamanan database menggunakan algoritma *Advanced Encryption Standard* (AES) 256 Bit ini dapat mengamankan data penting atau

informasi yang ada di Sekolah SMK Islam AL Hikmah Jakarta semoga lebih baik keamanan datanya, dalam hal kerahasiaannya dari pihak yang tidak bertanggung jawab.

b. Aplikasi dan hasil implementasi ini dapat mengembalikan data yang semula sudah diamankan kriptografi menggunakan metode algoritma *Advanced Encryption Standard* (AES) 256-Bit menjadi data yang asli atau orisinil tanpa mengalami perubahan sedikitpun.
c. Aplikasi ini juga mudah digunakan oleh Guru dan Tata Usaha.

DAFTAR PUSTAKA

[1] Muiz. 2015. *Pengertian Sistem Basis Data Menurut Para Ahli.*

[2] Riadi, Muchlisin. 2014. Pengertian, Sejarah dan Jenis Kriptografi. Diambil dari: http://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jeniskriptografi.html

[3] Setyaninsih Emi, *Kriptografi & Implementasinya Menggunakan Matlab,* Yoyakarta : Penerbit Andi, 2015:2.

[4] *Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015).* Implementasi *Kriptografi* keamanan Data dalam sebuah Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma

[5] S. Fricles Ariwisanto*, Perancangan dalam sebuah Aplikasi Pengaman Data Dengan menggunakan Kriptografi Advanced Encryption Standard (AES),* Jurnal Pendidikan Ilmiah, Vol. IV, No. 1, 2015.

[6] Putra, H., Santoso, E., & Muflikhah, L. (2013). Implementasi Algoritma Kriptografi Advance Ancryption Standard (AES) Pada Kompresi Data Teks. *Jurnal Ilmu Komputer Universitas Brawijaya.*

[7] *R. Cipta, Dasar Algoritma & Struktur Data Dengan Bahasa Java, Yogyakarta : Penerbit Andi, 2015*
Advanced Encryption Standard. Jurnal Informatika Mulawarman *, 10 (1), 20–31.*

[8] Ridwan, M. Khailani. (2016). Aplikasi Keamanan Menggunakan Algoritma Steganografi Discrete Cosine Transform (DCT) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Java Desktop pada PT. Hexindo Adiperkasa Tbk.