MENGAMANKAN BASIS DATA KEUANGAN KOPERASI DENGAN MENGGUNAKAN KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD

Vina Novianty[1], Rd. Erwin Gunadhi Ir.MT[2]

Jurnal Algoritma
Sekolah Tinggi Teknologi Garut
Jl. Mayor Syamsu No. 1 Jayaraga Garut 44151 Indonesia
Email : jurnal@sttgarut.ac.id

[1]1106120@sttgarut.ac.id
[2]erwin.gunadhi@sttgarut.ac.id

Abstrak *- Koperasi Padamukti Garut telah menerapkan teknologi informasi untuk pengelolaan data, khususnya data transaksi yang disimpan di dalam basis data Koperasi Padamukti. Namun data-data yang tersimpan dalam basis data tersebut masih berupa plaintext (teks asli) yang dapat dengan mudah dibaca. Hal ini dapat menimbulkan masalah karena data-data dalam basis data koperasi khususnya data mengenai transaksi keuangan adalah bersifat rahasia. Maka dari itu diperlukan sebuah metode keamanan yang dapat digunakan untuk mengamankan data-data keuangan dalam basis data Koperasi padamukti Garut. Metode pengamanan yang digunakan untuk mengamankan data-data keuangan dalam basis data Koperasi Padamukti Garut yaitu Advanced Encryption Standard. Advanced Encryption Standard, merupakan motode penyandian (mengubah teks asli menjadi teks tersandi) data dalam empat langkah dasar yaitu, langkah nonlinear (SubBytes), langkah dispersi (ShitRows), langkah difusi (MixColumns), dan penambahan kunci (AddRoundKey). Hasil akhir dari penelitian ini adalah berupa aplikasi desktop yang berfungsi untuk mengamankan data-data keuangan dalam basis data koperasi Padamukti Garut dengan menggunakan metode Advanced Encryption Standard.*

Kata Kunci *- Advanced Encryption Standard,* Aplikasi *desktop*, Mengamankan basis data keuangan.

I. PENDAHULUAN

Koperasi Padamukti Garut adalah salah satu bentuk usaha yang menyediakan jasa simpan pinjam yang sudah berbadan hukum nomor 372/BH/PAD/KWK-10/11/1997. Koperasi Padamukti Garut telah menerapkan teknologi informasi untuk pengelolaan data, khususnya data transaksi yang disimpan di dalam basis data Koperasi Padamukti. Namun data-data yang tersimpan dalam basis data tersebut masih berupa *plaintext* (teks asli) yang dapat dengan mudah dibaca. Hal ini dapat menimbulkan masalah karena data-data dalam basis data koperasi khususnya data mengenai transaksi keuangan adalah bersifat rahasia. Bagi pihak yang tak memiliki wewenang untuk mengubah data-data keuangan akan menimbulkan ancaman kebocoran data/informasi data keuangan. Sedangkan bagi orang yang memiliki wewenang untuk mengubah data-data keuangan bisa menimbulkan ancaman kerugian secara materiil baik bagi pihak koperasi maupun bagi pihak anggota koperasi. Ancaman terhadap basis data keuangan ini dapat berasal mana saja seperti dari pihak luar koperasi, anggota koperasi, maupun staf koperasi itu sendiri.

Febriansyah [1] pernah melakukan penelitian tentang cara mengamankan *password* dengan menggunakan metode kriptografi *Data Encryption System* (DES) pada sebuah basis data untuk mengenkripsi *password* tersebut. Penelitian tersebut dapat dijadikan sebagai bahan rujukan untuk mengamankan data-data keuangan yang terdapat di dalam basis data koperasi Padamukti Garut. Pada pengembangannya tidak hanya diterapkan pada data *password* saja tetapi pada seluruh atribut basis data keuangan koperasi dengan menggunakan metode kriptografi yang berbeda yaitu metode kriptografi *Advanced Encryption Standard* (AES).

II. TINJAUAN PUSTAKA

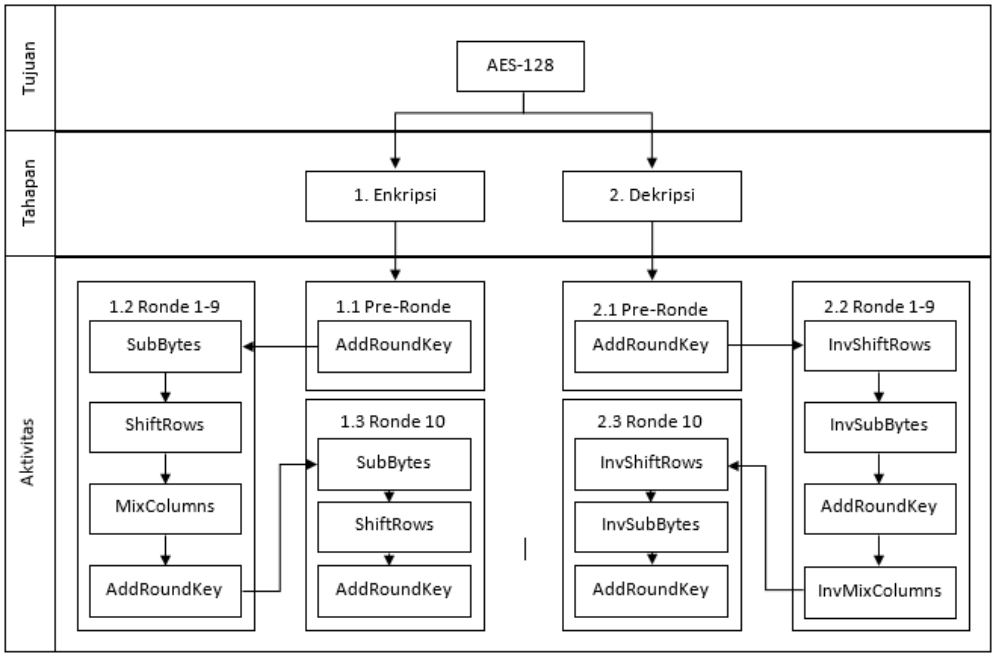
Koperasi adalah satu usaha yang beranggotakan orang-orang atau yang badan hukum, dengan melandaskan suatu kegiatan yang berdasarkan suatu prinsip koperasi sekaligus sebagai suatu gerakan perekonomian suatu rakyat yang berasaskan kekeluargaan (Pasal 1 Undang-Undang No. 25 tahun 1992). Menurut Munkner [2] koperasi merupakan sekumpulan organisasi yang saling tolong menolong dengan menjalankan urusniaga secara bersama-sama, yang berazaskan konsep saling tolong- menolong. Aktivitas tersebut hanya bertujuan untuk meningkatkan perekonomian, bukan hanya sosial seperti yang terkandung Dari beberapa definisi di atas dapat diambil disimpulkan bahwa definisi koperasi adalah suatu badan usaha urusniaga yang beranggotakan sekumpulan dalam kata gotong royong.

Metode pengamanan yang digunakan untuk mengamankan data-data keuangan dalam basis data Koperasi Padamukti Garut yaitu *Advanced Encryption Standard*. *Advanced Encryption Standard,* merupakan motode penyandian (mengubah teks asli menjadi teks tersandi) yang terbagi ke dalam dua tahapan yaitu tahapan enkripsi dan dekripsi.

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes yaitu SubByte, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi input yang telah disalin ke dalam *state* akan mengalami transformasi *byte* AddRoundKey. Kemudian *state* akan mengalami transformasi SubByte, ShiftRows, Mixcolumns, dan AddRoundKey secara berulang-ulang sebanyak Nr-1. Proses ini dalam algoritma AES disebut *round function*. *Round* yang terakhir sedikit berbeda degan *round* sebelumnya di mana pada *round* ini *state* tidak mengalami transformasi MixColumns[3]. Proses dekripsi merupakan kebalikan dari proses enkripsi yang terdiri dari 4 jenis transformasi *bytes* yaitu InvSubByte, InvShiftRows, InvMixcolumns, dan AddRoundKey. AddRoundKey dieksekusi sebagai initial round, diikuti sembilan round rentetan InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Round ke sepuluh yang mengikutinya tidak menyertakan InvMixColumns serupa dengan final round enkripsi[4].

III. KERANGKA KERJA KONSEPTUAL

Berdasarkan tujuan dan literatur yang telah dibahas sebelumnya, WBS *(Work Breakdown Structure)* yang dirancang dengan mengikuti tahapan pada metode *Advanced Encryption Standard* dapat digambarkan seperti pada gambar di bawah ini :



Gambar 1 : WBS Metode Kriptografi *Advanced Encryption Standard*

Pada tahap enkripsi, terdapat aktivitas penentuan pre-ronde, ronde satu sampai sembilan dan ronde terakhir atau ronde sepuluh. Setiap ronde memiliki aktivitas yang berbeda yakni pada pre-ronde memiliki aktivitas AddRoundKey. Untuk ronde satu sampai sembilan memiliki empat aktivitas yang diulang sebanyak sembilan kali (sembilan ronde), yaitu SubByte, ShiftRows, MixColumns, dan AddRoundKey. Sedangkan pada ronde terakhir atau ronde sepuluh aktivitas yang dimilikinya sama saja seperti ronde satu sampai sembilan, bedanya pada ronde sepuluh ini tidak terdapat aktivitas MixColumns.

Tahap yang selanjutnya yaitu tahap dekripsi, artinya mengubah teks yang telah tersandi menjadi teks biasa lagi (*plaintex*) yang dapat dibaca. Tahap dekripsi ini merupakan kebalikan dari tahap enkripsi sehingga aktivitasnya pun merupakan kebalikan (*invers*) dari aktivitas yang ada pada tahap enkripsi, kecuali tahap AddRoundKey. Pada pre-ronde, tahap dekripsi memiliki aktivitas AddRoundKey. AddRoundKey pada enkripsi dan dekripsi memiliki fungsi yang sama, sehingga *invers* dari AddRoundKey sama dengan AddRoundKey itu sendiri. Untuk ronde satu sampai sembilan pada tahap dekripsi terdiri dari InvShiftRows, InvSubByte, AddRoundKey dan InvMixColumns. Aktivitas yang memiliki kata "Inv" di awal katanya berarti merupakan kebalikan dari aktivitas yang ada pada tahapan enkripsi. Untuk ronde terakhir atau ronde sepuluh dari tahap dekripsi ini memiliki aktivitas yang sama seperti pada ronde satu sampai sembilan hanya saja bedanya pada ronde sepuluh ini tidak terdapat aktivitas InvMixColumns.

Pembuatan desain tampilan aplikasi dan implementasi AES ini menggunakan Microsoft Visual Studio Ultimate 2013 versi trial yang dapat diunduh pada halaman *website* www.visualstudio.com. Sedangkan untuk mengelola basis data koperasi yang akan diamankan menggunakan aplikasi XAMPP yang dapat diunduh secara gratis pada halaman *website* www.apachefriends.org.

IV. HASIL DAN PEMBAHASAN

A. *Implementasi Advanced Encryption Standard*

1. Dalam Bentuk Source Code Pada Aplikasi

   Potongan *source code* program untuk mengenkripsi dan mendekripsi atribut pada basis data keuangan dengan algoritma AES dapat dilihat pada gambar di bawah ini :

   a. *Source Code* Enkripsi

```
Public Function AES_Encrypt(ByVal input As String, ByVal pass As String) As String
    Dim AES As New System.Security.Cryptography.RijndaelManaged
    Dim Hash_AES As New System.Security.Cryptography.MD5CryptoServiceProvider
    Dim encrypted As String = ""
    Try
        Dim hash(31) As Byte
        Dim temp As Byte() = Hash_AES.ComputeHash(System.Text.ASCIIEncoding.ASCII.GetBytes(pass))
        Array.Copy(temp, 0, hash, 0, 16)
        Array.Copy(temp, 0, hash, 15, 16)
        AES.Key = hash
        AES.Mode = Security.Cryptography.CipherMode.ECB
        Dim DESEncrypter As System.Security.Cryptography.ICryptoTransform = AES.CreateEncryptor
        Dim Buffer As Byte() = System.Text.ASCIIEncoding.ASCII.GetBytes(input)
        encrypted = Convert.ToBase64String(DESEncrypter.TransformFinalBlock(Buffer, 0, Buffer.Length))
        Return encrypted
    Catch ex As Exception
    End Try
End Function
```

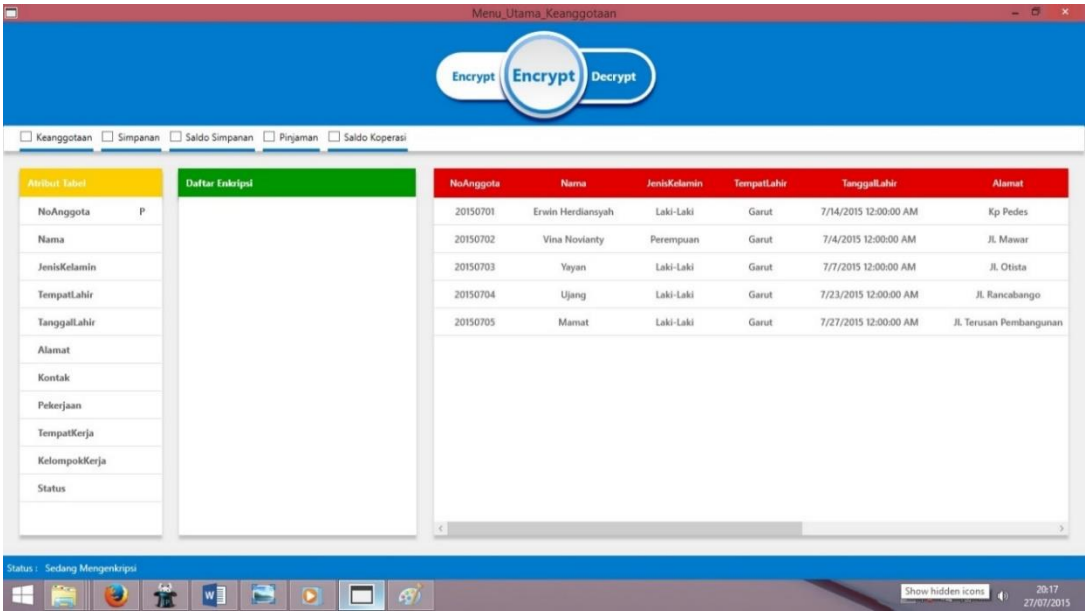
Gambar 2 : Potongan *Source Code* Enkripsi

   b. *Source Code* Dekripsi

```
Public Function AES_Decrypt(ByVal input As String, ByVal pass As String) As String
    Dim AES As New System.Security.Cryptography.RijndaelManaged
    Dim Hash_AES As New System.Security.Cryptography.MD5CryptoServiceProvider
    Dim decrypted As String = ""
    Try
        Dim hash(31) As Byte
        Dim temp As Byte() = Hash_AES.ComputeHash(System.Text.ASCIIEncoding.ASCII.GetBytes(pass))
        Array.Copy(temp, 0, hash, 0, 16)
        Array.Copy(temp, 0, hash, 15, 16)
        AES.Key = hash
        AES.Mode = Security.Cryptography.CipherMode.ECB
        Dim DESDecrypter As System.Security.Cryptography.ICryptoTransform = AES.CreateDecryptor
        Dim Buffer As Byte() = Convert.FromBase64String(input)
        decrypted = System.Text.ASCIIEncoding.ASCII.GetString(DESDecrypter.TransformFinalBlock(Buffer, 0, Buffer.Length))
        Return decrypted
    Catch ex As Exception
    End Try
End Function
```

Gambar 3 : Potongan *Source Code* Dekripsi

2. Implementasi Antarmuka



Gambar 4 : Antarmuka Aplikasi

B. Pembuktian Enkripsi dan Dekripsi

1. Enkripsi

a. Diketahui :
plaintext = Januari
key = 201507011501

b. Mengubah *plaintext* menjadi bilangan hexadecimal

String	J	A	n	u	a	r	i									
ASCII	74	97	110	117	97	114	105	32	32	32	32	32	32	32	32	32
Hex	4A	61	6E	75	61	72	69	20	20	20	20	20	20	20	20	20

c. Mengubah *plaintext* menjadi sebuah *state*

4A	61	20	20
61	72	20	20
6E	69	20	20
75	20	20	20

d. Mengubah *key* menjadi bilangan hexadecimal

Key	2	0	1	5	0	7	0	1	1	5	0	1				
ASCII	50	48	49	53	48	55	48	49	49	53	48	49	32	32	32	32
Hexa	32	30	31	35	30	37	30	31	31	35	30	31	20	20	20	20

e. Mengubah *key* menjadi sebuah *state*

32	30	31	20
30	37	35	20
31	30	30	20
35	31	31	20

f. Pre-Ronde

4A	61	20	20	⊕	32	30	31	20	=	78	51	11	00
61	72	20	20		30	37	35	20		51	45	15	00
6E	69	20	20		31	30	30	20		5F	59	10	00
75	20	20	20		35	31	31	20		40	11	11	00

g. Ronde Satu Sampai Sembilan

1) SubBytes

78	51	11	00
51	45	15	00
5F	59	10	00
40	11	11	00

SubBytes →

BC	D1	82	63
D1	6E	59	63
CF	CB	CA	63
09	82	82	63

2) ShiftRows

BC	D1	82	63
D1	6E	59	63
CF	CB	CA	63
09	82	82	63

ShiftRows →

BC	D1	82	63
6E	59	63	D1
CA	63	CF	CB
63	09	82	82

3) MixColumns

78	38	F7	E7
46	CF	8C	1E
F8	CF	F9	A2
BD	71	46	A0

$=$

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} BC & D1 & 82 & 63 \\ 6E & 59 & 63 & D1 \\ CA & 63 & CF & CB \\ 63 & 09 & 82 & 82 \end{pmatrix}$$

4) AddRoundKey

78	38	F7	E7
46	CF	8C	1E
F8	55	F9	A2
BD	71	46	A0

$\oplus$

0B	33	C4	23
7C	B3	3F	21
18	4D	B4	16
29	58	1E	BE

$=$

73	0B	33	C4
3A	7C	B3	3F
E0	18	4D	B4
94	29	58	1E

h. Ronde Sepuluh

2C	55	15	64
EE	B1	95	3B
4E	D4	0E	C8
A9	A5	A5	4E

Maka *plaintext* “Januari” dan *key* “201507011501” menghasilkan *chippertext* “2CEE4EA955B1D4B415950EA5643BC84E”

2. Dekripsi

a. Pre-Ronde

2C	55	15	64
EE	B1	95	3B
4E	D4	0E	C8
A9	B4	A5	4E

$\oplus$

37
B0
FE
13

37	3C	48	05
B0	90	86	78
FE	86	6E	5A
13	C5	B0	49

$=$

1B	69	5D	61
5E	21	13	43
B0	52	60	92
BA	71	15	07

b. Ronde Satu Sampai Sembilan

1) InvShiftRows

1B	69	5D	61
5E	21	13	43
B0	52	60	92
BA	71	15	07

InvShifRows →

1B	69	5D	61
43	5E	21	13
60	92	B0	52
71	15	07	BA

2) InvSubBytes

1B	69	5D	61
43	5E	21	13
60	92	B0	52

71	15	07	BA

InvSubByte →

44	EA	8D	D8
7B	82	64	9D
90	74	FC	48
E3	2F	38	C0

44	EA	8D	D8
7B	82	64	9D
90	74	FC	48
E3	2F	38	C0

37	3C	48	05
B0	90	86	78
FE	86	6E	5A
13	C5	B0	49

3) AddRoundKey

$\oplus$ =

73	D6	C5	DD
CB	12	E2	E5
6E	F2	92	12
F0	EA	88	89

4) InvMixColumns

1B	69	5D	61
5E	21	13	43
B0	52	60	92
BA	71	15	70

$=$ $\begin{pmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{pmatrix}$ $\begin{pmatrix} 73 & D6 & C5 & DD \\ CB & 12 & E2 & E5 \\ 6E & F2 & 92 & 12 \\ F0 & EA & 88 & 89 \end{pmatrix}$

c. Ronde Sepuluh

4A	61	20	20
61	72	20	20
6E	69	20	20
75	20	20	20

Maka *chipertext* "2CEE4EA955B1D4B415950EA5643BC84E" dan *key* "201507011501" telah berhasil menjadi teks asli lagi yaitu "Januari"

V. KESIMPULAN

Berdasarkan hasil kajian, maka dapat diambil kesimpulan dengan adanya pengamanan basis data menggunakan metode *Advanced Encryption Standard* pada aplikasi koperasi bisa meningkatkan keamanan basis data terhadap ancaman dari pihak luar maupun dalam yang tidak bertanggung jawab.

UCAPAN TERIMAKASIH

Penulis V.N mengucapkan banyak terima kasih kepada kedua orang tua penulis yang telah banyak memberi dukungan baik secara moril maupun materiil. Penulis juga mengucapkan banyak terima kasih kepada Bapak Rd. Erwin Gunadhi Ir.MT. selaku pembimbing yang telah memberikan arahan serta bimbingan selama penyelesaian laporan penelitian ini

DAFTAR PUSTAKA

[1] Febriansyah, (2012). Analisis dan Perancangan Keamanan Data Menggunakan Algoritma Kriptografi DES. Universitas Bina Darma. Palembang.
[2] Munkner, H. (1987), Hukum Koperasi, Bandung, Penerbit Alumni.

[3] NIST (2001). *Announcing the ADVANCED ENCRYPTION STANDART (AES)*, Federal Information Processing Standards Publication, USA.
[4] Sadikin, R. (2012). "Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Jawa". Yogyakarta. Andi.

