Digital Document Security System Ministry of Defense uses the Advance Encryption Standard (AES) Method

Muhammad Sutomo[1], Erly Krisnanik[2]

Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
email:erlykrisnanik@upnvj.ac.id
Jl. RS. Fatmawati, Pondok Labu, Jakarta Selatan, DKI Jakarta, 12450, Indonesia

Abstrak

Information is a valuable asset that must be managed properly by individuals, government and private organizations. Therefore the security of information becomes very important. The Indonesian Ministry of Defense requires security of valid documents, especially classified letters that are distributed through electronic communication facilities, carried out by a unit called the Ministry of Defense's Password Room. The purpose of the document coding is 1) to provide convenience, speed and security in the distribution of letters given the wide distribution of the location of the Ministry of Defense Work Unit Office; 2) Efficiency of the stages of processing letters from receipts to shipments to the satker's address can be shortened and 3) Speeding up the data search process and providing convenience for leaders to carry out monitoring and analysis of strategic information. Based on this, the researcher built the Ministry of Defense Document Coding Information System managed by the Password Room using the Advance Encryption Standard (AES) method to increase security from possible information leakage / theft. The technique used in AES uses substitution (S-boxes) directly on the document using a larger encryption key that is 256 bits. The results of this study are an integrated Ministry of Defense digital document security system.

Keywords: Room Password, Encryption, Keywords, Primary Key and AES

1 PENDAHULUAN

Kementrian Pertahanan memiliki Kamar Sandi yang merupakan salah satu unit operasional yang dikendalikan oleh Infosan Pusdatin Kemhan. Salah satu tugas Kamar Sandi adalah mengamankan surat berklarifikasi rahasia yang dikirimkan memalalui sarana komunikasi elektronik dan penyandian. Aplikasi penyandian dokumen digital yang ada saat ini menggunakan Microsoft Access berbasis *standalone* tidak terkoneksi dengan jaringan. Hal ini menyebabkan satuan kerja maupun pimpinan tidak dapat secara cepat memperoleh arsip surat dan melakukan analisa terhadap informasi-informasi strategis dengan cepat. Menurut (Dony Ariyus, 2008), Keamanan data pada komputer tidak hanya tergantung pada teknologi saja, tetapi dari aspek prosedur dan kebijakan keamanan yang diterapkan serta kedisiplinan sumber daya manusia. Jika *firewall* dan perangkat keamanan lainnya bisa dibobol oleh orang yang tidak berhak, maka peran utama kriptografi untuk mengamankan data atau dokumen dengan menggunakan teknik enkripsi sehingga data atau dokumen tidak bisa dibaca. Oleh karena Keamanan terhadap data dan informasi menjadi prioritas bagi Kemhan terutama untuk dokumen yang memiliki sifat rahasia serta prosedur dan kebijakan keamanan yang dijadikan sebagai

pedoman operasional dalam pelaksanaan tugas. Menurut Peraturan Menteri Pertahanan Republik Indonesia Nomer 18 tahun 2011 tentang Pedoman Pengelolaan Arsip Dinamis Kementerian Pertahanan Dan Tentara Nasional Indonesia, Surat adalah alat komunikasi tertulis yang dibuat dan/atau diterima oleh suatu instansi berkenaan dengan pelaksanaan tugas pokok dan fungsi instansi yang bersangkutan.

Pengelolaan surat dalam suatu lembaga dikategorikan atas dua, yaitu surat masuk dan surat keluar. Surat masuk merupakan surat yang diterima oleh organisasi/instansi yang dibuat oleh organisasi/ instansi lain yang bersifat kedinasan dan surat keluar adalah surat yang dikirimkan oleh organisasi/instansi yang dibuat oleh organisasi/ instansi lain yang bersifat kedinasan. (Kemenhan RI, 2011) Penggunaan dan pencantuman naskah dinas diatur berdasarkan: a). Klasifikasi naskah dinas berdasarkan tingkat keamanan isi suatu naskah dinas; b). Klasifikasi suatu naskah dinas/berita ditentukan oleh pejabat yang berhak menandatangani naskah dinas / berita tersebut, Kabagum / Kabag TU/ Kabag Takahdissip / Kasubbag TU/ Kasubbag Takahdis; c). Setiap pejabat dan petugas yang bersangkut paut dengan naskah dinas/ berita tersebut berkewajiban memperlakukan sesuai dengan tingkat klasifikasi yang ditetapkan; dan d). Klasifikasi naskah dinas terdiri atas: 1). Sangat rahasia, disingkat SR merupakan klasifikasi naskah dinas yang isinya memerlukan tingkat pengamanan tertinggi, klasifikasi ini erat hubungannya dengan keamanan dan keselamatan negara dan hanya boleh diketahui oleh pejabat yang berhak menerima; 2). Rahasia, disingkat R merupakan klasifikasi naskah dinas yang isinya memerlukan pengamanan yang tinggi, klasifikasi ini erat hubungannya dengan keamanan kedinasan dan hanya boleh diketahui oleh pejabat yang berwenang atau yang ditunjuk; dan 3). Biasa, disingkat B merupakan klasifikasi naskah dinas yang isinya tidak perlu pengamanan khusus, tetapi tidak berarti bahwa isi naskah dinas dapat disampaikan kepada yang tidak berhak mengetahuinya.

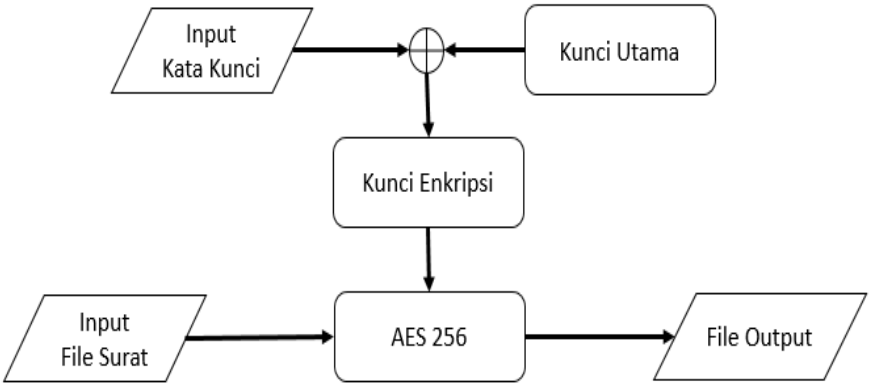
Berdasarkan hal tersebut penulis melakukan pengkajian terhadap pengamanan dokumen digital yang telah dikelompokkan berdasarkan derajat dan klasifikasi surat yang dikelola oleh disinfolahta pusdatin kemhan melalui kamar sandi.

2 METODOLOGI PENELITIAN

(Sentot Kromodimoeldjo, 2010). AES (Advanced Encryption Standard) adalah teknik enkripsi yang dijadikan standard FIPS *(Federal Information Processing Standards)* oleh NIST *(National Institute of Standards and Technology)*. Teknik enkripsi AES menggunakan substitusi (S-boxes) secara langsung terhadap naskah. AES juga menggunakan kunci enkripsi yang lebih besar yaitu 128 bit,192 bit, atau 256 bit. Metodelogi penelitian yang digunakan dalam penulisan artikel ilmiah ini adalah metode *Advance Encryption Standard (AES)* guna meningkatkan keamanan dari kemungkinan kebocoran/pencurian informasi. Teknik yang digunakan pada AES menggunakan subtitusi (S-boxes) secara langsung pada naskah dokumen Kemhan dengan menggunakan kunci enkripsi yang lebih besar yaitu 256 bit. Menurut (Daemen, 2003), Algoritma *Rijndael* menggunakan substitusi dan permutasi, dan sejumlah putaran (*cipher* berulang), setiap putaran menggunakan kunci internal yang berbeda (kunci setiap putaran disebut *round key*).-Garis besar Algoritma *Rijndael* yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut

Pada tulisan ini peneliti menggunakan AES Method dengan teknik substitusi dengan kunci lebih besar dari 128 bit. Hasil dari penelitian ini adalah sebuah Sistem keamanan dokumen digital Kemhan yang terintegrasi menggunakan metode *Advance Encryption Standard (AES).* Alur proses dari pengamanan dokumen digital dilakukan melalui beberapa tahap yaitu:

a. Pembuatan dan pengaturan penggunaan kata kunci pada Sistem Informasi Persandian dokumen Kemhan dilakukan oleh Pusdatin Kemhan selaku Pengelola Persandian Kemhan yang dilakukan secara berkala dengan menerbitkan buku Kata Kunci yang berisi Kata Kunci dan jadwal penggunaannya.
b. Pembuatan Kunci AES berasal dari hasil pencampuran (XOR) antara Kunci Utama yang telah tersimpan didalam sistem dengan Kata Kunci yang dimasukkan oleh pengguna.
c. Proses Enkripsi pengamanan naskah dinas menggunakan kunci yang dihasilkan dari proses XOR diatas yang digunakan sebagai kunci pada AES-256 mengunakan algoritma *Rijndael* untuk menyandi file input dan menghasilkan file output berupa file yang telah terenkripsi. Kunci tersebut juga digunakan untuk membuka enkripsi file yang sama, sehingga kunci untuk mengenkrip dan mendekrip file adalah sama (tidak boleh berbeda).



Gambar 1. Alur proses dari pengamanan dokumen digital menggunakan AES 256

3 HASIL DAN PEMBAHASAN

3.1 Pembuatan Kata Kunci

Pusat Pengolahan Data dan informasi pada Kementrian Pertahanan RI membutuhkan buku sandi yang dijadikan sebagai landasan dan aturan untuk penyandian terhadap dokumen digital surat masuk dan surat keluar yang bersifat rahasia. Pendistribusian Kata Kunci dilaksanakan setiap bulan melalui Kurir terpercaya dan diserahkan kepada Petugas yang ditunjuk. Tabel 1 merupakan salah satu contoh daftar kata kunci yang diperlakukan dengan periode tertentu.

Tabel 1: Kata kunci

Number	**Masa Berlaku**		***Kata Kunci***
	Mulai Tanggal	***Sampai Tanggal***	
1	01-01-2019	10-01-2019	Perjuangan191
2	11-01-2019	20-01-2019	Keadilan191
3	21-01-2019	31-01-2019	junipancasilakita

3.2 Pembuatan Kunci AES

Pengamanan dokumen digital membutuhkan kata kunci sebagai acuan dalam melakukan enkripsi dan deskripsi. Berdasarkan buku kata kunci yang telah dibuat pada tabel 1 maka bagian kamar sandi pada kementrian pertahanan akan melakukan substitusi antara kata kunci dengan kunci utama dari bilangan biner menjadi bilangan hexadecimal. Berikut adalah contoh pembuatan kunci sandi dengan menggunakan

Kata Kunci : junipancasilakita
Dengan Kunci Utama : KTHECPGDNGLSIDRPWPXWPUSKGQPUSGIDICENG

Maka Kunci yang dihasilkan adalah : **21 21 26 2C 33 29 29 27 2F 34 25 38 28 2F 3B 24.** (dalam bentuk Hexadesimal).

Tabel 2: Konvert Kata Kunci dan kunci utama ke bilangan Biner

Huruf Pertama	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	j	0110 1010	
Kunci Utama (KU)	K	0100 1011	
Kunci = KK xor KU		0010 0001	**21**
Huruf kedua	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	u	0111 0101	
Kunci Utama (KU)	T	0101 0100	
Kunci = KK xor KU		0010 0001	**21**
Huruf ketiga	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	N	0110 1110	
Kunci Utama (KU)	H	0100 1000	
Kunci = KK xor KU		0010 0110	**26**
Huruf keempat	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	i	0110 1001	
Kunci Utama (KU)	E	0100 0101	
Kunci = KK xor KU		0010 1100	**2C**
Huruf kelima	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	p	0111 0000	
Kunci Utama (KU)	C	0100 0011	
Kunci = KK xor KU		0011 0011	**33**
Huruf keenam	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	a	0110 0001	
Kunci Utama (KU)	H	0100 1000	
Kunci = KK xor KU		0010 1001	**29**
Huruf ketujuh	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	n	0110 1110	
Kunci Utama (KU)	G	0100 0111	
Kunci = KK xor KU		0010 1001	**29**
Huruf kedelapan	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	c	0110 0011	
Kunci Utama (KU)	D	0100 0100	
Kunci = KK xor KU		0010 0111	**27**

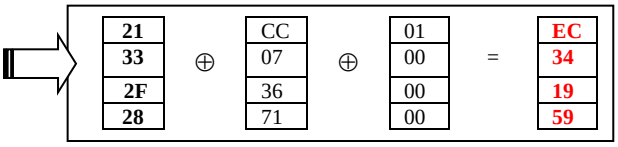
Huruf kesembilan	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	a	0110 0001	
Kunci Utama (KU)	N	0100 1110	
Kunci = KK xor KU		0010 1111	**2F**
Huruf kesepuluh	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	s	0111 0011	
Kunci Utama (KU)	G	0100 0111	
Kunci = KK xor KU		0011 0100	**34**
Huruf kesebelas	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	i	0110 1001	
Kunci Utama (KU)	L	0100 1100	
Kunci = KK xor KU		0010 0101	**25**
Huruf keduabelas	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	l	0110 1011	
Kunci Utama (KU)	S	0101 0011	
Kunci = KK xor KU		0011 1000	**38**
Huruf ketigabelas	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	a	0110 0001	
Kunci Utama (KU)	I	0100 1001	
Kunci = KK xor KU		0010 1000	**28**
Huruf keempat belas	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	k	0110 1011	
Kunci Utama (KU)	D	0100 0100	
Kunci = KK xor KU		0010 1111	**2F**
Huruf kelima belas	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	i	0110 1001	
Kunci Utama (KU)	R	0101 0010	
Kunci = KK xor KU		0011 1011	**3B**
Huruf keenambelas	**Char**	**Binari**	**Hex**
Kata Kunci (KK)	t	0111 0100	
Kunci Utama (KU)	P	0101 0000	
Kunci = KK xor KU		0010 0100	**24**

3.3 Proses Enkripsi

Proses pengamanan naskah dinas menggunakan kunci yang dihasilkan dari proses XOR diatas yang digunakan sebagai kunci pada AES-256 untuk menyandi file input dan menghasilkan file output berupa file yang telah terenkripsi. Kunci tersebut juga digunakan untuk membuka enkripsi file yang sama, sehingga kunci untuk mengenkrip dan mendekrip file adalah sama (tidak boleh berbeda). Pada pembuatan enkripsi dilakukan melalui beberapa tahap sebagai berikut:

a. Membuat enkripsi file.

Pembuatan enkripsi file dilakukan dengan cara pembuatan Roundkey pertama dengan mengambil kolom keempat Kunci, geser satu langkah ke atas substitusikan dengan nilai pada S-Box. Kemudian lakukan XOR antara kolom 1 dan kolom 4 hasil subtitusi dan kolom 1 tabel Rcon. Hasil pada point (3) dimasukkan kedalam tabel kunci kolom 5. Dan seterusnya. Proses ini dilakukan terus sampai dengan round key 14. Lakukan kegiatan pada point a) sehingga didapatkan 14 tabel kunci untuk 14 round putaran enkripsi untuk AES 256



21	⊕	CC	⊕	01	=	**EC**
33		07		00		**34**
2F		36		00		**19**
28		71		00		**59**

21	**21**	**26**	**2C**	**EC**	**CD**	**EB**	**C7**
33	**29**	**29**	**27**	**34**	**1D**	**34**	**13**
2F	**34**	**25**	**38**	**19**	**2D**	**08**	**30**
28	**2F**	**3B**	**24**	**59**	**76**	**4B**	**69**

b. Convert file

Berikut adalah salah satu contoh convert file yang akan di enkrip kedalam format Hexadesimal.

25 50 44 46 2D 31 2E 34 0D 25 E2 E3 CF D3 0D 0A 36 33 20 30 20 6F 62 6A 3C 3C 2F 48 5B 39 37 36 20 34 36 32 5D 2F 4C 69 6E 65 61 72 69 7A 65 64 20 31 2F 45 20 37 33 39 38 30 2F 4C 20 32 38 30 30 38 34 2F 4E 20 31 32 2F 4F 20 36 36 2F 54 20 32 37 38 37 37 37 3E 3E 0D 65 6E 64 6F 62 6A 0D 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20.

c. Proses Enkripsi

Proses enkripsi dilakukan dengan cara:

1) Sub Byte, ambil 16 angka hexa pertama dari file hasil convert diatas. Kemudian subtitusikan dengan tabel SBox.

25	50	44	46
2D	31	2E	34
0D	25	E2	E3
CF	D3	0D	0A

Menjadi

3F	53	1B	5A
D8	C7	31	18
D7	3F	98	11
8A	66	D7	67

2) Shif Row, lakukan pergeseran satu langkah kekiri untuk baris kedua dari tabel 4

3F	53	1B	5A	
C7	31	18	D8	← Geser 1 langkah ke kiri
98	11	D7	3F	← Geser 2 langkah ke kiri
67	8A	66	D7	← Geser 3 langkah ke kiri

3) Mix kolom,

02	03	01	01	*	3F	=	02	03	01	01	*	3F
01	02	03	01		C7							C7
01	01	02	03		98							98
03	01	01	02		67							67

4) Round Key, lakukan penjumlahan antara tabel blok 1 dengan tabel round key 1

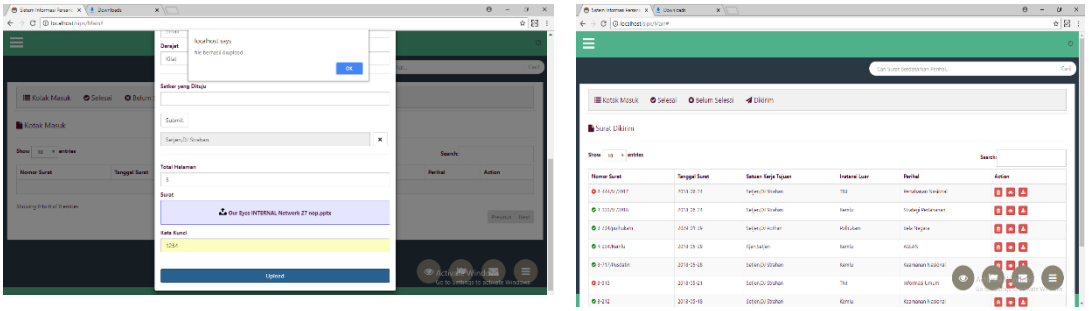
Blok 1					Round Key 1								
D3	38	30	38	⊕	EC	CD	EB	C7	=	3F	F5	2B	FF
34	2F	4E	20		34	1D	34	13		00	32	7A	33
31	32	2F	4F		19	2D	08	30		28	1F	27	7F
20	36	36	2F		59	76	4B	69		79	30	7D	46

5) Lakukan Proses Tersebut dari point a) s.d d) sebanyak 13 kali, untuk proses ke 14 tanpa dilakukan Mix Column. Maka akan dihasilkan tabel chipertext untuk blok pertama.

Lakukan proses yang sama untuk 16 angka hexa kedua dan selanjutnya hingga semua angka hexa terproses dan mendapatkan ciphertext. Proses pengamanan naskah dilakukan secara kontinue dengan melakukan berbagai perubahan pada kata kunci dan kunci utama agar system keamanan file lebih terjamin dan terjaga kerahasiaannya. Untuk memudahkan pekerjaan bagian kamar sandi, maka penulis membantu Pengelola Persandian Pusdatin Kemhan membangun aplikasi persandian berbasis web.

3.4 Desain Tampilan Program Penyandian Berbasis Web

Penulis menggunakan library PHP yaitu MCryptAES256implementation.php dan AESCryptFileLib.php untuk melakukan enkripsi file surat yang akan disimpan ke dalam SIPK. Berikut dapat dilihat desain tampilan user interface penggunaan aplikasi pengamanan dokumen digital menggunakan AES.



Gambar 2 Desain tampilan program aplikasi sistem sandi berbasis web

4 KESIMPULAN

a. Sistem Informasi Persandian Dokumen Kemhan merupakan sistem yang digunakan untuk melakukan pendistribusian sekaligus penyimpanan informasi maupun dokumen surat berklasifikasi khusus di lingkungan Kementerian Pertahanaan yang dikirimkan melalui Kamar Sandi (Kasa) Kemhan.

b. Sistem Informasi yang dibangun ini, akan mempercepat pendistribusian surat serta mempermudah petugas dalam pencarian dokumen maupun informasi surat bila suatu saat dibutuhkan.

c. Sistem berjalan saat ini memerlukan mekanisme kerja yang cukup panjang dimana disamping proses administrasi manual di Kamar Sandi, surat yang didistribusikan oleh Caraka harus melalui Bagian Tata Usaha masing-masing Satker Kemhan, sehingga memperlambat surat sampai ke Pimpinan. Dengan adanya Sistem Informasi Persandian Kemhan, surat dapat langsung dikirimkan kepada Pejabat sesuai alamat.

Referensi

Daemen, J. (2003) ‘Note on naming Rijndael’, in. Belgium.

Dony Ariyus (2008) *Pengantar Ilmu Kriptografi Teori Analisis & Implementasi*. Edited by S. S. FI. Indonesia: Andi Offset.

Kemenhan RI (2011) *Pedoman Pengelolaan Arsip Dinamis Kementerian Pertahanan Dan Tentara Nasional Indonesia*. Indonesia, Indonesia.

Sentot Kromodimoeldjo (2010) *Teori dan Aplikasi Kriptografi*. Indonesia.