Jurnal CyberTech
Vol.x. No.x, September 201x, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

Penerapan Algoritma *Advanced Encryption Standard* (AES) Untuk Pengamanan Data Taspen Di Pt.Pos Indonesia

M.Type Sultan Lubis* ,Nurcahyo Budi Nugroho S.Kom, M.Kom , Rico Imanta Ginting S.Kom, M.Kom*****
* Program Studi Mahasiswa, STMIK Triguna Dharma
** Program Studi Dosen Pembimbing, STMIK Triguna Dharma

Article Info
Article history:
Received Jun 12th, 201x
Revised Aug 20th, 201x
Accepted Aug 26th, 201x

Keyword:
Algoritma AES
simetris
Block Cipher
Ciphertext
TASPEN
Enrollment
Visual Basic

ABSTRACT
Keamanan membuat data menjadi sangat bahaya jika diketahu oleh pihak yang tidak berhak. Salah satu contoh pengelolahan ini terjadi pada PT.Pos Indonesia cabang Medan yang melayani proses transaksi pembayaran dana pensiun. Dalam proses ini terdapat Bidang pelayanan terdiri dari bagian kepersetaan, bagian layanan dan manfaat. Pada bagian pelayan dan kegunaa terdapat Enrollment (pendaftaran). AES merupakan algoritma cryptographic yang penggunaanya untuk melakukan proses mengamankan data. Algoritma AES adalah blokchipertext simetrik yang dapat melakukan enkripsi (encipher) dan dekripsi (decipher) informasi.Untuk meneliti kemampuan algoritma AES (Advanced Encryption Standard) dalam melakukan pengamanan data TASPEN yang ada di PT,Pos Indonesai Cabang Medan. Pengamanan data TASPEN yang dilakukan terkait proses pendaftaran (Enrollment) pensiunan TASPEN yang diterapkan proses enkripsi sehingga menghasilkan data yang tidak dapat dibaca lagi dalam bentuk ciphertext. Proses enkripsi yang dilakukan terhadapt data pensiunan TASPEN untuk data nama, tanggal lahir dan gaji. AES mampu memberikan keamanan yang luar biasa dan juga performansi yang baik.

Corresponding Author: *First Author
Nama : M.Type Sultan Lubis
Program Studi Sistem Informasi
STMIK Triguna Dharma
Email: typesultann@gmail.com

1. PENDAHULUAN

Masalah keamanan data merupakan salah satu aspek penting dari sebuah sistem informasi. Keamanan data menjadi sangat penting untuk pengambilan keputusan. Keputusan yang diambil harus berdasarkan data yang diperoleh [1]. Hal ini membuat data menjadi sangat bahaya jika diketahu oleh pihak yang tidak berhak. Pada umumnya manusia tidak mau jika data dirinya diketahui oleh pihak yang tidak dikenal, Apalagi data tersebut berupa hak akses yang berhubungan dengan privasi. Kejahatan data ini tidak hanya terjadi pada internet yang meminta data pribadi namun juga pada data yang berhubungan dengan perbankan. Hal inipun tidak terlepas dari sektor pemerintahan ialah sektor yang perlu dicermati dengan hati-hati dan sebaik-baiknya karena setiap kebijakan yang diambil sangat berpengaruh bagi seluruh masyarakat, dan untuk membantu kebijakan-kebijakan dalam pemerintahan maka harus ada badan-badan pengelola yang di dalamnya yaitu termasuk Badan Usaha Milik Negara. BUMN memiliki bermacam bentuk dan jenis BUMN salah satunya badan usaha Perseroan atau persero yang didalamnya ada PT TASPEN (Persero). PT TASPEN (Persero) merupakan suatu perusahaan yang dikelola oleh BUMN yang memiliki tugas utama yaitu memberi pelayanan jasa dan melayani transaksi pembayaran kepada peserta pensiun, yang dimana penerima pensiun PT TASPEN (Persero) hanya untuk Pegawai Negeri Sipil atau PNS [2]. Salah satu contoh pengelolahan ini terjadi pada PT.Pos Indonesia cabang Medan yang melayani proses transaksi pembayaran dana pensiun. Dalam proses ini terdapat Bidang pelayanan terdiri dari bagian kepersetaan, bagian layanan dan manfaat. Pada bagian pelayan dan kegunaa terdapat *Enrollment* (pendaftaran) yaitu sistem untuk melayani peserta TASPEN melakukan perekaman data sebagai bukti bahwa peserta sudah terdaftar di

perusahaan tersebut. Perekaman data dilakukan apabila peserta telah mengikuti persyaratan yang telah disediakan oleh perusahaan, perekaman data berupa pemotretan foto yang akan di arahkan oleh petugas, perekaman suara dan sidik jari [3] . Berdasakan keadaan tersebut, Pensiunan yang melakukan proses *Enrollment* (pendaftaran) di PT.Pos Indonesia cabang Medan selain melakukan *Enrollment* juga memberikan data yang akan digunakan dalam proses pendaftaran. Data tersebut berupa NOTAS, nama, tanggal lahir, gaji. Pemberian data ini, dapat digunakan orang yang tidak berhak untuk melakukan tindakan kejahatan, dikarenakan proses otentifikasi dilakukan 1 x 24 jam sesudah proses *Enrollment* (pendaftaran) terjadi.Berdasakan keadaan tersebut, kayawan dari PT.Pos maupun TASPEN atau orang yang tidak berhak dapat mengambil data para pensiun untuk melakukan tindak kejahatan.

penelitian ini mencoba untuk menerapkan keamanan menggunakan ilmu kriptografi pada proses *Enrollment* (pendaftaran) yang terjadi pada peserta TASPEN di PT. Pos Indonesia cabang Medan. Kriptografi adalah bagian dari ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi, seperti integritas data kerahasian data, keabsahan data, serta autentikasi data [4]. Kriptografi sendiri merupakan seni untuk mengamankan data yang didalamnya terdapat algoritma tertentu yang bertujuan sebagai *confusion* atau pembingungan, dengan cara mengubah teks polos (*plaintext*) menjadi teks yang tidak bisa dibaca artinya secara langsung oleh manusia atau teks rahasia (*ciphertext*). Algoritma kriptografi diklasifikasikan menjadi dua yaitu algoritma simetris dan algoritma asimetris.

Algoritma simetri disebut juga sebagai algoritma kriptografi konvensional merupakan algoritma yang penggunaan kuncinya sama untuk melakukan proses enkripsi dan proses dekripsi. Bagian- bagian algoritma kunci simetris adalah twofish, MARS, IDEA, DES (*Data Encryption Standard*), blowfish, 3DES (DES diaplikasikan 3 kali), AES (*Advanced Encryption Standard)* yang bernama asli *Rijndael* [5]. AES merupakan algoritma *cryptographic* yang penggunaanya untuk melakukan proses mengamankan data. Algoritma AES adalah blok*chipertext* simetrik yang dapat melakukan enkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi mengubah data yang tidak dapat dibaca lagi disebut *ciphertext*, sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bit untuk proses enkripsi dan dekripsi data pada blok 128 bits [6]. AES mampu memberikan keamanan yang luar biasa dan juga performansi yang baik [7], itulah mengapa pada penelitian sistem *Enrollment* (pendaftaran) yang terjadi pada peserta TASPEN di PT. Pos Indonesia cabang Medan yang dirancang menggunakan AES dalam implementasi keamanannya.

2. METODE PENELITIAN

Dalam teknik pengumpulan data dilakukan dengan dua tahapan, diantaranya yaitu:

2.1. Pengumpulan Data (*Data Collecting*)

1. Observasi
   Dalam penelitian ini dilakukan observasi pra-riset telebih dahulu untuk mencari masalah yang terjadi di PT. Pos Indonesia cabang Medan terkhusus dalam pengamanan data TAPSEN, dari masalah tersebut masalah akan dirumusakan dalam penelitian ini sehingga dapat menemukan rumusan apa saja yang perlu dipersiapkan untuk bagaimana cara menyelesaikan masalah tersebut.
2. Wawancara
   Setelah itu dilakukan wawancara kepada bagian IT pada PT. Pos Indonesia cabang Medan yang mempunyai andil dalam pengelolaan data TAPSEN. Serta mencari solusi untuk kendala yang dihadapi oleh bagian IT itu sendiri selama ini.

Gambar 1. *Screenshoot* Data TAPSEN di PT. Pos Indonesia Cabang Medan

2.2 Studi Kepustakaan (*Study of Literature*)

Di dalam studi literatur, penelitian ini banyak menggunakan jurnal-jurnal baik jurnal internasional, jurnal nasional, jurnal lokal maupun buku sebagai sumber referensi. Dari komposisi yang ada jumlah literatur yang

digunakan sebanyak 32 sumber referensi. Diharapkan dengan literatur tersebut dapat membantu peneliti dalam menyelesaikan permasalahan yang terjadi di PT. Pos Indonesia cabang Medan terkait pengamanan data TASPEN. Dikarenakan dalam penelitian ini menggunakan konsep pendekatan eksperimental maka di bawah ini adalah metode penelitian yaitu sebagai berikut:

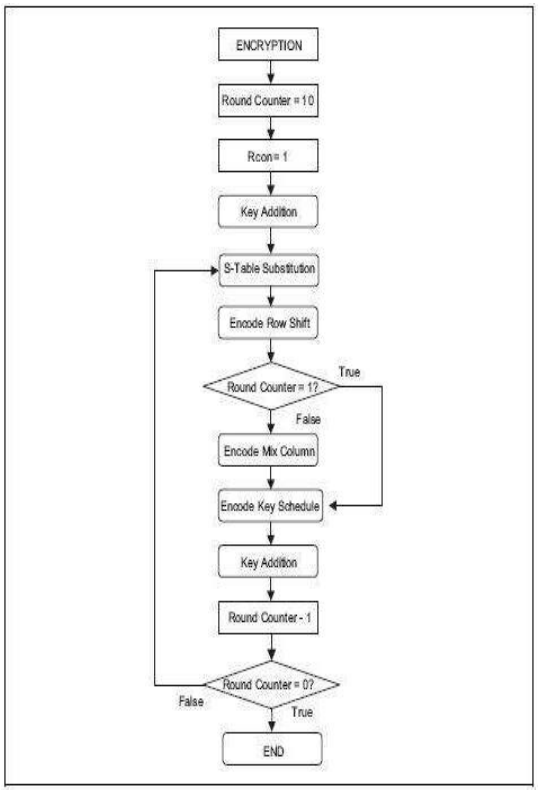
Gambar 2. Metode Penelitian

2.3 Algoritma Sistem

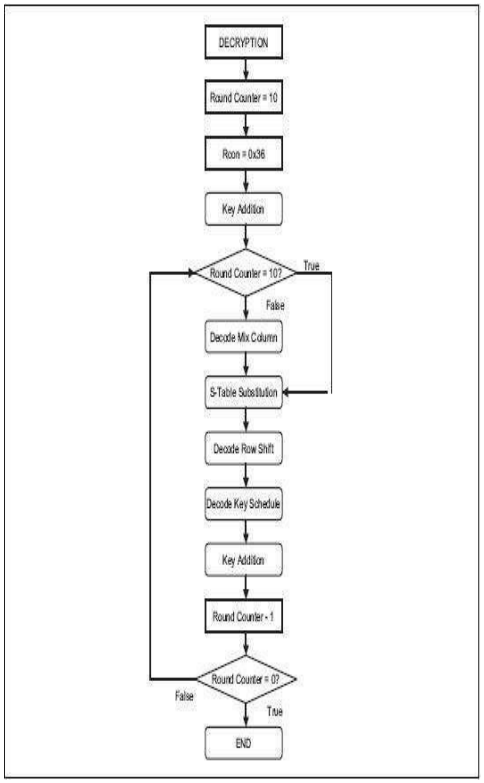
Algoritma sistem merupakan penjelasan langkah-langkah dalam penyelesaian masalah dalam perancangan sistem keamanan data TAPSEN dengan menggunakan algoritma AES. Hal ini dilakukan untuk meningkatkan keamanan data TAPSEN tersebut.

2.3.1 *Flowchart* dari Metode Penyelesaian

Berikut ini adalah *flowchart* dari proses enkripsi dan dekripsi dari algoritma AES yaitu sebagai berikut:



Gambar 3. *Flowchart* Proses Enkripsi AES



Gambar 4. *Flowchart* Proses Dekripsi AES

2.4 Dekripsi Data Dari Penelitian

Berikut ini adalah data TAPSEN yang di dapat dari PT. Pos Indonesia Cabang Medan, yang akan diamankan. Dalam pengujiannya, sebagai contoh data yang digunakan sebagai sampel dalam penelitian ini yaitu sebagai berikut:

Tabel 1. Sampel Data TAPSEN di PT. Pos Indonesia Cabang Medan

Notas	Nama Penerima	Tanggal Lahir	Valid	Tanggal	Pensiun Pokok
1982021004	CINTA DAMAI SBRG	24 November 1961	Y	10:21:05 01/12/2019	Rp.3.750.000

2.5 Penyelesaian Masalah Dengan Mengadopsi Metode

Sesuai dengan referensi yang telah dipaparkan pada bab sebelumnya, berikut ini adalah langkah-langkah penyelesaiannya yaitu:

2.5.1 Proses Enkripsi AES

Proses enkripsi algoritma AES, ada dua tahapan yaitu proses ekspansi kunci dan proses enkripsi.

1. Proses *Ekspansi* Kunci

Kunci ronde (*round key*) dibutuhkan untuk proses enkripsi dan dekripsi pada algoritma *Advanced Encryption Standart*. Maksimal panjang kunci adalah 16 digit dan jumlah kunci ronde nya adalah 10 kunci ronde yang diperoleh dari proses *ekspansi* kunci. Pada kasus ini, kunci yang akan digunakan yaitu "typesultanlubiss".

a. Urutkan kunci kedalam blok berukuran 128 bit (16 kode ASCII). Lalu ubah kunci kedalam bentuk heksadecimal

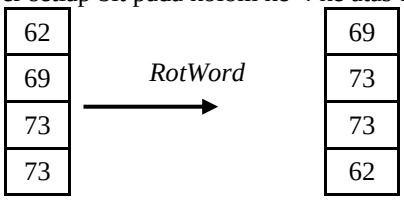
T	y	p	E	s	U	l	t	a	n	l	u	b	i	s	s
74	79	70	65	73	75	6C	74	61	6E	6C	75	62	69	73	73

b. Langkah selanjutnya yaitu susun kunci yang telah diubah kedalam bentuk heksadesimal kedalam state berukuran 4 × 4 seperti dibawah ini :

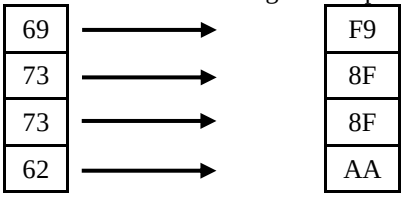
74	73	61	62
79	75	6E	69
70	6C	6C	73
65	74	75	73

State diatas merupakan cipherkey/kunci ronde ke-0

c. Setelah itu, untuk mendapatkan kolom pertama pada sub kunci, langkah pertama yaitu dilakukan fungsi *RotWord*, yaitu dengan menggeser setiap bit pada kolom ke-4 ke atas 1 kali dari kunci ronde ke-0.



d. Kemudian hasil dari *RotWord* tersebut disubtitusikan dengan nilai pada tabel S-*Box* (*SubBytes*).



e. Tahap yang terakhir yaitu lakukan proses XOR antara kolom pertama dari kunci ronde ke-0, hasil dari *SubBytes* lalu di-XOR-kan lagi dengan *RCon*.

Kolom pertama (wi) pada kunci ronde selanjutnya (ronde ke-1) = K1

F9	⊕	74	⊕	01	=	8C
8F		79		00		F6
8F		70		00		FF
AA		65		00		CF

f. Untuk mendapatkan kolom kedua, diperoleh dari proses XOR antara *Wi* dengan kolom kedua dari kunci ronde ke-0. Sedangkan untuk mendapatkan kolom ketiga dan keempat kunci ronde ke-1, dilakukan proses seperti memperoleh kolom kedua.

Kolom ke-2

8C	73	=	FF
F6	75		83
FF	6C		93
CF ⊕	74		BB

Kolom ke-3

FF	61	=	9E
83	6E		ED
93	6C		FF
BB ⊕	75		CE

Kolom ke-4

9E	62	=	FC
ED	69		84
FF	73		8C
CE ⊕	73		BD

g. Dari seluruh proses diatas, maka telah didapatlah *ekspansi* kunci untuk ronde ke-1 yaitu :

8C	FF	9E	FC
F6	83	ED	84
FF	93	FF	8C
CF	BB	CE	BD

Untuk mendapatkan kunci ronde ke-2 sampai ke-10, proses diatas diulang 10 kali. Dibawah ini adalah hasil *ekpansi* kunci dari ronde ke 1 sampai ronde 10.

2. Proses Enkripsi

Plaintext yang akan digunakan yaitu “CINTA DAMAI SBRG”. Kemudian urutkan kedalam blok lalu ubah kedalam bilangan heksadesimal.

C	I	N	T	A		D	A	M	A	I		S	B	R	G
43	49	4E	54	41	20	44	41	4D	41	49	20	53	42	52	47

Susun 16 *byte* pertama dari *plaintext* yang telah diubah kedalam *state* 4x4:

43	41	4D	53
49	20	41	42
4E	44	49	52
54	41	20	47

Lakukan XOR antara *plainteks* dengan *RoundKey* 0. Proses ini dinamakan *AddRoundKey.*

43	41	4D	53		74	73	61	62		37	32	2C	31
49	20	41	42		79	75	6E	69		30	55	2F	2B
4E	44	49	52		70	6C	6C	73	=	3E	28	25	21
54	41	20	47	⊕	65	74	75	73		31	35	55	34

Proses *AddRoundKey* diatas masih sebagai *pra-round* dan akan menjadi masukan untuk ronde ke1 yang akan diproses dengan 4 transformasi yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey.*

1. Hasil dari *pra-round* disubtitusikan dengan nilai pada tabel *S-Box* (*SubBytes*).

37	32	2C	31	→	9A	23	71	C7
30	55	2F	2B	→	04	FC	15	F1
3E	28	25	21	→	B2	34	3F	FD
31	35	55	34	→	C7	96	FC	18

2. Lakukan *ShiftRows* pada hasil dari subtitusi *SubBytes* yang dieksekusi lewat pergeseran *siklik* secara memutar dengan geseran yang acak pada tiga baris terakhir *state* (baris pertama, r = 0, tidak digeser). Baris ke dua digeser secara *siklik* ke kiri sekali, baris ke tiga dua kali, dan baris ke empat tiga kali.

9A	23	71	C7		9A	23	71	C7
04	FC	15	F1	→	FC	15	F1	04
B2	34	3F	FD	→	3F	FD	B2	34
C7	96	FC	18	→	18	C7	96	FC

3. Transformasi *MixColumns* dengan mengoperasikan *state* kolom demi kolom pada *state* kolom, dengan mengkoversikan setiap kolom sebagai polinomial.

MixColumns

	$S_{0.1}$		
$S_{0.0}$	$S_{1.1}$	$S_{0.2}$	$S_{0.3}$
$S_{1.0}$	$S_{2.1}$	$S_{1.2}$	$S_{1.3}$
$S_{2.0}$	$S_{3.1}$	$S_{2.2}$	$S_{2.3}$
$S_{3.0}$		$S_{3.2}$	$S_{3.3}$

	$S^1_{0.1}$		
$S^1_{0.0}$	$S^1_{1.1}$	$S^1_{0.2}$	$S^1_{0.3}$
$S^1_{1.0}$	$S^1_{2.1}$	$S^1_{1.2}$	$S^1_{1.3}$
$S^1_{2.0}$	$S^1_{3.1}$	$S^1_{2.2}$	$S^1_{2.3}$
$S^1_{3.0}$		$S^1_{3.2}$	$S^1_{3.3}$

02	03	01	01		$S_{0.1}$		$S^1_{0.1}$
01	02	03	01		$S_{1.1}$		$S^1_{1.1}$
01	01	02	03	**X**	$S_{2.1}$	=	$S^1_{2.1}$
03	01	01	02		$S_{3.1}$		$S^1_{3.1}$

$S^1_{0.1} = ([02].S_{0.1})\ xor\ ([03].S_{1.1})\ xor\ ([01].S_{2.1})\ xor\ ([01].S_{3.1})$

$S^1_{3.0} = ([03].S_{0.3})\ xor\ ([01].S_{1.3})\ xor\ ([01].S_{2.3})\ xor\ ([02].S_{3.3})$

$S^1_{3.0} = 00011000 = 18$

Lakukan perulangan seperti yang diatas, hingga didapatkan hasil *MixColumns* seperti sebagai berikut.

9A	23	71	C7		17	43	CE	51
FC	15	F1	04	→	20	D2	D3	6F
3F	FD	B2	34		30	85	5E	B4
18	C7	96	FC		46	18	E7	81

4. Langkah terakhir untuk mendapatkan enkripsi putaran pertama, lakukan XOR antara hasil *MixColumns* dengan *RoundKey* Ke-1, proses ini disebut *AddRoundKey*.

MixColumns					*RoundKey* Ke-1					*AddRoundKey*			
17	43	CE	51		8C	FF	9E	FC		9B	BC	50	AD
20	D2	D3	6F		F6	83	ED	84		D6	51	3E	EB
30	85	5E	B4	⊕	FF	93	FF	8C	=	CF	16	A1	38
46	18	E7	81		CF	BB	CE	BD		89	A3	29	3C

Lakukan proses diatas sampai 10 kali putaran (*round*). Berikut adalah hasil enkripsi hingga *round* ke 10. Hasil dari proses *AddRoundKey* atau *round* ke-10 diubah ke bentuk karakter didalam tabel ASCII Dan hasil dari enkripsi dengan algoritma AES menghasilkan cipherteks sebagai berikut.

Tabel 2. Hasil Enkripsi Dengan Algoritma AES

Notas	**Nama Penerima**	**Tanggal Lahir**	**Valid**	**Tanggal**	**Pensiun Pokok**
1982021 004	A À ¾ ß©Á3¡ ÙN ŠË«	ÛdMF«‡©Z, ,1Ž	Y	10:21:05 01/12/2019	O mÏòÏÃôWÇ×,ñM

2.5.2 Proses Dekripsi AES

Kunci yang digunakan untuk proses dekripsi sama dengan yang digunakan pada proses enkripsi. Berikut adalah proses dekripsi dari hasil *ciphertext* yang telah diperoleh dari proses enkripsi sebelumnya.

A	À	¾		ß	©	Á	3	¡		ù	N		Š	ë	«
61	E0	BE	10	DF	A9	C1	33	A1	1B	F9	4E	A0	8A	EB	AB

Kemudian susun 16 *byte* pertama dari *ciphertext* yang telah diubah ke bentuk heksadesimal kedalam *state* 4x4:

61	DF	A1	A0
E0	A9	1B	8A
BE	C1	F9	EB
10	33	4E	AB

Lakukan XOR antara *cipherteks* dengan *RoundKey* Ke-10. Proses ini dinamakan *AddInvRoundKey*.

61	DF	A1	A0	6A	29	74	79		)B	F6	D5	D9
E0	A9	1B	8A	F0	87	6C	A3	=	10	2E	77	29
BE	C1	F9	EB	01	F8	15	39		BF	39	EC	D2
10	33	4E	AB	63	61	5C	D7		73	52	12	7C

Proses *AddInvRoundKey* diatas masih dalam *initial-round*, dan akan menjadi masukan untuk ronde ke-1 yang akan diproses dengan 4 transformasi yaitu *InvShiftRows, InvSubBytes*, *AddInvRoundKey*, dan *InvMixColumns*.

1. Lakukan *InvShiftRows* pada hasil *initial-round* dari *AddInvRoundKey* yang dieksekusi lewat pergeseran *siklik* secara memutar. Baris ke dua digeser secara *siklik* ke kiri tiga kali, baris ke tiga dua kali, baris ke empat sekali.

0B	F6	D5	D9	0B	F6	D5	D9
10	2E	77	29	29	10	2E	77
BF	39	EC	D2	EC	D2	BF	39
73	52	12	7C	52	12	7C	73

2. Hasil dari *InvShiftRows* disubtitusikan dengan nilai pada tabel $S - Box^{-1}$ (*InvSubBytes*).

0B	F6	D5	D9	9E	D6	B5	E5
29	10	2E	77	4C	7C	C3	02
EC	D2	BF	39	83	7F	F4	5B
52	12	7C	73	48	39	01	8F

3. XOR hasil dari *InvSubBytes* dengan *RoundKey* Ke-9. Proses ini disebut *AddInvRoundKey*

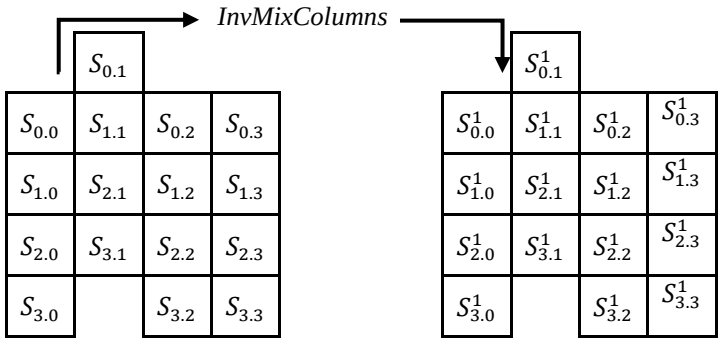
9E	D6	B5	E5	D6	43	5D	D		48	95	E8	E8
4C	7C	C3	02	81	77	EB	CF	=	CD	0B	28	CD

83	7F	F4	5B
48	39	01	8F

3C	F9	ED	2C
B4	02	3D	8B

BF	86	19	77
FC	3B	3C	04

4. Hasil dari *AddInvRoundKey* ditransformasikan oleh *InvMixColumns* dengan mengoperasikan *state* kolom demi kolom. Operasi ini dilakukan pada *state* kolom, dengan mengkoversikan setiap kolom sebagai polinomial.



$S^1_{0.1} = ([0E].S_{0.1})\ xor\ ([0B].S_{1.1})\ xor\ ([0D].S_{2.1})\ xor\ ([09].S_{3.1})$
$S^1_{0.0} = 01111111\ xor\ 10111110\ xor\ 00111011\ xor\ 10100110$
$S^1_{0.0} = 10101000 = A8$
$S^1_{1.0} = ([09].S_{0.1})\ xor\ ([0E].S_{1.1})\ xor\ ([0B].S_{2.1})\ xor\ ([0D].S_{3.1})$
$S^1_{0.0} = 10101010 = AA$
$S^1_{2.0} = ([0D].S_{0.2})\ xor\ ([09].S_{1.2})\ xor\ ([0E].S_{2.2})\ xor\ ([0B].S_{3.2})$
$S^1_{0.0} = 01101011 = 6B$
$S^1_{3.0} = ([0B].S_{0.3})\ xor\ ([0D].S_{1.3})\ xor\ ([09].S_{2.3})\ xor\ ([0E].S_{3.3})$
$S^1_{0.0} = 00110101 = 35$
Lakukan perulangan seperti yang diatas, hingga didapatkan hasil *InvMixColumns* seperti sebagai berikut.

48	95	E8	E8
CD	0B	28	CD
BF	86	19	77
FC	3B	3C	04

→

04	DE	16	38
41	EA	96	7B
64	8B	36	0B
E7	9C	53	1E

Proses diatas diulang sampai 10 kali putaran (*round*). Berikut adalah hasil dari dekripsi hingga *round* ke 10. Dan hasil dari dekripsi dengan algoritma AES menghasilkan plainteks sebagai berikut.

Tabel 3. Hasil Dekripsi Dengan Algoritma AES

Notas	**Nama Penerima**	**Tanggal Lahir**	**Valid**	**Tanggal**	**Pensiun Pokok**
1982021004	CINTA DAMAI SBRG	24 November 1961	Y	10:21:05 01/12/2019	Rp.3.750.000

3. ANALISA DAN HASIL

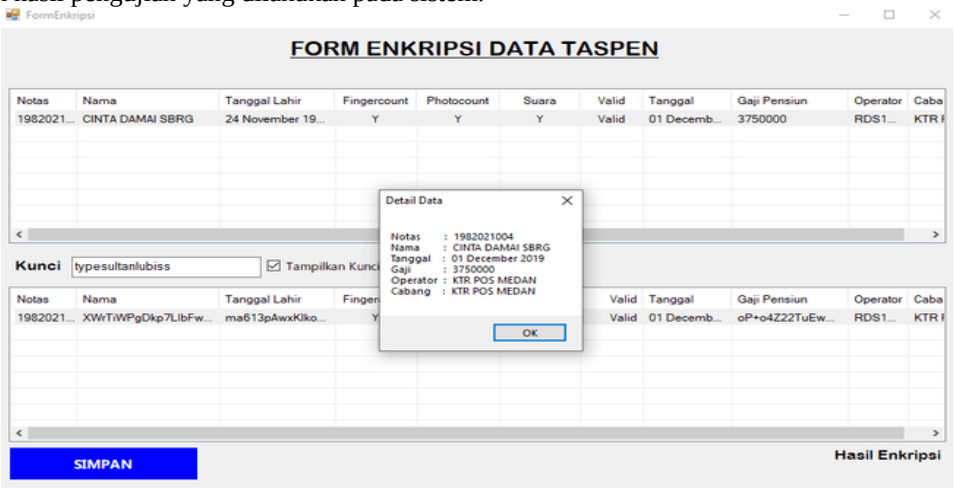
3.1 Pengujian Sistem

Uji coba sistem bertujuan untuk membuktikan bahwa *input*, *proses*, *output* yang dihasilkan oleh sistem aplikasi *Visual Studio 2010* telah benar dan sesuai dengan yang diinginkan.

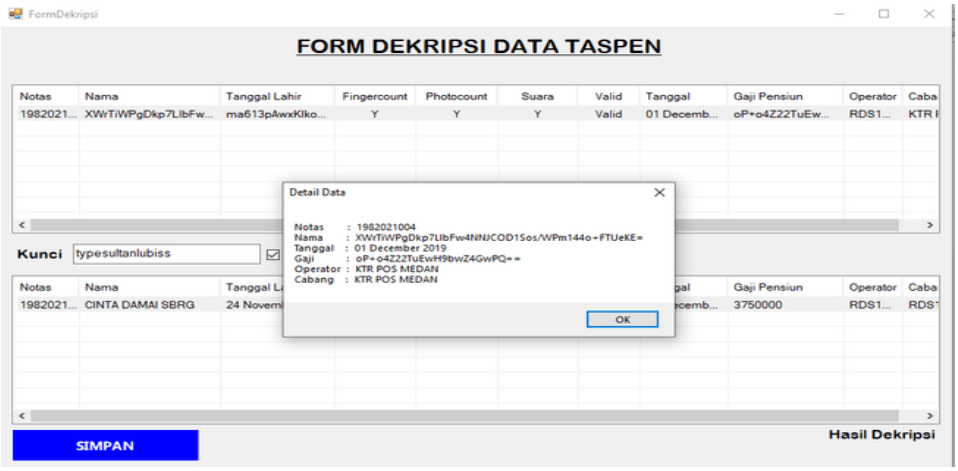
Pengujian sistem dengan cara memasukkan data ke dalam sistem dan memperhatikan *output* yang dihasilkan. Jika *input*, proses dan *output* telah sesuai, maka sistem telah benar. Berikut merupakan tahapan untuk pengujian sistem yaitu:

1. Melakukan *input* data taspen yang kemudian sistem akan menampilkan data taspen yang tersimpan di *database*.
2. Menggunakan bahasa pemrograman *Microsoft Visual Studio 2010* dalam pengolahan data yang disimpan dalam *database Microsoft Office Access 2013* .

Penggunaan sistem pengamanan data taspen pada PT.Pos Indonesia Cabang Medan, agar dapat berjalan dengan baik *file* aplikasi *Visual Studio 2010* harus ditempatkan pada satu *folder* dan dilengkapi dengan *input* data dari analisa sistem. Lokasi *folder* yang telah ditentukan adalah tempat untuk menyimpan *file-file* yang telah dikumpulkan, untuk menghindari kesalahan sebaiknya data tidak diletakkan kedalam *folder* yang berbeda. Selanjutnya untuk menerapkan metode dalam mengamankan data gaji taspen, maka data tersebut akan *diinput* ke aplikasi lalu simpan data tersebut ke dalam *database Access*. Jalankan aplikasi *Visual Studio 2010* yang telah terinstal dikomputer. Berikut ini merupakan hasil pengujian yang dilakukan pada sistem.



Gambar 5. Pengujian Untuk Enkripsi Data Taspen



Gambar 6. Pengujian Kunci Benar Untuk Dekripsi Data Taspen

3.2. Kelemahan dan Kelebihan Sistem

Berikut ini diuraikan kelemahan dan kelebihan dari sistem:

1. Kelemahan Sistem

   Dalam sistem tentunya masih ada kekurangan dan kelemahan. Adapun kelemahan yang ada di dalam sistem adalah:

   a. Kunci yang digunakan hanya bisa dengan 16 karakter, sehingga cukup sulit untuk mengingat kunci tersebut.
   b. Sistem yang dibangun tidak dapat diakses secara online, sehingga sistem hanya dapat digunakan secara lokal saja.
   c. Hasil ini hanya digunakan pada kasus di PT.Pos Indonesia Cabang Medan, tidak di perusahaan lain.

2. Kelebihan Sistem

   Hasil yang didapat dari pengujian sistem ini mempunyai kelebihan-kelebihan antara lain :

   a. Proses Pengamanan Data

   Bagi pengguna sistem khususnya pada PT.Pos Indonesia Cabang Medan yang ingin menggunakan sistem ini, cukup meng*input* data taspen yang akan dijadikan sebagai objek pengamanan data, kemudian melakukan proses enkripsi, maka hasil yang di dapat yaitu sebuah *cipherteks*, data taspen tersebut diamankan dengan

menggunakan kombinasi kriptografi algoritma AES sehingga sulit untuk mengetahui dan membaca data taspen tersebut.

b. Menjalankan Program
Program yang dibangun berbasis *desktop programming*, walaupun tidak terhubung jaringan ataupun internet sistem tetap dapat untuk dijalankan.

c. Dapat membantu pihak karyawan pada PT.Pos Indonesia Cabang Medan dalam mengamankan data taspen.

4. KESIMPULAN

Berdasarkan pembahasan dan evaluasi dari bab sebelumnya, maka dapat ditarik kesimpulan sebagai berikut :

1. Dalam menganalisa masalah yang terjadi terkait dengan pengamanan data TASPEN di PT. Pos Indonesia cabang Medan menggunakan algoritma AES (*Advanced Encryption Standard)* maka dilakukan proses enkripsi untuk data taspen dari nama, tanggal lahir dan gaji untuk menyelesaikan permasalahan tersebut.
2. Perancang sistem kriptografi yang mengadopsi algoritma AES (*Advanced Encryption Standard)* dengan metode sistem *Block Cipher* di dalam menyelesaikan masalah terkait pengamanan data TASPEN di PT. Pos Indonesia cabang Medan menggunakan pemrograman yang berbasis desktop yaitu *Visual Basic*.
3. Pengimplementasikan sistem kriptografi yang terintegrasi dengan sistem yang berbasis *Visual Basic* 2010 dan Microsoft Acsess 2013 dapat dilakukan dalam menyelesaikan masalah terkait pengamanan data TASPEN di PT. Pos Indonesia cabang Medan .
4. Pengujian sistem ini dilakukan sebelum nantinya dapat dicoba untuk membantu instansi -instansi terkait di dalam pengamanan data TASPEN di PT. Pos Indonesia cabang Medan.

REFERENSI

[1] "Peningkatan Keamanan Data dengan Metode Cropping Selection Pseudorandom."

[2] L. Bruno, "済無No Title No Title," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019.

[3] A. A. Safitri, T. S. Jaya, and D. K. Widyawati, "APLIKASI PEMBERITAHUAN PEREKAMAN ULANG DATA PESERTA PENSIUN BERBASIS SMS GATEWAY MENGGUNAKAN API PADA PT . TASPEN," pp. 1–13, 1960.

[4] M. M. Amin, J. T. Komputer, P. Negeri, and S. Palembang, "IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS," *J. Pseudocode*, vol. 2, 2016.

[5] R. Toyib and A. Wijaya, "ANALISIS PERBANDINGAN ALGORITMA SIMETRIS RIVEST CODE 5 DENGAN ALGORITMA SIMETRIS RIVEST CODE 6) (Studi Kasus : SMK Negeri Seluma)," *J. Inform. Upgris*, vol. 4, no. 2, pp. 203–209, 2019.

[6] D. A. Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.

[7] A. F. Ramdhansya, E. Ariyanto, and H. H. Nuha, "Implementasi Advanced Encryption Standard (Aes) Pada Sistem Kunci Elektronik Kendaraan Berbasis Sistem Operasi Android Dan Mikrokontroler Arduino," *Semin. Nas. Inform.*, vol. 2014, no. semnasIF, pp. 92–98, 2014.

BIBLIOGRAFI PENULIS

	Nama : M.Type Sultan Lubis Tempat Lahir : Medan TanggalLahir : 27 May 1993 Jenis Kelamin : Laki-Laki Agama : Islam Warga Negara : Indonesia Status :Lajang Alamat : Jl. Delitua Gg Saudara no 10
Second author's photo(3x4cm)	Nama : Nurcahyo Budi Nugroho S.Kom, M.Kom
Thirth author's photo(3x4cm)	Nama : Rico Imanta Ginting S.Kom

NB : Untuk Second dan Thirth Author's dapat di kosongkan dan cukup isikan nama author