JISKa, Vol. 5, No. 3, NOVEMBER, 2020, Pp. 153 – 163
ISSN: 2527 – 5836 (print) | 2528 – 0074 (online)

Implementasi *Algoritma Advanced Encryption Standard* (AES) pada Layanan SMS Desa

Intan Fitriani [(1)*], Aryo Baskoro Utomo [(2)]
[1,2] Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang, Semarang
e-mail : intan4250@gmail.com, aryobaskoro@mail.unnes.ac.id.
* Penulis korespondensi.
Artikel ini diajukan 17 April 2020, diterima 12 Mei 2020, dan dipublikasikan 9 November 2020.

Abstract

Along with the development of technology, Short Message Service (SMS) has begun to be used to communicate between someone and the system in an agency. But in some cases, the security of messages sent through the SMS application has not been well protected. To improve data security and confidentiality, cryptographic algorithms with Advanced Encryption Standard (AES) can be done. The method used is the Waterfall method. AES encryption testing is done by comparing the manual calculations and the results of the encryption on the system. Blackbox test, CrackStation test, and Avalanche Effect (AE) test were also carried out. Brute force test results using CrackStation software that ciphertext cannot be solved. And in the avalanche effect (AE) test, the AE value of each 128-bit AES key is 44.53%, 192-bit is 48.44%, and 256-bit is 56.25%. Therefore, 192-bit and 256-bit AES keys are recommended for use because AE values are in the range of 45% - 60%.

Keywords: Village SMS Service, AES Algorithm, Brute Force, Avalanche Effect

Abstrak

Seiring dengan perkembangan teknologi, *Short Message Service* (SMS) sudah mulai digunakan untuk berkomunikasi antara seseorang dengan sistem dalam sebuah instansi. Namun dalam beberapa kasus, keamanan pesan yang dikirimkan melalui aplikasi SMS belum terproteksi dengan baik. Untuk meningkatkan keamanan dan kerahasiaan data dapat dilakukan dengan kriptografi algoritma *Advanced Encryption Standard* (AES). Metode yang digunakan adalah metode *Waterfall*. Pengujian enkripsi AES dilakukan dengan melakukan perbandingan antara perhitungan manual dan hasil enkripsi pada sistem. Selain itu, dilakukan juga uji *blackbox*, uji *CrackStation*, dan uji *Avalanche Effect* (AE). Hasil uji *brute force* menggunakan *software CrackStation* bahwa *chipertext* tidak dapat dipecahkan. Dan pada uji *avalanche effect* (AE) diperoleh nilai AE masing-masing kunci AES 128-*bit* sebesar 44,53%, 192-*bit* sebesar 48,44%, dan 256-*bit* sebesar 56,25%. Dengan demikian, kunci AES 192-*bit* dan 256-*bit* lebih direkomendasikan untuk digunakan karena nilai AE berada pada rentang 45% - 60%.

Kata Kunci: Layanan SMS Desa, Algoritma AES, *Brute Force*, *Avalanche Effect*

1. PENDAHULUAN

Perkembangan teknologi informasi dewasa ini berkembang sangat pesat. salah satunya dibidang telepon seluler yang di dalamnya terdapat fitur SMS. Seiring perkembangannya, SMS tidak hanya digunakan untuk bertukar informasi antara dua orang saling membutuhkan. Kini SMS sudah mulai digunakan untuk berhubungan antara seseorang dengan system (Afrina & Ibrahim, 2015). SMS sudah banyak diterapkan diberbagai bidang, salah satunya pada bidang pemerintahan. Untuk menyelenggarakan suatu pemerintahan yang efektif dan demokratis menuntut adanya kinerja pemerintah daerah yang lebih baik. Dalam hal ini pemerintah desa menciptakan upaya keterlibatan masyarakat untuk menuju masyarakat yang lebih maju. Diperlukan sistem tata kelola pemerintah yang baik, khususnya pemerintah desa, serta partisipasi dari masyarakat (Purba & Djamin, 2015). Salah satunya dengan meningkatkan komunikasi antara pemerintah desa dengan warga maupun sebaliknya berupa layanan informasi dan pengaduan. Pengaduan dari masyarakat penting bagi pemerintah guna mengetahui tingkat keberhasilan pemerintah khususnya desa dalam melaksanakan suatu kegiatan (Prasetya, 2013). Untuk mewujudkan suatu layanan informasi maupun pengaduan salah satunya dengan teknologi SMS. Dalam beberapa kasus, pesan aduan atau informasi yang dikirimkan bersifat rahasia. Namun keamanan pesan

yang dikirimkan melalui SMS belum terproteksi dengan baik (Atmojo et al., 2016). Sehingga memudahkan bagi penyadap untuk melakukan pencurian data mengingat banyaknya informasi penting milik pengguna. Sebagai upaya untuk meningkatkan keamanan dan menjaga kerahasiaan data dapat dilakukan dengan kriptografi. Terdapat beberapa algoritma kriptografi yang dapat digunakan untuk keamanan data, salah satunya algoritma AES. Hingga saat ini algoritma AES cukup aman untuk melindungi data atau informasi yang bersifat rahasia (Muharram et al., 2018).

Penelitian terkait keamanan data SMS pernah dilakukan oleh peneliti terdahulu. Seperti penelitian yang dilakukan oleh Layansari & Marisa (2018), pada penelitian tersebut sistem pelayanan informasi berbasis SMS Gateway dapat meningkatkan mutu pelayanan terhadap masyarakat. Pada penelitian lainnya yang dilakukan oleh Alvianto & Darmaji (2015), Ibrahim (2017), Azhar & Kurniawan (2017) menambahkan pengamanan pada data SMS dan *file* menggunakan kriptografi algoritma AES. Algoritma AES termasuk algoritma *simetris* yang menggunakan kunci yang sama dalam proses ekripsi maupun dekripsi. Algoritma AES merupakan algoritma yang sangat sensitif, dimana setiap karakter yang di*input* akan menghasilkan *output* yang berbeda sehingga sangat baik untuk keamanan data SMS.

2. METODE PENELITIAN

Penelitian ini menggunakan metode *Waterfall.* Terdapat lima tahapan pada metode *Waterfall*, antara lain *communication*, *planning*, *modeling*, *construction*, dan *deployment*.

2.1. Communication

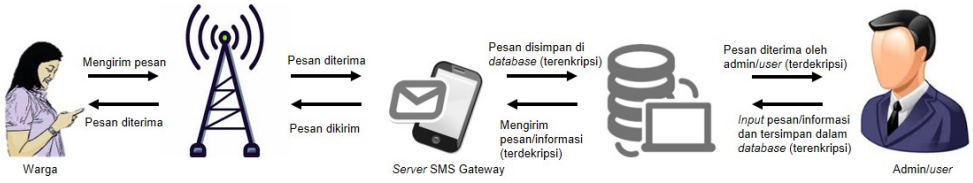
Tahap *communication* dilakukan dengan mewawancarai kepala desa dan perangkat desa. Penelitian dilakukan di Desa Talang, Kec. Talang, Kab. Tegal. Dari tahap komunikasi ini diperoleh permasalahan adalah belum adanya sistem informasi yang dapat menjembatani komunikasi antara pemerintah dengan desa maupun sebaliknya. Selain wawancara, dilakukan pula studi kepustakaan untuk mengumpulkan data tambahan atau referensi terkait Layanan SMS Desa dan keamanan data SMS melalui jurnal, artikel, dan internet.

2.2. Planning

Pada tahap ini dilakukan analisis terkait kebutuhan *user*. Kebutuhan *user* yang terlibat dalam sistem ini antara lain administrator, perangkat desa, ketua komunitas, dan warga. Adapun hasil yang ingin dicapai dalam penelitian ini yaitu berupa sistem layanan SMS Desa dan mengimplementasikan algoritma AES untuk meningkatkan keamanan pada data SMS.

2.3. Modeling

Tahap *modeling* dimulai dengan merancang skema sistem Layanan SMS Desa kemudian merancang *database* menggunakan MySQL untuk penyimpanan data perangkat desa, komunitas, warga, pesan masuk, dan pesan keluar. Dilanjutkan dengan merancang antarmuka sistem Layanan SMS Desa. Skema sistem Layanan SMS Desa dapat dilihat pada Gambar 1.



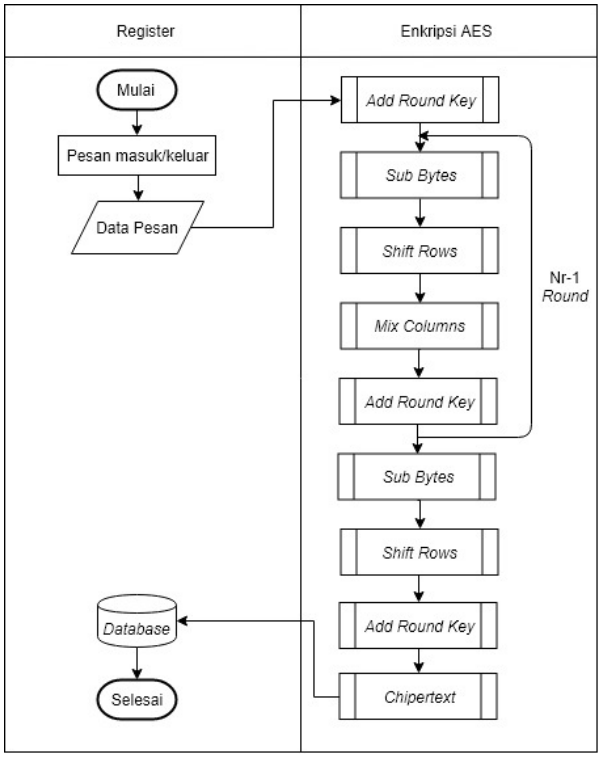
Gambar 1. Skema Sistem Layanan SMS Desa.

Skema sistem Layanan SMS Desa pada Gambar 1 merupakan cara kerja sistem yang dirancang untuk memberikan gambaran terkait sistem yang akan dibuat. Skema sistem Layanan SMS Desa dimulai dari warga mengirimkan pesan kemudian pesan dikirimkan oleh *provider* dan dikirimkan menuju *server* SMS *gateway*, kemudian pesan akan tersimpan di *database* dalam bentuk

terenkripsi dan pesan dapat dilihat oleh admin/*user* dalam bentuk terdekripsi. Setelah admin/*user* melihat pesan kemudian admin memberikan balasan/mengirimkan pesan kepada warga. Data terkait *user*, perangkat desa, komunitas, dan warga sebelumnya sudah di*input*kan oleh admin/perangkat desa yang berwenang.

2.4. Construction

Pada tahap ini dilakukan penerjemahan kode dari rancangan yang telah dibuat sebelumnya ke dalam bahasa pemrograman. Bahasa pemrograman yang digunakan untuk membangun sistem layanan SMS Desa menggunakan bahasa pemrograman PHP dengan *framework Laravel* dan *database* MySQL untuk penyimpanan datanya. Algoritma AES digunakan untuk keamanan data yang akan diimplementasikan pada data pesan di dalam *database*. Gambar 2 merupakan alur enkripsi data pesan menggunakan algoritma AES. Data pesan masuk berupa pesan asli kemudian dilakukan proses enkripsi oleh sistem, hasil enkripsi berupa *chiper text* dan tersimpan di dalam *database*.



Gambar 2. *Flowchart* Enkripsi Pesan.

Setelah pengkodean selesai, kemudian dilakukan pengujian pada sistem. *Pengujian blackbox* dilakukan dengan cara memeriksa apakah program yang telah dibuat sudah dapat menerima *input* data, memproses, dan memberikan *output* dengan baik sesuai dengan yang diharapkan. Pengujian selanjutnya berfokus pada hasil enkripsi algoritma AES pada SMS. Pengujian dilakukan pada hasil enkripsi algoritma AES dengan cara melakukan perbandingan antara perhitungan enkripsi secara manual dan enkripsi pada sistem. Selain pengujian manual, pengujian juga dilakukan menggunakan *software* penyerang *CrackStation* dan *avalanche effect*. Uji kelayakan sistem yang dilakukan oleh ahli yang berkompeten dibidangnya.

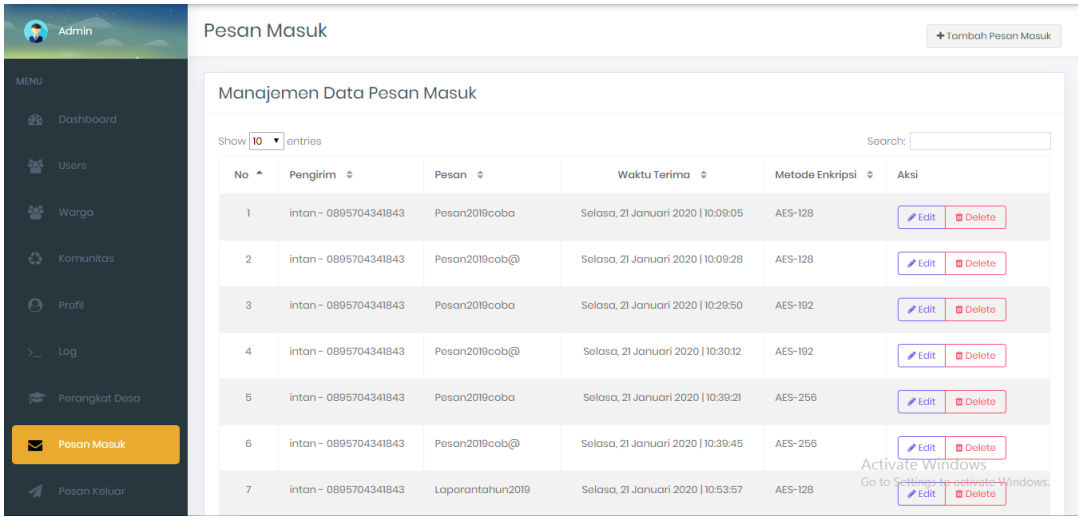
2.5. Deployment

Pada tahap ini dilakukan perbaikan sistem sesuai kebutuhan sebelum diimplementasikan oleh pihak pemerintah desa. Apabila sistem Layanan SMS Desa dengan keamanan data SMS sudah sesuai dengan keinginan pihak *customer,* maka sistem dapat langsung diimplementasikan.

3. HASIL DAN PEMBAHASAN

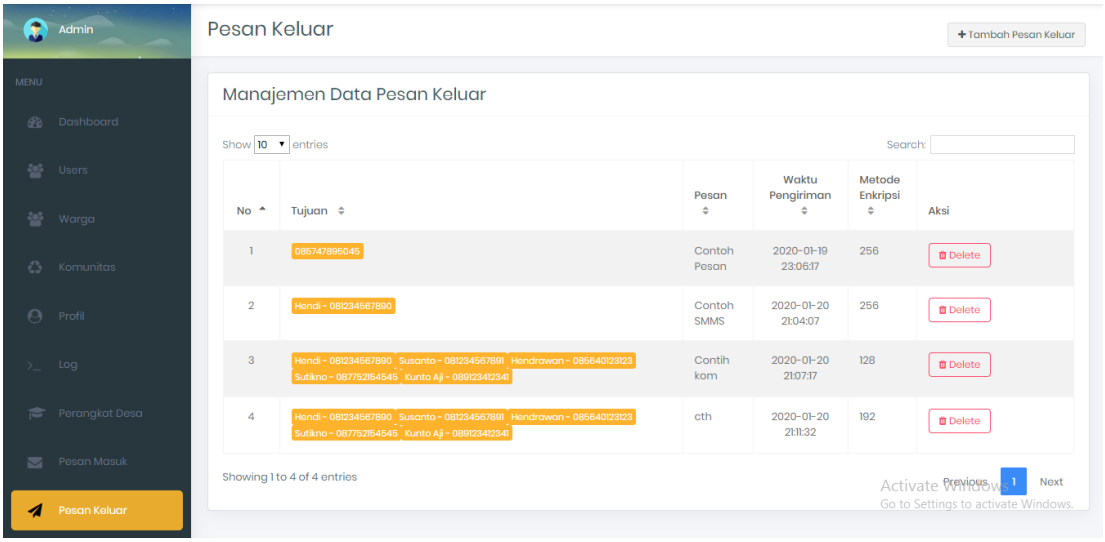
3.1. Hasil Implementasi

Sistem layanan SMS Desa ini dapat mengirimkan dan menerima pesan dari pemerintah desa kepada warganya maupun sebaliknya. Sehingga memudahkan bagi warga dalam penyampaian informasi atau aduan yang bersifat penting tanpa harus mendatangi ke kantor kelurahan terlebih dahulu. Selain itu, sistem ini juga dapat melakukan pengiriman massal (*broadcast*). Tampilan antarmuka dan database sistem layanan SMS Desa dapat dilihat pada Gambar 3 sampai Gambar 5. Gambar 3 merupakan tampilan pesan masuk pada sistem. Pesan masuk yang ditampilkan pada sistem merupakan bentuk pesan asli (*plain text*). Manajemen data pesan SMS masuk memuat informasi nama pengirim, isi pesan, waktu terima, metode enkripsi, dan aksi.



Gambar 3. Halaman Pesan Masuk.

Gambar 4 merupakan tampilan pesan keluar pada sistem. Pesan keluar yang ditampilkan pada sistem merupakan bentuk pesan asli (*plain text*). Manajemen data pesan keluar memuat informasi tujuan pengirim, isi pesan, waktu pengiriman, metode enkripsi, dan aksi. Admin dapat mengirimkan pesan baik *personal* maupun *broadcast* ke beberapa komunitas yang telah terdaftar.



Gambar 4. Halaman Pesan Keluar.

Gambar 5 merupakan tampilan hasil enkripsi pesan pada *database*. Pesan masuk akan tersimpan ke dalam *database* berupa *chiper text* sehingga pesan terjaga keamanannya.

id	pengirim	pesan	waktu_terima	metode_enkripsi	tipe	status
47	0895704341843	/BNyYMnEFVdta1zXf1HO7A==	2020-01-21 10:09:05	128		NULL
48	0895704341843	gaflsJJ0Qp6+Lg7mFw0V5Q==	2020-01-21 10:09:28	128		NULL
49	0895704341843	9klJPw8BiH4fQOqpQKK/cw==	2020-01-21 10:29:50	192		NULL
50	0895704341843	7dKyj9CD6wqXT9CfoWEPtg==	2020-01-21 10:30:12	192		NULL
51	0895704341843	UK6TvTzgl+wZWkSkx1QuRg==	2020-01-21 10:39:21	256		NULL
52	0895704341843	p1gP7UnhwEios97TWIcLjA==	2020-01-21 10:39:45	256		NULL
53	0895704341843	H9JAfVNR0qd+ocRWv5xL7Q==	2020-01-21 10:53:57	128		NULL
54	0895704341843	GzrytFnP+MmbO6KSj3EtpQ==	2020-01-21 10:54:44	128		NULL
55	0895704341843	Ubhr4aAuXgpFNWyUwq/V+Q==	2020-01-21 11:04:45	192		NULL
56	0895704341843	Zf46uxX26KVQkHtFwBUs7A==	2020-01-21 11:05:02	192		NULL
57	0895704341843	Jwa0E95DCvA/NYDjS/CJiQ==	2020-01-21 11:27:34	256		NULL
58	0895704341843	EDh3x6lw/oTsLIlSi1z07w==	2020-01-21 11:28:23	256		NULL

Gambar 5. Hasil Enkripsi Pesan di dalam *Database.*

3.2. Uji *Blackbox*

Hasil pengujian *blackbox* menunjukkan bahwa sistem sudah berjalan sesuai *input* yang diberikan. Hasil uji *blackbox* dapat dilihat pada Tabel 1.

Tabel 1. Hasil *Blackbox Testing.*

No.	Kelas Uji	Butir Uji	Hasil
1	*Login*	Verifikasi *password*	Berhasil
2	Menu Data Perangkat Desa	Tambah Data Perangkat Desa	Berhasil
		Ubah Data Perangkat Desa	Berhasil
		Pencarian Data Perangkat Desa	Berhasil
3	Menu Komunitas	Tambah Data Komunitas	Berhasil
		Ubah Data Komunitas	Berhasil
		Pencarian Data Komunitas	Berhasil
4	Menu Data Warga	Tambah Data Perangkat Desa	Berhasil
		Ubah Data Perangkat Desa	Berhasil
		Pencarian Data Perangkat Desa	Berhasil
5	Menu Data Warga	Tambah Data Warga	Berhasil
		Ubah Data Warga	Berhasil
		Pencarian Data Warga	Berhasil
6	Menu Data SMS	Buat Pesan	Berhasil
		Lihat Pesan Masuk	Berhasil
		Lihat Pesan Keluar	Berhasil
		Hapus Pesan	Berhasil

3.3. Uji Hasil Enkripsi 128-*bit*

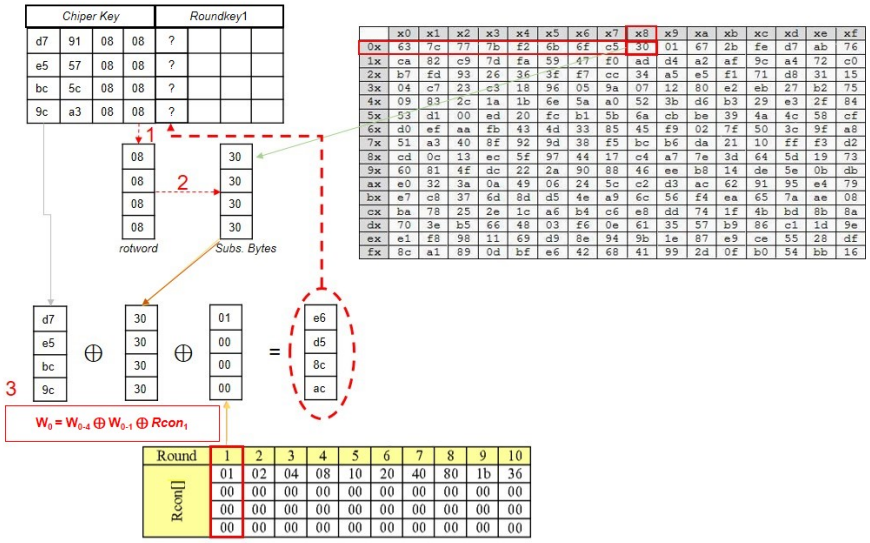
Pengujian hasil enkripsi dilakukan dengan cara menghitung manual pada proses enkripsi. Sebagai percobaan pengujian algoritma AES 128-*bit* untuk mengenkripsi kalimat “Saya ingin tanya” dengan kunci “d7e5bc9c91575ca3”. Adapun proses perhitungannya adalah sebagai berikut:
Konversikan *plain text* “Saya ingin tanya” ke bentuk *hexadecimal* menjadi “53 61 79 61 20 69 6e 67 69 6e 20 74 61 6e 79 61” dan kunci “d7 e5 bc 9c 91 57 5c a3 08 08 08 08 08 08 08 08”. “08”

pada kunci merupakan padding untuk memenuhi jumlah kapasitas 16 karakter dengan menambahkan nilai dari sisa jumlah karakter (Gumira et al., 2016).

1) Enkspansi Kunci
Ekspansi kunci atau pembangkitan kunci dilakukan untuk mendapatkan kunci ronde (*roundkey*) untuk proses enkripsi berikutnya. Langkah-langkah ekspansi kunci adalah sebagai berikut:
   a) Salin elemen kunci ke dalam blok matriks 4x4.
   W_0 = d7 e5 bc 9c
   W_1 = 91 57 5c a3
   W_2 = 08 08 08 08
   W_3 = 08 08 08 08

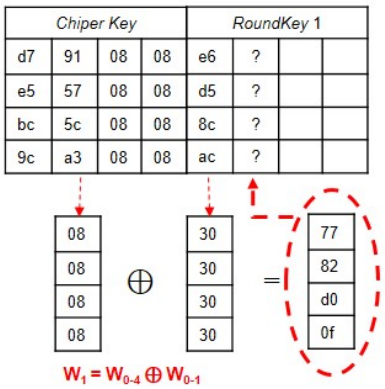
   b) Untuk mencari nilai W0 baru pada masing-masing *roundkey* dilakukan dengan menggunakan nilai W3 pada *roundkey* sebelumnya, kemudian *rotword* yaitu dengan memindahkan baris paling atas ke baris paling bawah, kemudian substitusikan dengan tabel *S-Box*, dan lakukan operasi XOR dengan Pers. (1).

$$W_i = W_{i-4} \oplus W_{i-1} \oplus R\text{-}Con_i \qquad (1)$$



   c) Untuk mencari nilai W1, W2, dan W3 pada masing-masing *roundkey* dilakukan dengan Pers. (2).

$$W_i = W_{i-4} \oplus W_{i-1} \qquad (2)$$



Hasil ekspansi kunci keseluruhan dapat dilihat pada Gambar 6.

Chiper Key				*RoundKey* 1				*RoundKey2*				*RoundKey3*				*RoundKey4*				*RoundKey5*			
d7	91	08	08	e6	77	7f	77	f7	80	ff	88	41	c1	3e	b6	90	51	6f	d9	b9	e8	87	5e
e5	57	08	08	d5	82	8a	82	b4	36	bc	3e	51	67	db	e5	02	65	be	5b	c2	a7	19	42
bc	5c	08	08	8c	d0	d8	d8	fa	2a	f2	2a	a2	88	7a	50	bd	35	4f	1f	86	b3	fc	e3
9c	a3	08	08	ac	0f	07	0f	59	56	51	5e	9d	cb	9a	cb	d3	18	82	49	e6	fe	7c	35

RoundKey6				*RoundKey7*				*RoundKey8*				*RoundKey9*				*RoundKey10*			
b5	5d	da	84	e0	bd	67	e3	ad	10	77	94	c8	d8	af	3b	b3	6b	c4	ff
d3	74	6d	2f	b6	c2	af	80	67	a5	0a	8a	40	e5	ef	65	e7	02	ed	88
10	a3	5f	bc	11	b2	ed	51	33	81	6c	3d	59	d8	b4	89	a9	71	c5	4c
be	40	3c	09	e1	a1	9d	94	f0	51	cc	58	d2	83	4f	17	30	b3	fc	eb

Gambar 6. Hasil Ekspansi Kunci.

2) Proses Enkripsi 128-*bit*

Setelah *roundkey* untuk masing-masing putaran didapatkan, langkah selanjutnya adalah proses enkripsi. Proses enkripsi 128-*bit* dilakukan sebanyak 10 putaran. Setiap putarannya terdiri dari proses *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundkey* sebanyak 9 putaran, dan pada putaran terakhir tanpa proses *MixColumns*. Adapun proses enkripsi algoritma AES adalah sebagai berikut:

a) *AddRoundkey*: langkah pertama proses enkripsi adalah melakukan XOR antara *plain text* “53 61 79 61 20 69 6e 67 69 6e 20 74 61 6e 79 61” dan kunci “d7 e5 bc 9c 91 57 5c a3 08 08 08 08 08 08 08 08” menjadi “84 84 c5 fd b1 3e 32 c4 61 66 28 7c 69 66 71 69”.

b) Dari hasil *AddRoundkey* pertama selanjutnya dilakukan proses *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundkey* sebanyak 9 putaran. Adapun hasilnya sebagai berikut:

i. *SubBytes*, pada tahap ini lakukan substitusi *byte* hasil *AddRoundkey* dengan tabel substitusi *(S-Box)*.
Hasil *SubBytes* putaran 1: 5f 5f a6 54 c8 b2 23 1c ef 33 34 10 f9 33 a3 f9
Hasil *SubBytes* putaran 2: 6a 53 d4 93 58 44 7e 92 fc 28 f5 cd 29 a9 30 1a
Hasil *SubBytes* putaran 3: 63 52 2b aa e9 54 22 14 f4 b0 56 fe de bb e1 a7
Hasil *SubBytes* putaran 4: 7e c6 1f a8 c4 85 55 e6 36 f1 cf 3f e2 c5 0c 71
Hasil *SubBytes* putaran 5: 5a b1 53 99 9f df 0f 0f e4 1d 6d 03 27 28 70 ee
Hasil *SubBytes* putaran 6: bf 43 8c ff 7b 2b ef 63 ca 5b 17 31 48 ab 9f 69
Hasil *SubBytes* putaran 7: 66 02 82 7e f7 b0 65 ce 4a 6f 46 46 76 2d fd c0
Hasil *SubBytes* putaran 8: ef 32 ca f7 da a7 3b bd e8 ce 86 7f e5 af 3f d9
Hasil *SubBytes* putaran 9: a6 2a 9c 00 b2 2f a5 b7 fd cf bc e9 5b e2 a4 4f

ii. *ShiftRows*,pada tahap ini lakukan pergeseran pada tiap-tiap baris *array state* pada blok matriks 4x4. Baris pertama tetap. Baris kedua geser satu *byte* ke kiri, baris kedua geser 2 *bytes* ke kiri, dan baris ketiga geser 3 *bytes* ke kiri.
Hasil *ShiftRows* putaran 1: 5f b2 34 f9 c8 33 a3 54 ef 33 a6 1c f9 5f 23 10
Hasil *ShiftRows* putaran 2: 6a 44 f5 1a 58 28 30 93 fc a9 d4 92 29 53 7e cd
Hasil *ShiftRows* putaran 3: 63 54 56 a7 e9 b0 e1 aa f4 bb 2b 14 de 52 22 fe
Hasil *ShiftRows* putaran 4: 7e 85 cf 71 c4 f1 0c a8 36 c5 1f e6 e2 c6 55 3f
Hasil *ShiftRows* putaran 5: 5a df 6d ee 9f 1d 70 99 e4 28 53 0f 27 b1 0f 03
Hasil *ShiftRows* putaran 6: bf 2b 17 69 7b 5b 9f ff ca ab 8c 63 48 43 ef 31
Hasil *ShiftRows* putaran 7: 66 b0 46 c0 f7 6f fd 7e 4a 2d 82 ce 76 02 65 46
Hasil *ShiftRows* putaran 8: ef a7 86 d9 da ce 3f f7 e8 af ca bd e5 32 3b 7f
Hasil *ShiftRows* putaran 9: a6 2f bc 4f b2 cf a4 00 fd e2 9c b7 5b 2a a5 e9

iii. *MixColumns* yaitu pada tahap ini lakukan perkalian matriks tertentu dengan matriks hasil proses *ShiftRows* pada masing-masing putaran.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 5f & c8 & ef & f9 \\ b2 & 33 & 33 & 5f \\ 34 & a3 & a6 & 23 \\ f9 & 54 & 1c & 10 \end{bmatrix} \rightarrow \begin{bmatrix} be & 29 & 2a & 3b \\ 85 & 04 & 64 & 35 \\ 95 & 5a & af & d0 \\ 8e & 7b & 87 & 4c \end{bmatrix}$$

Hasil *MixColumns* putaran 1: be 85 95 8e 29 04 5a 7b 2a 64 af 87 3b 35 d0 4c
Hasil *MixColumns* putaran 2: f7 fc f1 3b 6b cb be cd 45 40 4b 5d 14 c0 ca d7
Hasil *MixColumns* putaran 3: cb 96 69 f2 49 00 65 3e 1a f0 25 bf 8d e2 d1 e7
Hasil *MixColumns* putaran 4: d6 54 ed 2a 3f 8a ce e3 c1 60 fc 57 e4 b5 cf d0
Hasil *MixColumns* putaran 5: 4d a6 76 9b eb ac d2 fe 97 4e 7b 52 8a 4c 8d d1
Hasil *MixColumns* putaran 6: 66 b9 01 34 7b 88 1f ac 86 6b c7 a4 8b d5 9d 16
Hasil *MixColumns* putaran 7: 81 17 01 c7 c7 4b fb 6c af 43 31 f6 c9 9b 74 71
Hasil *MixColumns* putaran 8: 68 f2 2f a2 2e eb 68 71 56 55 14 27 c3 b3 20 ca
Hasil *MixColumns* putaran 9: d5 68 3b fc 91 c0 2e a6 f7 2a fe 17 84 12 00 ab

iv. *AddRoundkey*, lakukan XOR antara state baru dengan kunci masing-masing putaran.
Hasil *AddRoundkey* putaran 1: 58 50 19 22 5e 86 8a 74 55 ee 77 80 4c b7 08 43
Hasil *AddRoundkey* putaran 2: 00 48 0b 62 eb fd 94 9b ba fc b9 0c 9c fe e0 89
Hasil *AddRoundkey* putaran 3: 8a c7 cb 6f 88 67 ed f5 24 2b 5f 25 3b 07 81 2c
Hasil *AddRoundkey* putaran 4: 46 56 50 f9 6e ef fb fb ae de b3 d5 3d ee d0 99
Hasil *AddRoundkey* putaran 5: f4 64 f0 7d 03 0b 61 00 10 57 97 2e d4 0e 6e e4
Hasil *AddRoundkey* putaran 6: d3 6a 11 8a 26 fc bc ec 5c 06 98 98 0f fa 21 1f
Hasil *AddRoundkey* putaran 7: 61 a1 10 26 7a 89 49 cd c8 ec dc 6b 2a 1b 25 e5
Hasil *AddRoundkey* putaran 8: c5 95 1c 52 3e 4e 29 20 21 5f 78 eb 57 3b 1d 92
Hasil *AddRoundkey* putaran 9: 1d 28 62 2e 49 25 f6 25 58 c5 4a 58 bf 77 89 bc

c) Proses pada putaran terakhir:
   i. *SubBytes* putaran 10: a4 34 aa 31 3b 3f 42 3f 6a a6 d6 6a 08 f5 a7 65
   ii. *ShiftRows* putaran 10: a4 3f d6 65 3b a6 a7 31 6a f5 aa 3f 08 34 42 6a
   iii. *AddRoundkey* putaran 10: 17 d8 7f 55 50 a4 d6 82 ae 18 6f c3 f7 bc 0e 81

Pada perhitungan manual, hasil enkripsi dari “Saya ingin tanya” adalah 17 d8 7f 55 50 a4 d6 82 ae 18 6f c3 f7 bc 0e 81 kemudian dikonversikan ke *base*64 yaitu “F9h/VVCk1oKuGG/D97wOgQ==”. Hasil tersebut dicocokkan dengan hasil pada sistem. Tabel 1 menunjukkan perbandingan hasil enkripsi AES 128-*bit* antara perhitungan manual dan sistem. Berdasarkan perbandingan antara perhitungan manual algoritma AES kunci 128-*bit* dengan hasil enkripsi pada sistem Layanan SMS Desa dengan *plain text* dan kunci yang sama diperoleh hasil enkripsi yang sama. Perbandingan hasil enkripsi AES 128-*bit* dapat dilihat pada Tabel 2.

Tabel 2. Tabel Perbandingan Hasil Enkripsi AES 128-bit.

	Plain text	**Jenis enkripsi**	***Chiper text***
Perhitungan manual	Saya ingin tanya	AES 128-*bit*	F9h/VVCk1oKuGG/D97wOgQ==
Hasil enkripsi pada sistem	Saya ingin tanya	AES 128-*bit*	F9h/VVCk1oKuGG/D97wOgQ==

3.4. Uji *CrackStation*

Hasil pengujian terhadap 3 sampel diketahui bahwa algoritma AES baik kunci 128-*bit*, 192-*bit*, maupun 256-*bit* 100% tidak dapat dipecahkan. Hasil uji *CrackStation* dapat dilihat pada Tabel 3.

Tabel 3. Hasil Uji *CrackStation.*

No.	*Plain text*	Kunci	Hasil Uji
1.	Laporantahun2019	AES 128-*bit*	Tidak berhasil
		AES 192-*bit*	Tidak berhasil
		AES 256-*bit*	Tidak berhasil
2.	Pengumuman	AES 128-*bit*	Tidak berhasil
		AES 192-*bit*	Tidak berhasil
		AES 256-*bit*	Tidak berhasil
3.	Lokasi kejadian	AES 128-*bit*	Tidak berhasil
		AES 192-*bit*	Tidak berhasil
		AES 256-*bit*	Tidak berhasil

3.5. Uji *Avalanche Effect* (AE)

Pengujian AE dilakukan dengan menganalisis nilai perubahan *bit* dari hasil enkripsi pada sistem. Hasil uji AE dapat dilihat pada tabel 4. Berdasarkan hasil uji AE pada 3 percobaan, kunci 192-*bit* dan 256-*bit* lebih direkomendasikan untuk digunakan karena nilai AE baik yaitu berada pada rentang 45%-60% (Sutanto et al., 2015).

Tabel 4. Hasil Uji *Avalanche Effect.*

Plain text	*Chiper text*	Perubahan *bit*	Jumlah *bit* keseluruhan	AE (%)
Percobaan 1 AES 128-*bit*				
Laporantahun2019	H9JAfVNR0qd+ocRWv5xL7Q==	57	128	44,53
Laporantahun201g	GzrytFnP+MmbO6KSj3EtpQ==			
Percobaan 2 AES 192-*bit*				
Laporantahun2019	Ubhr4aAuXgpFNWyUwq/V+Q==	62	128	48,44
Laporantahun201g	Zf46uxX26KVQkHtFwBUs7A==			
Percobaan 3 AES 256-*bit*				
Laporantahun2019	Jwa0E95DCvA/NYDjS/CJiQ==	72	128	56,25
Laporantahun201g	EDh3x6lw/oTsLllSi1z07w==			

3.6. Uji Kelayakan Sistem

Hasil uji kelayakan dapat dilihat pada Tabel 5. Berdasarkan hasil uji kelayakan sistem yang dilakukan oleh 2 orang ahli, diperoleh persentase sebesar 93,05%. Dengan persentase tersebut maka sistem layak untuk digunakan.

Tabel 5. Hasil Uji Kelayakan Sistem.

No	Nama Responden	Aspek Kelayakan									
		Kinerja Sistem			Efisiensi Sistem		Layanan Sistem	Ekonomi Sistem		Kontrol Sistem	Informasi Sistem
		Nomor Angket									
		1	2	4	3	9	5	6	7	8	10
1	Aji Purwinarko	4	4	4	4	4	4	4	4	4	4
2	Ardian Rizqi Rahmawan	4	4	3	3	4	3	3	4	4	3
Jumlah		8	8	7	7	8	7	7	8	8	7
Jumlah Maksimum		8	8	8	8	8	8	8	8	8	8
Persentase		95,83			93,75		87,5	93,75		100	87,5
Rata-rata Persentase		**93,05**									

Sistem yang dibuat pada penelitian ini memiliki perbedaan dengan penelitian yang sudah dilakukan oleh peneliti terdahulu, di antaranya informasi berbasis SMS Gateway pada Kantor Dispendukcapil Kabupaten Belu oleh Layansari & Marisa (2018), pada penelitian tersebut belum adanya keamanan pada data pesan yang tersimpan di *database*. Pada penelitian yang dilakukan oleh Alvianto & Darmaji (2015) keamanan SMS menggunakan algoritma RSA, sedangkan pada penelitian ini menggunakan algoritma AES. Penelitian yang dilakukan oleh Azhar & Kurniawan (2017) dan Ibrahim (2017) yang menerapkan algoritma AES untuk keamanan data SMS, perbedaan pada penelitian ini yaitu pada implementasi pembangunan sistemnya.

Guna meningkatkan keamanan data SMS, dalam penelitian ini peneliti menggunakan tiga variasi kunci AES 128-*bit*, 192-*bit*, dan 256-*bit*. Pengujian algoritma AES dilakukan dengan melakukan perbandingan hasil enkripsi antara perhitungan manual dan hasil enkripsi pada sistem. selanjutnya pengujian AE, pada pengujian AE diperoleh nilai AE masing-masing kunci 128-*bit* sebesar 44,53%, 192-*bit* sebesar 48,44%, dan 256-*bit* sebesar 56,25%. Dengan demikian, kunci 192-*bit* dan 256-*bit* lebih direkomendasikan untuk digunakan karena nilai AE baik yaitu berada pada rentang 45% - 60% (Sutanto et al., 2015). Pengujian menggunakan *software* penyerang *CrackStation* pada 20 sampel *plain text*, 100% hasil enkripsi tidak dapat dipecahkan. Persentase rata-rata kelayakan sistem sebesar 93,05%.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan terkait sistem layanan SMS Desa dengan memanfaatkan teknologi informasi dan layanan SMS *Gateway*, maka dapat disimpulkan bahwa sistem ini dapat membantu pemerintahan desa dalam meningkatkan pelayanan terhadap warganya terkait informasi dan aduan. Serta dengan mengimplementasikan algoritma AES dapat meningkatkan keamanan terkait data SMS. Sebagaimana dalam uji ketahanan terhadap serangan menggunakan *software* penyerang *CrackStation, chiper text* 100% tidak dapat dipecahkan. Pada pengujian *avalanche effect* dihasilkan perbandingan tingkat keamanan dari proses enkripsi kunci 128-*bit*, 192-*bit*, dan 256-*bit*. Nilai *avalanche effect* enkripsi AES 192-*bit* sebesar 48,44% dan 256-*bit* sebesar 56,25% lebih aman dibandingkan dengan AES 128-*bit* sebesar 44,53%. Dan berdasarkan uji kelayakan sistem oleh ahli diperoleh persentase sebesar 93,05%, sistem layanan SMS Desa sangat layak digunakan.

DAFTAR PUSTAKA

Afrina, M., & Ibrahim, A. (2015). Pengembangan Sistem Informasi SMS Gateway Dalam Meningkatkan Layanan Komunikasi Sekitar Akademika Fakultas Ilmu Komputer Unsri. *Jurnal Sistem Informasi (JSI)*, *7*(2), 852–864.

Alvianto, A. R., & Darmaji. (2015). Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android. *JURNAL SAINS Dan SENI ITS*.

Atmojo, W. P., Isnanto, R. R., & Kridalukmana, R. (2016). Implementasi Aplikasi Kriptografi Pada Layanan Pesan Singkat (SMS) Menggunakan Algoritma RC6 Berbasis Android. *Jurnal Teknologi Dan Sistem Komputer*. https://doi.org/10.14710/jtsiskom.4.3.2016.450-453

Azhar, R., & Kurniawan, K. (2017). Aplikasi Keamanan Sms Menggunakan Algoritma Rijndael. *Jurnal Matrik*, *16*(1), 105. https://doi.org/10.30812/matrik.v16i1.15

Gumira, G., Ernawati, & Erlanshari, A. (2016). Implementasi Metode Advanced Encryption Standard (AES) Dan Message Digest 5 (MD5) Pada Enkripsi Dokumen (Studi Kasus LPSE UNIB). *Jurnal Rekursif*.

Ibrahim, A. A. (2017). Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard). *Jurnal Teknik Informatika STMIK Antar Bangsa*, *3*(1), 53–60.

Layansari, F. A., & Marisa, F. (2018). Perancangan Sistem Pelayanan Informasi Berbasis Sms Gateway Pada Kantor Dispendukcapil Kabupaten Belu. *J I M P - Jurnal Informatika Merdeka Pasuruan*. https://doi.org/10.37438/jimp.v3i2.169

Muharram, F., Azis, H., & Manga, A. R. (2018). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES). *Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informasi*.

Prasetya, D. R. (2013). Analisis Pengelolaan Pengaduan Masyarakat Dalam Rangka Pelayanan Publik (Studi Pada Dinas Komunikasi Dan Informatika Kota Malang). *Jurnal Administrasi*

Publik Mahasiswa Universitas Brawijaya.

Purba, I. S., & Djamin, D. (2015). Partisipasi Masyarakat dalam Meningkatkan Good Governance di Tingkat Desa. *Jurnal Ilmu Pemerintahan Dan Sosial Politik UMA*, *3*(1), 25–36. https://doi.org/10.31289/jppuma.v3i1.908

Sutanto, L., Budhi, G. S., & Santoso, L. W. (2015). PERBANDINGAN APLIKASI MENGGUNAKAN METODE CAMELLIA 128 BIT KEY DAN 256 BIT KEY. *Jurnal Informatika*. https://doi.org/10.9744/informatika.12.2.109-116