IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) PADA LAYANAN SMS DESA

Skripsi

Diajukan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Pendidikan Program Studi Pendidikan Teknik Informatika dan Komputer

Oleh:

Intan Fitriani NIM. 5302414018

PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS NEGERI SEMARANG

2020

PERSETUJUAN PEMBIMBING

Nama : Intan Fitriani

NIM : 5302414018

Program Studi : Pendidikan Teknik Informatika dan Komputer

Judul Skripsi : Implementasi Algoritma Advanced Encryption Standard (AES) Pada Layanan SMS Desa

Skripsi ini telah disetujui oleh pembimbing untuk diajukan ke sidang panitia ujian Skripsi Program Studi Pendidikan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Semarang.

Semarang, Januari 2020

Pembimbing

Aryo Baskoro Utomo, S.T., M.T.
NIP. 198409092012121002

PENGESAHAN

Skripsi dengan judul Implementasi Algoritma *Advanced Encryption Standard* (AES) Pada Layanan SMS Desa telah dipertahankan dihadapan Panitia Ujian Skripsi Fakultas Teknik Elektro Universitas Negeri Semarang pada tanggal Februari 2020.

Nama : Intan Fitriani

NIM : 5302414018

Program Studi : S-1 Pendidikan Teknik Informatika dan Komputer

Panitia Ujian:

Ketua Panitia

Ir. Ulfah Mediaty Arief, M.T. IPM
NIP. 196605051998022001

Sekretaris Panitia

Budi Sunarko, S.T., M.T., Ph.D.
NIP. 197101042006041001

Penguji I

Dr. Ir. Subiyanto, S.T., M.T.
NIP. 197411232005011001

Penguji II

Budi Sunarko, S.T., M.T., Ph.D.
NIP. 197101042006041001

Penguji III/Pembimbing

Aryo Baskoro Utomo, S.T., M.T.
NIP. 198409092012121002

Mengetahui,

Dekan Fakultas Teknik Universitas Negeri Semarang

Dr. Nur Qudus, M.T.
NIP. 196911301994031001

PERNYATAAN KEASLIAN

Dengan ini saya menyatakan:

1. Skripsi/TA ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, magister, dan/atau doktor), baik di Universitas Negeri Semarang (UNNES) maupun perguruan tinggi lain.
2. Karya tulis ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan Pembimbing dan masukan Tim Penguji.
3. Dalam karya tulis ini terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebaga acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya ini, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini,

Semarang, Februari 2020

Intan Fitriani
NIM. 5302414018

MOTTO DAN PERSEMBAHAN

“Selalu Libatkan Allah SWT dalam Segala Hal”.

“Keramahtamahan dalam perkataan menciptakan keyakinan, keramahtamahan dalam pemikiran menciptakan kedamaian, keramahtamahan dalam memberi menciptakan kasih”. (Lao Tse)

Skripsi ini penulis persembahkan kepada:

1. Allah SWT yang telah memberikan kemudahan dan kelancaran dalam penyusunan skripsi ini,
2. Kedua orang tua yang selalu memberikan doa dan dukungan baik moril maupun materiil,
3. Kakak dan seluruh keluarga besar yang selalu memberikan doa dan dukungan,
4. Teman-teman terdekat yang selalu memberikan doa dan dukungan,
5. Teman-teman PTIK 2014.

ABSTRAK

Intan Fitriani. 2018. Implementasi Algoritma *Advanced Encryption Standard* (AES) pada Layanan SMS Desa. Aryo Baskoro Utomo, S.T., M.T. Pendidikan Teknik Informatika dan Komputer.

SMS sudah mulai digunakan untuk berhubungan 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. Tujuan penelitian ini adalah menambahkan keamanan data SMS pada sistem Layanan SMS Desa agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

Metode penelitian yang digunakan adalah metode *waterfall* yang bertujuan membangun dan menguji tingkat keamanan sistem Layanan SMS Desa. Tahapan penelitian antara lain *communication*, *planning*, *modeling*, *construction*, dan *deployment*. Algoritma kriptografi yang digunakan adalah algoritma *Advanced Encryption Standard* (AES). Sistem layanan SMS Desa diuji menggunakan *blackbox testing* sedangkan keamanan sistem diuji menggunakan *software* penyerang dan *avalanche effect*.

Hasil dari penelitian ini membuktikan bahwa penerapan algoritma AES dapat memberikan keamanan terhadap data SMS pada sistem Layanan SMS Desa. Hal ini berdasarkan uji *brute force* menggunakan *software CrackStation* bahwa *chiper text* tidak dapat dipecahkan. Pada uji *avalanche effect* (AE) diperoleh nilai AE masing-masing kunci AES 128-*bit*, 192-*bit*, dan 256-*bit* sebesar 44,53%, 48,44%, dan 56,25%. Dengan demikian, kunci AES 192-*bit* dan 256-*bit* lebih direkomendasikan untuk digunakan karena nilai AE berada pada rentang 45%-60%. Berdasarkan uji kelayakan sistem oleh ahli diperoleh persentase sebesar 93,05% sehingga sangat layak untuk digunakan.

Kata Kunci: Layanan SMS Desa, AES, brute force, avalanche effect.

KATA PENGANTAR

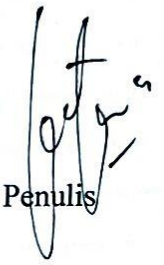
Puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya seingga penulis dapat menyelesaikan skripsi dengan judul "Implementasi Algoritma *Advanced Encryption Standard* (AES) Pada Layanan SMS Desa". Sholawat serta salam penulis haturkan kepada Rasulullah SAW. Skripsi ini disusun sebagai salah satu persyaratan meraih gelar Sarjana Pendidikan pada program studi S1 Pendidikan Teknik Informatika dan Komputer Universitas Negeri Semarang. Penyelesaian skripsi ini tidak lepas dari bantuan berbagai pihak, oleh karena itu penulis menyampaikan ucapan terimakasih kepada:

1. Dr. Nur Qudus, M.T., Dekan Fakultas Teknik Universitas Negeri Semarang yang telah memberikan kesempatan untuk menyelesaikan skripsi ini.
2. Ir. Ulfah Mediaty Arief, M.T., Ketua Jurusan Teknik Elektro Universitas Negeri Semarang.
3. Budi Sunarko, S.T., M.T., Ph.D., Koordinator Program Studi Pendidikan Teknik Informatika dan Komputer Universitas Negeri Semarang sekaligus selaku penguji II.
4. Aryo Baskoro Utomo, S.T., M.T., selaku Dosen Pembimbing yang dengan sabar memberikan bimbingan, arahan, petunjuk, serta motivasi dalam menyelesaikan skripsi ini.
5. Dr. Ir. Subiyanto, S.T., M.T. Dosen Penguji I yang telah memberikan waktu dan saran dalam menyelesaikan skripsi ini.

7. Teman-teman PTIK Universitas Negeri Semarang Angkatan 2014 yang telah membantu.
8. Berbagai pihak yang telah memberi bantuan untuk karya tulis ini yang tidak dapat disebutkan satu persatu.

Penulis berharap semoga semua pihak yang telah membantu dalam penyclesaian skripsi ini mendapatkan balasan kebaikan dari Allah SWT. Semoga skripsi ini dapat bermanfaat untuk pelaksanaan pembelajaran.

Semarang, Februari 2020



Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dewasa ini berkembang sangat pesat. Seperti sekarang ini, banyak sekali membawa perubahan yang mengarah pada penyempurnaan dibidang-bidang tertentu. Salah satu teknologi informasi yang sudah ada saat ini adalah telepon seluler. Hampir semua kalangan mulai dari masyarakat perkotaan sampai ke pedesaan menggunakan layanan teknologi telepon seluler baik berbasis *Global System for Mobile Communication* (GSM) maupun *Code Division Multiple Access* (CDMA). Salah satu fitur yang terdapat pada telepon seluler adalah fitur *Short Message Service* (SMS) (Katadata, 2017).

SMS merupakan media untuk mengirim dan menerima pesan singkat berupa teks melalui telepon seluler. Pengguna telepon seluler dapat bertukar informasi secara jarak jauh. Seiring perkembangan teknologi dan kebutuhan maka SMS tidak hanya digunakan untuk mengirimkan atau bertukar informasi antara dua orang yang saling mengenal atau membutuhkan, kini SMS sudah mulai digunakan untuk berhubungan antara seseorang dengan sistem sesuai dengan kebutuhan (Afrina dan Ibrahim, 2015).

Pada sistem SMS terdapat pula istilah SMS *Gateway*. SMS *Gateway* merupakan sebuah program yang dapat mengkomunikasikan antara sistem operasi komputer dengan perangkat komunikasi yang terpasang untuk mengirim atau

menerima SMS (Fachriyah dan Tajidun, 2015). SMS *Gateway* saat ini sudah banyak diterapkan di berbagai bidang. Salah satunya pada bidang pemerintahan.

Menurut Permen no. 113 tahun 2014, Pemerintahan Desa adalah penyelenggaraan urusan pemerintahan dan kepentingan masyarakat setempat dalam sistem pemerintahan Negara Kesatuan Republik Indonesia. Pemerintahan Desa merupakan struktur birokrasi terkecil dari suatu negara dimana pemerintahan dilakukan oleh perangkat desa, dan dikepalai oleh kepala desa. Untuk menyelenggarakan suatu pemerintahan yang efektif dan lebih demokratis menuntut adanya praktek pemerintah lokal yang lebih baik, dalam hal ini pemerintah desa, yang membuka peran serta masyarakat menuju masyarakat yang lebih maju. Diperlukan sistem tata kelola pemerintah yang baik, khususnya pemerintah desa, serta partisipasi dari masyarakat (Purba dan 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 seberapa besar keberhasilan pemerintah khususnya desa dalam melaksanakan suatu kegiatan (Prasetya, 2013).

Banyak sekali media yang dapat digunakan untuk mewujudkan suatu layanan informasi dan pengaduan. Salah satunya dengan memanfaatkan teknologi SMS. Meskipun jumlah pengguna layanan SMS mengalami penurunan, namun dalam beberapa kondisi, layanan SMS masih diminati karena dapat diandalkan di wilayah dengan kualitas jaringan minim sekalipun. Namun dalam beberapa kasus, terkadang komunikasi tersebut bersifat rahasia. Pesan yang dikirimkan melalui aplikasi SMS belum terproteksi dengan baik. Dalam pengirimannya, SMS tidak langsung sampai

ke penerima melainkan harus melewati *Short Message Service Center* (SMSC). Dengan tersimpannya SMS pada SMSC, seseorang yang dapat mengakses SMSC dapat dengan mudah memperoleh atau melihat SMS tersebut (Atmojo, *et al*., 2016). Banyak sekali kasus penyadapan pesan SMS. Salah satu kasus penyadapan terjadi pada tahun 2018, terjadi penyadapan pada pesan SMS sejumlah lebih dari 26 juta di perusahaan telekomunikasi di California. Perusahaan bernama Vovox bertindak sebagai *gateway* yang meneruskan pesan ke penggguna. Vovox menyediakan *database* sebagai penyimpanan data SMS. Namun *database* tersebut tidak dilapisi dengan keamanan yang memadai sehingga memberikan celah bagi peretas untuk melakukan penyadapan secara besar-besaran mengingat banyaknya informasi penting milik pengguna (Wardani, 2018).

Keamanan dan kerahasiaan sebuah data atau informasi merupakan hal yang sangat penting, baik dalam suatu organisasi seperti perusahaan, perguruan tinggi, maupun individual (Sulaiman dan Vebu, 2018). Untuk meningkatkan keamanan dan kerahasiaan data dapat dilakukan dengan cara kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data (Arief dan Ragil, 2016).

Terdapat beberapa algoritma kriptografi yang dapat digunakan untuk keamanan data, salah satunya algoritma *Advanced Encryption Standard* (AES). Algoritma AES merupakan algoritma *simetris* yaitu suatu algoritma yang menggunakan kunci yang sama dalam proses ekripsi maupun dekripsi. Algoritma AES merupakan algoritma yang sangat sensitif, dimana tiap karakter masukan akan

menghasilkan keluaran yang berbeda sehingga sangat baik untuk keamanan data SMS (Azhar dan Kurniawan, 2016).

AES merupakan algoritma kriptografi yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia hingga saat ini. Pada tahun 2001, AES digunakan sebagai *standard* algoritma kriptografi terbaru yang digunakan sebagai pengganti algoritma *Data Encryption Standard* (DES) yang sudah berakhir masa penggunaannya (Muharram, *et al*., 2018). DES dianggap sudah tidak aman lagi karena kuncinya dapat ditemukan dalam beberapa hari menggunakan perangkat keras khusus (Munir, 2006).

Berdasarkan permasalahan tersebut, maka dalam penelitian ini akan dibuat implementasi kriptografi pada SMS *Gateway* dengan judul "Implementasi Algoritma *Advanced Encryption Standard* (AES) pada Layanan SMS Desa" guna meningkatkan keamanan data SMS.

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka rumusan masalah pada penelitian ini antara lain:

1. Apa hasil implementasi algoritma AES pada SMS *Gateway*?
2. Apa hasil pengujian tingkat keamanan data SMS dengan menggunakan algoritma AES pada Layanan SMS Desa berdasarkan *brute force* dan *avalanche effect*?

1.3 Batasan Masalah

Berdasarkan rumusan masalah, maka pada penelitian ini diperlukan batasan masalah agar tujuan penelitian ini dapat tercapai. Adapun batasan masalah yang dibahas pada penelitian ini anatara lain:

1. Sistem yang dibangun difokuskan pada layanan SMS saja.
2. Proses enkripsi dan dekripsi hanya mencakup data SMS saja.
3. Proses enkripsi dan dekripsi menggunakan algoritma AES tiga variasi kunci, yaitu 128-*bit*, 192-*bit*, dan 256-*bit*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, maka tujuan yang ingin dicapai pada penelitian ini antara lain:

1. Mengetahui implementasi algoritma AES pada SMS *Gateway*.
2. Mengetahui dan menguji tingkat keamanan data SMS dengan menggunakan algoritma AES pada Layanan SMS Desa berdasarkan *brute force* dan *avalanche effect.*

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini antara lain:

1. Menghasilkan suatu sistem yang menambah tingkat keamanan data SMS dalam sistem layanan SMS desa.
2. Menambah wawasan dan pengalaman ilmu yang diperoleh selama perkuliahan serta mampu menerapkan dan menghasilkan sebuah sistem dari ilmu tersebut.

BAB II

KAJIAN PUSTAKA DAN LANDASAN TEORI

2.1 Kajian Pustaka

Penelitian yang relevan dengan SMS *Gateway* dan keamanan pernah dilakukan oleh beberapa peneliti terdahulu, antara lain:

Layansari dan Marisa (2018) telah melakukan penelitian tentang perancangan sistem pelayanan informasi berbasis SMS *Gateway* pada Kantor Dispendukcapil Kabupaten Belu. Sistem informasi tersebut dapat mempermudah pihak kantor dalam meningkatkan mutu pelayanan terhadap masyarakat, selain itu juga memberikan informasi seputar kantor dan otoritas negara melalui SMS. Tingkat presentasi kepuasan pada sistem tersebut mencapai 72,62% lebih unggul berbanding dengan sistem pelayanan berbasis *web*. Kekurangan pada sistem tersebut yaitu belum adanya keamanan pada data SMS.

Afridi (2017) telah melakukan penelitian tentang penerapan *Aplication Programming Interface* (API) SMS *Gateway* melalui layanan *web*. Hasil dari penelitian tersebut berupa aplikasi yang dapat memenuhi kebutuhan pelayanan sebuah organisasi. Pada penelitian tersebut dapat diketahui bahwa API SMS *Gateway* memberikan kemudahan bagi penggunanya. Dalam mengakses SMS dapat melalui PC ataupun *smartphone* sehingga lebih fleksibel. Berbeda dengan SMS *Gateway* menggunakan Gammu yang mengharuskan modem selalu terhubung dengan PC untuk dapat mengakses SMS.

Alvianto dan Darmaji (2015) telah melakukan penelitian tentang pengamanan pesan SMS dengan menggunakan algoritma *Rivest Shamir Adleman* (RSA) berbasis Android. Hasil dari penelitian tersebut berupa modifikasi aplikasi keamanan pesan yang diterapkan pada Android. keamanan pesan akan terjamin setelah dilakukan proses enkripsi menggunakan algoritma RSA.

Ibrahim (2017) telah melakukan penelitian tentang rancangan aplikasi pengamanan data file dan teks dengan algoritma AES. Hasil penelitian tersebut dapat diketahui bahwa algoritma AES cukup sulit dipecahkan karena belum ada *software* penyerang yang mampu untuk memecahkan hasil enkripsi. Namun dalam pengimplementasiannya, cakupan sistem pada penelitian tersebut masih kecil dan sangat mendasar, sistem tersebut dibangun menggunakan Microsoft Visual Studio 2010.

Azhar dan Kurniawan (2016) telah melakukan penelitian tentang aplikasi keamanan SMS menggunakan algoritma AES. Penelitian tersebut bertujuan untuk meningkatkan keamanan data SMS. Aplikasi tersebut diimplementasikan pada perangkat Android. Sedangkan sistem pada penelitian ini dibuat menggunakan bahasa pemrograman PHP dengan *framework* Laravel dan *database* MySQL. Hasil dari penelitian tersebut berdasarkan pengujian terhadap waktu proses enkripsi dan dekripsi, dapat diketahui bahwa panjang *plain text* dan kunci akan berpengaruh terhadap waktu proses enkripsi dan dekripsi.

Dari beberapa penelitian tersebut, dapat disimpulkan bahwa sistem keamanan data dapat diimplementasikan pada sistem layanan SMS *Gateway* yang bertujuan untuk meningkatkan keamanan serta kerahasiaan data SMS.

2.2 Landasan Teori

2.2.1 *Short Message Service* (SMS)

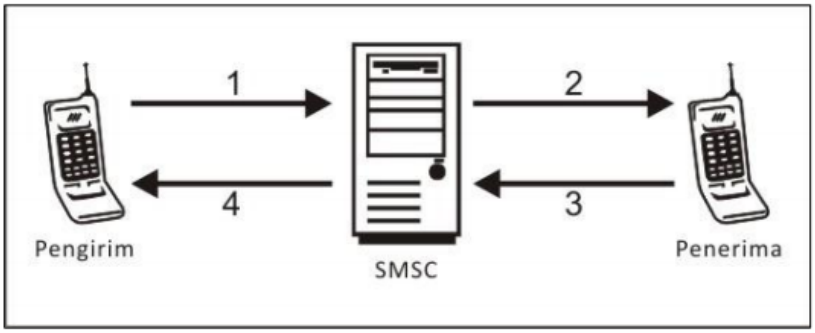
SMS merupakan teknologi yang memungkinkan pengiriman dan penerimaan pesan dalam bentuk teks antar telepon seluler (Noviyantono, 2012). Selain teks, SMS juga dapat memuat data *binary*, misalnya logo, *ringtone*, *bussiness card* (*vCard*) dan konfigurasi *Wireless Aplication Protocol* (WAP) (Pardede, 2014).

Data yang dapat dibawa oleh SMS sangat terbatas, satu pesan SMS dapat memuat:

1. Maksimum 160 karakter jika menggunakan *encoding* karakter 7 *bit* (biasa digunakan untuk *encoding* huruf latin).
2. Maksimum 140 karakter jika menggunakan *encoding* karakter 8 *bit* (biasa digunakan untuk mengirim *ringtone* dan *image-smart messaging*).
3. Maksimum 70 karakter jika menggunakan *encoding* karakter 16 *bit unicode* (untuk SMS yang memuat huruf *non*-latin seperti Cina, Jepang, Arab, dan Korea).

Cara kerja SMS adalah pengguna mengirimkan sebuah pesan dari satu terminal ke pengguna yang lain dengan bantuan sebuah entitas yang biasa disebut *Short Message Service Center* (SMSC). Pada saat pengguna mengirimkan pesan SMS dari satu terminal, pesan tersebut tidak dapat langsung sampai pada terminal tujuan. Sebelumnya pesan tersebut dikirim dahulu menuju SMSC. Kemudian SMSC mengirimkan pesan tersebut menuju terminal tujuan akhir. Setelah pesan masuk, secara otomatis penerima pengirimkan pemberitahuan bahwa pesan telah sampai dan diterima menuju SMSC. Kemudian SMSC mengirimkan laporan pengiriman

kepada pengirim yang memberitahukan bahwa pesan telah terkirim. Pada SMSC tersebut data SMS berpeluang untuk disadap oleh orang yang memiliki akses ke SMSC sehingga kerahasiaan pesannya terancam (Satriawan, 2014). Gambar 2.1 menunjukkan skema cara kerja SMS.



Gambar 2.1 Skema Cara Kerja SMS (Pardede, 2014)

2.2.2 SMS *Gateway*

SMS *Gateway* merupakan perangkat penghubung antara pengirim SMS dengan basis data. Perangkat ini terdiri satu set PC, telepon, dan program aplikasi. Program aplikasi ini yang akan meneruskan setiap *request* dari setiap SMS yang masuk dengan melakukan *query* ke dalam basis data, kemudian diberi respon dari hasil *query* kepada pengirim. Artinya, SMS tersebut harus bisa melakukan transaksi dengan basis data. Untuk itu perlu dibangun sebuah sistem yang disebut sebagai SMS *Gateway*. Pada prinsipnya, SMS *Gateway* adalah sebuah perangkat lunak yang menggunakan bantuan komputer dan memanfaatkan teknologi seluler yang diintegrasikan untuk mendistribusikan pesan-pesan yang di *generate* pada sistem informasi melalui media SMS yang ditangani oleh jaringan seluler (Fallis, 2013). Gambar 2.2 menunjukkan skema SMS *Gateway*.

Gambar 2.2 Skema SMS *Gateway* (Fallis, 2013)

Adapun beberapa fitur yang terdapat pada SMS *Gateway* menurut Wahana (2014:2) antara lain:

1. *Auto Reply*, fitur SMS yang secara otomatis akan mengirimkan balasan dengan format tertentu.
2. *Broadcast Message*, yaitu fitur yang dapat mengirimkan SMS secara massal dalam waktu bersamaan. Fitur ini banyak disediakan pada telepon seluler maupun *gadget.*
3. Pengiriman Terjadwal, fitur ini memungkinkan pengiriman SMS dalam waktu yang sudah ditetapkan sebelumnya.

Mekanisme kerja pengiriman SMS dibagi menjadi 3 bagian, yaitu: Intra-operator SMS dimana pengiriman SMS dalam satu operator, Inter-operator SMS dimana pengiriman SMS antar operator yang berbeda, dan SMS Internasional dimana pengiriman SMS dari operator suatu negara ke negara lain (Afrina dan Ibrahim, 2015).

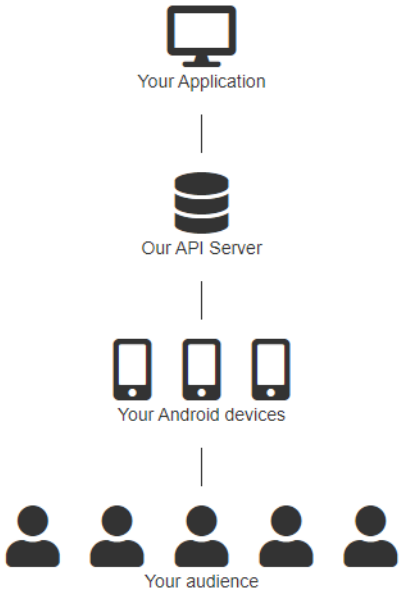
Pada umumnya, pembuatan SMS *Gateway* dapat dilakukan dengan dua cara, diataranya menggunakan perangkat tambahan berupa modem dan aplikasi pendukung seperti Gammu dan menggunakan aplikasi dari pihak ketiga seperti smsgateway.me. Menurut Winarni (2018), masing-masing cara tersebut memiliki kelebihan dan kekurangan, diantaranya sebagai berikut:

1. Pada penggunaan Gammu, modem harus tertancap pada PC atau laptop selama 24 jam penuh selama SMS digunakan. Sedangkan smsgateway.me dapat online 24 jam tanpa harus menyalakan PC atau laptop.
2. Penggunaan layanan pihak ketiga lebih mudah, *user* cukup mengirim SMS secara *programatically* ke *server*, kemudian sistem dan perangkat yang akan mengirim SMS ke penerima.

2.2.3 Smsgateway.me

Smsgateway.me merupakan aplikasi yang memungkinkan pengguna untuk mengirim dan menerima SMS secara *programatically*. Aplikasi smsgateway.me memberikan kode-kode singkat yang dapat ditambahkan di dalam program berbasis *web* sebagai sarana API. API merupakan sebuah teknologi untuk memfasilitasi pertukaran informasi atau data antara dua atau lebih perangkat lunak, API dapat dikatakan sebuah *interface virtual* antara dua fungsi perangkat lunak yang saling bekerjasama. Tulach dalam Yulianto (2018) menyatakan bahwa API bukan hanya satu *set class* dan *method* atau fungsi dan *signature* yang sederhana. API bertujuan untuk mengintegrasikan atau menggabungkan antara dua aplikasi yang berbeda secara bersamaan. API terdiri dari berbagai elemen seperti *function*, *protocol*, dan *tools* lainnya untuk membuat aplikasi.

API berperan sebagai pembawa pesan yang menerima permintaan pengguna dan memberitahu sistem perintah apa yang harus dilakukan dan memberikan *respon* sesuai permintaan. Dengan demikian, *programmer* tidak perlu lagi membuang waktu untuk membuat fitur serupa dalam hal ini SMS *Gateway* sehingga lebih efisien (Yulianto, 2018). Gambar 2.3 merupakan arsitektur API SMS *Gateway* dari aplikasi smsgateway.me.



Gambar 2.3 Arsitektur API SMS *Gateway* dari aplikasi smsgateway.me (http://smsgateway.me/)

Syarat penggunaan smsgateway.me cukup sederhana, *instal* aplikasi smsgateway.me di android. Android berfungsi sebagai SMS *server*. Pastikan pulsa untuk mengirim SMS mencukupi, serta *smartphone* dalam keadaan aktif saat digunakan.

1. Mekanisme Kerja Smsgateway.me

Daftar terlebih dahulu pada layanan smsgateway.me untuk mendapatkan *username* dan *password. Instal* aplikasi smsgateway.me pada *smartphone* android yang ingin digunakan sebagai SMS *server*. Setelah aplikasi ter*instal*, *login* ke aplikasi smsgateway.me pada android dengan *username* dan *password* yang sama pada saat mendaftar pada versi *web.*

Dengan *login* ke dalam aplikasi android, pengguna akan mendaftarkan dan mendapatkan informasi baru berupa *device ID* dan API *token*. *Device ID* dan API *token* ini digunakan untuk autentikasi bersamaan dengan *email* dan *password* pada saat mengirim dan menerima SMS pada sistem.

2. Konsep Smsgateway.me terhadap Sistem Layanan SMS Desa

Konsep aplikasi smsgateway.me pada dasarnya menggunakan API dari SMS *Gateway* sehingga lebih praktis tanpa menggunakan perangkat tambahan seperti modem. *Smartphone* android sebagai *server* SMS. Fitur SMS yang digunakan pada sistem Layanan SMS Desa ini adalah SMS *personal* dan *broadcast*.

2.2.4 Kriptografi

Keamanan data merupakan suatu hal yang sangat penting dan harus diperhatikan ketika melakukan pengiriman data dari satu pihak ke pihak lainnya (Yusfrizal, 2015). Berbagai aspek dalam keamanan informasi seperti kerahasiaan data, integritas, autentikasi dan *non*-repundansi merupakan pusat dari kriptografi modern (Laurentinus, 2017).

Kriptografi merupakan ilmu dan seni yang berfungsi untuk menjaga kerahasiaan pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat

dimengerti lagi maknanya. Dalam ilmu kriptografi terdapat dua proses, yaitu enkripsi dan dekripsi (Prabokory, *et al*., 2015). Enkripsi yaitu mengubah bentuk pesan asli (*plain text*) menjadi pesan yang sulit dibaca (*chiper text*). Sebaliknya, dekripsi yaitu mengembalikan bentuk pesan yang sulit dibaca (*chiper text*) ke bentuk pesan asli (*plain text*) (Fachry, 2018).

Menurut Rahardjo (2003), terdapat empat elemen utama di dalam proses kriptografi yang saling berkaitan satu sama lain, diantaranya:

1. *Plain Text*

   Plain text merupakan sebagai pesan awal atau pesan asli yang nantinya akan dilakukan enkripsi dan dekripsi.

2. *Cipher Text*

   Cipher text merupakan pesan yang sudah dienkripsi pada proses kriptografi. *Cipher text* ini dapat diubak ke bentuk aslinya (*plain text*) dengan memanfaatkan *key* yang telah disediakan. Proses tersebut merupakan proses dekripsi.

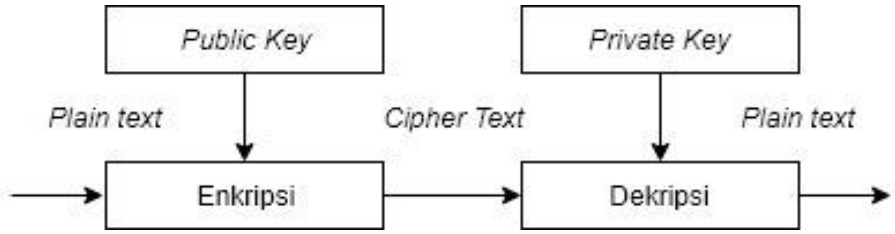
3. *Cryptography Key*

   Cryptography key merupakan kunci yang digunakan untuk melakukan enkripsi dan dekripsi pada proses kriptografi. Proses enkripsi dan dekripsi menggunakan satu kunci yang sama.

4. *Encryption Decryption Algorithm*

   Encryption Decryption Algorithm adalah komponen terakhir terpenting dalam proses kriptografi yaitu algoritma yang digunakan untuk proses enkripsi dan

dekripsi. Gambar 2.4 menunjukkan tahapan dari sistem kriptografi kunci-publik.



Gambar 2.4 Sistem Kriptografi Kunci-Publik

Kriptografi menjadi teknik alternatif untuk memungkinkan dua orang saling bertukar pesan dengan mengubah pesan ke bentuk sandi sehingga pesan tersebut tidak dapat disalahgunakan oleh pihak yang tidak bertanggung jawab (Muharram, 2018). Dalam kriptografi terdapat dua teknik enkripsi yaitu *asimetris* dan *simetris*. Algoritma kunci *asimetris* yaitu suatu enkripsi dengan menggunakan kunci yang berbeda dalam melakukan proses ekripsi dan dekripsi. Sedangkan kunci *simetris* yaitu suatu enkripsi menggunakan kunci yang sama baik dalam proses enkripsi maupun dekripsi (Satriawan, 2014). Dalam melakukan enkripsi SMS hanya membutuhkan satu kunci sehingga digunakanlah algoritma kriptografi *simetris*. Terdapat beberapa algoritma kriptografi *simetris*, diantaranya *Data Encryption Standard* (DES), *blowfish*, *Rivest Chiper* 4 (RC4), *Rivest Chiper* 5 (RC5), *twofish*, dan yang terbaru adalah algoritma AES.

2.2.5 Algoritma *Advanced Encryption Standard* (AES)

Menurut Munir (2006) algoritma AES merupakan pengganti dari algoritma DES pada tahun 2000. Algoritma ini sebelumnya bernama Rijndael yang berasal dari nama penemunya, kemudian pada tahun 2001 algoritma ini ditetapkan menjadi AES oleh *National Institute of Standard and Technology* (NIST). Algoritma AES

menjadi acuan yang dipakai sebagai *standard* algoritma kriptografi pada masa sekarang (Qurniawan, 2012).

Menurut Primartha (2013) algoritma AES bersifat *simetris* dan *cipher* blok. Algoritma AES menggunakan substitusi, permutasi, dan sejumlah putaran yang dikenakan pada tiap blok yang akan dienkripsi atau didekripsi. Untuk setiap putarannya, algoritma AES menggunakan kunci yang berbeda. Kunci pada setiap putaran disebut *round key*. Ukuran blok untuk algoritma AES adalah 128 *bit* (Qurniawan, 2012). Algoritma AES mempunyai kunci 128-*bit*, 192-*bit*, dan 256-*bit*, atau dikenal juga AES-128, AES-192, dan AES-256. Tabel 2.1 menunjukkan versi kunci algoritma AES.

Tabel 2.1 Versi AES (Munir, 2006)

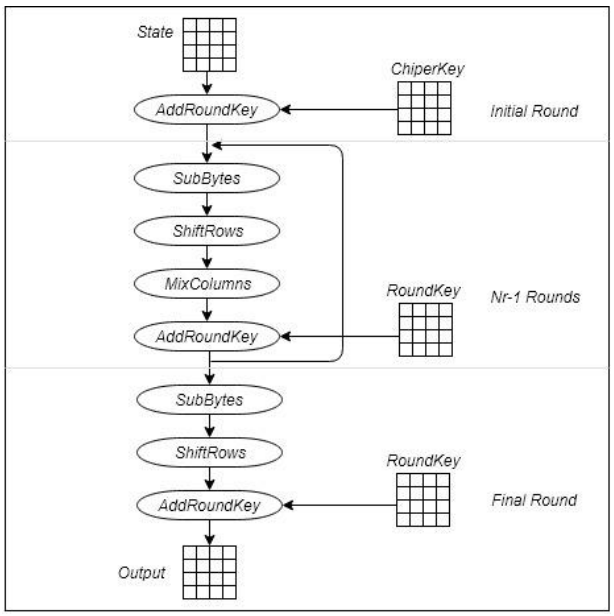
	Panjang Kunci (Nk *words*)	**Ukuran Blok (Nb *words*)**	**Jumlah Putaran (Nr)**
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Catatan: 1 *word* = 32 *bit*

2.2.5.1 Proses Enkripsi

Proses enkripsi terdiri dari 4 jenis transformasi *byte*s, yaitu *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*. *AddRoundKey* yaitu melakukan XOR antara *plain text* dengan *chiper key*. *SubBytes* atau substitusi *bytes* merupakan transformasi *byte* pada *state* dengan menggunakan tabel substitusi (*S-Box*). *ShiftRows* merupakan pergeseran *byte* pada tiap-tiap *array state*. *MixColumns* merupakan pengacakan data dari masing-masing *array state* (Ibrahim, 2017).

Awal proses enkripsi, *state* akan mengalami transformasi *byte AddRoundKey*, kemudian *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang sebanyak Nr. Proses ini disebut juga sebagai *Round Function*. Pada *Round* terakhir, proses berbeda dari sebelumnya dimana *state* tidak mengalami transformasi *MixColumns* (Wijaya, 2015). Gambar 2.5 menunjukkan tahapan proses enkripsi algoritma AES.



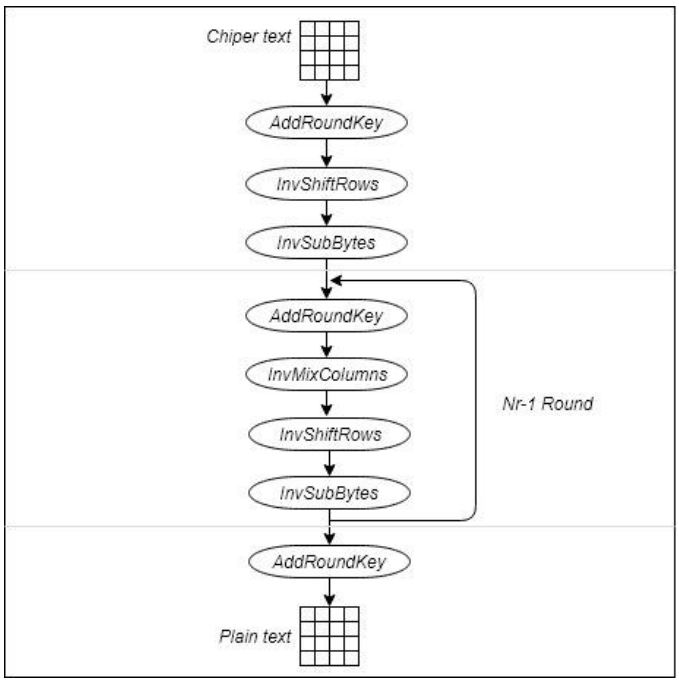
Gambar 2.5 Diagram Proses Enkripsi Algoritma AES (Munir, 2006)

2.2.5.2 Proses Dekripsi

Proses dekripsi berlawanan dengan proses enkripsi. Transformasi *bytes* yang digunakan dalam proses dekripsi yaitu *AddRoundKey*, *InvShiftRows*, *InvSubBytes*, dan *InvMixColumns*.

Pada proses dekripsi, untuk iterasi pertama dilakukan transformasi *AddRoundKey*, *Inverse ShiftRows*, dan *Inverse SubBytes*. *Chiper text* akan melakukan transformasi *AddRoundKey*. Transformasi *AddRoundKey* pada proses dekripsi tidak berbeda dengan transformasi *AddRoundKey* pada proses enkripsi

karena pada transformasi ini juga menggunakan operasi XOR antara *chiper text* dengan *subkey*. Setelah *AddRoundKey*, kemudian dilakukan *Inverse ShiftRows* dimana transformasi *byte* berlawanan dengan transformasi *ShiftRows* pada proses enkripsi. Pada proses transformasi *Inverse ShiftRows*, dilakukan pergeseran *bit* ke kanan sedangkan pada *ShiftRows* dilakukan pergeseran *bit* ke kiri. Pada baris kedua pergeseran *bit* dilakukan sebanyak tiga kali, pada baris ke tiga dilakukan pergeseran *bit* sebanyak dua kali dan pada baris ke empat dilakukan pergeseran *bit* satu kali. Proses selanjutnya yaitu *Inverse SubBytes*. Transformasi *Inverse SubBytes* berlawanan dengan transformasi *SubBytes*. Pada *Inverse SubBytes* tranformasi *byte* pada *state* dengan menggunakan tabel *Inverse*e *S-Box*. Kemudian pada iterasi dua sampai Nr-1 putaran, *state* akan mengalami proses *AddRoundKey*, *Inverse MixColumns*, *Inverse ShiftRows*, dan *Inverse SubBytes* (Ibrahim, 2017). Gambar 2.6 menunjukkan tahapan proses dekripsi algoritma AES.



Gambar 2.6 Diagram Proses Dekripsi Algoritma AES (Ibrahim, 2017)

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi dan analisis algoritma AES pada sistem Layanan SMS Desa yang telah dilakukan, maka dapat disimpulkan sebagai berikut:

1. Penerapan algoritma AES dapat memberikan keamanan terhadap data SMS pada sistem Layanan SMS Desa. Sistem dibuat menggunakan *framework* Laravel dan untuk implementasi SMS *Gateway* menggunakan API. Penggunaan API SMS *Gateway* lebih efisien karena tidak perlu menggunakan perangkat tambahan seperti modem. API SMS *Gateway* menggunakan *smartphone* android sebagai *server* SMS. Keamanan data SMS menggunakan enkripsi AES tiga variasi kunci yaitu 128-*bit*, 192-*bit*, dan 256-*bit*.
2. Dari hasil pengujian yang telah dilakukan, diperoleh hasil bahwa *chiper text* yang dihasilkan cukup aman setelah dilakukan enkripsi menggunakan algoritma AES. Sebagaimana dalam uji ketahanan terhadap serangan *brute force* 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.

5.2 Saran

Saran yang diberikan untuk pengembangan penelitian lebih lanjut adalah sebagai berikut:

1. Pada sistem ini pesan masuk belum menggunakan klasifikasi, untuk penelitian selanjutnya diharapkan sistem dapat memberikan klasifikasi SMS sehingga pengelompokan pesan lebih jelas.
2. Pada sistem yang telah dibuat, pesan aduan dari warga masuk ke server SMS pada *smartphone* android. sistem belum dapat menyimpan pesan masuk secara otomatis ke dalam sistem, sehingga admin perlu meng*input*kan pesan masuk secara manual. Untuk penelitian selanjutnya diharapkan sistem dapat menyimpan pesan secara otomatis.
3. Pada penelitian selanjutnya, harapannya sistem dapat dikembangkan ke media *online* lain seperti telegram.

DAFTAR PUSTAKA

Afridi, M. Z. (2017) *Implementation of API Technologies using SMS Gateway System Through Web Services.* Journal of Information & Communication Technology – JICT (Vol. 11, Issue. 2).

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

Alvianto, A. R., & Darmaji, D. (2015). *Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android*. Jurnal Sains dan Seni ITS, *4*(1), A1-A6.

Arief, A., & Saputra, R. (2016). *Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging.* Scientific Journal of Informatics, 3(1), 46-54.

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, 4(3), 450-453.

Azhar, R., & Kurniawan, K. (2016). *Aplikasi Keamanan SMS Menggunakan Algoritma Rijndael.* MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, 16(1), 105-112.

Fachriyah, I., & Tajidun, L. M. (2015). *Implementasi SMS Gateway Dan Papan Pengumuman Digital Penyebaran Informasi Kegiatan Akademik (Studi Kasus: Jurusan Teknik Informatika Universitas Halu Oleo).* semanTIK, 1(2).

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

Kridalaksana, A. H., Arriyanti, E., & Widodo, W. (2013). *Aplikasi Pengaman SMS dengan Metode Kriptografi Advanced Encryption Standard (AES) 128 Berbasis Android*. Sebatik, 10(1), 8-14.

Layansari, F. A., & Marisa, F. (2018). *Perancangan Sistem Pelayanan Informasi Berbasis Sms Gateway Pada Kantor Dispendukcapil Kabupaten Belu*. JIMP-Jurnal Informatika Merdeka Pasuruan, 3(2).

Laurentinus, L. (2017). *Implementas Kriptografi dan Kompresi SMS Menggunakan Algoritma RC6 dan Algoritma Huffman Berbasis Android*. Jurnal Informatika Global, 8(1).

Muharram, F., Aziz, H., & Manga, A. R. (2018). *Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES).* Prosiding SAKTI (Seminar Ilmu Komputer dan Teknologi Informasi) (Vol. 3, No. 2, pp. 112-115).

Munir, R. 2006. *Kriptografi*. Bandung: Informatika Bandung.

Noviyantono, E. (2012). *Integration System Of Web Based And SMS Gateway For Information System Of Tracer Study*. International Conference on Engineering and Technology Development (ICETD).

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). *Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard.* Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, 10(1), 20-31.

Purba, I. S., & Djamin, D. (2015). *Partisipasi Masyarakat dalam Meningkatkan Good Governance di Tingkat Desa*. JPPUMA Jurnal Ilmu Pemerintahan dan Sosial Politik Universitas Medan Area, 3(1), 25-36.

Prasetya, D. R. (2013). *Analisis Pengelolaan Pengaduan Masyarakat Dalam Rangka Pelayanan Publik (Studi Pada Dinas Komunikasi dan Informatika Kota Malang).* Jurnal Administrasi Publik, 1(6), 1151-1158.

Primartha, R. (2013). *Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Advanced Encryption Standard (AES).* Journal of Research in Computer Science and Applications Informatics Engineering Department, Sriwijaya University, 1(01), 1-19.

Qurniawan, W., Wintolo, H., & Nugraheny, D. (2012). *Penerapan Sistem Keamanan dengan Kriptografi Advanced Encryption Standard (AES) dan Key Administrator pada Sinkronisasi File.* Compiler, 1(2).

Rahardjo, B. (2003). *Memahami Model Enkripsi & Security Data.* Yogyakarta: Wahana Komputer dan Andi Offset.

Satriawan, I. W. D., Sasmita, I. G. M. A., & Bayupati, I. P. A. (2014). *Aplikasi Enkripsi SMS dengan Metode RSA pada Smartphone Berbasis Android*. Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi).

Saxena, N., & Chaudhari, N. S. (2014). *SecureSMS: A secure SMS protocol for VAS and other applications*. Journal of Systems and Software, 90, 138-150.

Shahbazi, K., M. Eshghi, & R.F. Mirzaee. (2017). *Design and Implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5*. Engineering Science and Technology, an International Journal, (20): 1308-1317.

Stone, Nugros. (2017). *Penjelasan Lengkap Tentang SMS Gateway*. https://www.istanakecilku.com/penjelasan-lengkap-tentang-sms-gateway/. Diakses pada tanggal 4 Juli 2018 pukul 21.27.

Wahana. (2015). *Mudah Membuat Aplikasi SMS Gateway dengan CodeIgniter*. Yogyakarta: Wahana Komputer.

Wardani, A. S. (2018). *Hacker Bobol 26 Juta SMS*. https://www.liputan6.com/tekno/read/3694968/hacker-bobol-26-juta-sms. Diakses pada tanggal 1 Maret 2020 pukul 19.00.

Sugiyanto, & Hapsari. R. K. (2016). *Pengembangan Algoritma Advanced Encrytion Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere*. Ultimatics, Vol. VIII, No. 2: 2085-4552.

Sulaiman, R., & Vebu, M. (2018). *Peningkatan Keamanan Pesan Berbasis Android Menggunakan Algoritma Kriptografi RSA*. Jurnal Sisfokom (Sistem Informasi dan Komputer), 7(2), 116-120.

Susanto, S. (2018). *Keamanan SMS Gateway Nilai SMK Negeri Tugumulyo Menggunakan Algoritma RSA*. Techno. Com, 17(1), 80-90.

Sutanto, L., Budhi, G. S., & Santoso, L. W. (2014). *Perbandingan Aplikasi Menggunakan Metode Camellia 128 Bit Key Dan 256 Bit Key*. Jurnal Informatika, 12(2), 109-116.

Tampubolon, N. B., Isnanto, R. R., & Sinuraya, E. W. (2016). *Implementasi dan Analisis Algoritma Advanced Encryption Standard (AES) pada Tiga Variasi Panjang Kunci Untuk Berkas Multimedia*. TRANSIENT, 4(4), 1008-10112.

Wijaya, A., Purwanto, Y., & Nasution, S. M. (2015). *Sistem Enkripsi Menggunakan Algoritma AES-128 pada Prototype Community Messenger Berbasis Android*. eProceedings of Engineering, 2(2).

Winarni, A. (2018). *Sistem Informasi Pengajuan Cuti Berbasis Website dan Penerapan SMS Gateway Notification PT. Bank Negara Indonesia (PERSERO) Tbk Kantor Cabang Tanjung Pinang*. Jurnal Bangkit Indonesia, 7(1), 113-113.

Yulianto, E. (2018). *Implementation of Short Message Service Gateway Application Programming Interface on Communication Media Design of Rukun Tetangga-Rukun Warga*. Infosecure, 1(1).

Yusfrizal. (2015). *Penerapan RC6 Untuk Perancangan Aplikasi Pengamanan SMS pada Mobile Device Berbasis Android*. Seminar Nasional Informatika 2015.