e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

# Android-Based Text Message Encryption and Decryption Application Using the Advanced Encryption Standard Algorithm

# Aplikasi Enkripsi Dan Dekripsi Pesan Teks Berbasis Android Menggunakan Algoritma Advanced Encryption Standard

**Riski Adi Putra [1)], Yupianti [2)], Eko Prasetyo R [3)]**
[1,2,3)] ***Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu***
**Email: [1)]**

*How to Cite :*
Putra, R. A.,Yupianti., Prasetyo R. E. (2023). Android-Based Text Message Encryption and Decryption Application Using the Advanced Encryption Standard Algorithm. Jurnal Media Computer Science, 2(1).

ARTICLE HISTORY
*Received [02 Desember 2022]*
*Revised [28 Desember 2022]*
*Accepted [06 Januari 2023]*

***KEYWORDS***
*Application, Encryption and Decryption, Text Messaging, Based on Android, Advanced Encryption Standard Algorithm*



## ABSTRAK

SMA Negeri 2 Kaur merupakan salah satu Sekolah Menengah Atas Negeri yang terdapat di Kabupaten Kaur Provinsi Bengkulu. Komunikasi antar guru atau guru dengan siswa atau siswa dengan siswa selama ini dilakukan melalui aplikasi pesan teks yang telah tersedia di smartphone pengguna sehingga saling bertukar informasi. Namun informasi yang dikirim tersebut belum sepenuhnya diterapkan keamanan, dimana pesan yang dikirim adalah pesan asli, dan langsung terbaca penerima pesan asli tersebut. Hal ini tentunya mempermudah pihak-pihak tertentu yang berniat untuk mendapatkan pesan tersebut. Aplikasi enkripsi dan dekripsi pesan teks berbasis android menggunakan algoritma Advanced Encrytion Standard dibuat untuk membantu menjaga keamanan berkomunikasi antara pengirim dan penerima sehingga terjaga kerahasiaannya. Aplikasi ini dibuat menggunakan android studio dan sudah dipasang web service JSON, sehingga dapat diakses oleh perangkat smartphone android dengan internet. Pesan yang telah dikirim akan tersimpan ke dalam database MySQL dalam bentuk record yang telah diacak, sehingga perlu dilakukan penyandian untuk mengetahui apa isi pesan tersebut, dimana Algoritma Advanced Encryption Standard merupakan kriptografi yang menggunakan kunci simetris (kunci enkripsi dan dekripsi harus sama). Berdasarkan hasil pengujian yang telah dilakukan, fungsional dari aplikasi enkripsi dan dekripsi pesan teks berbasis android di SMA Negeri 2 Kaur berjalan dengan baik sesuai yang diharapkan dan pesan yang dikirim antara penerima dan pengirim terjaga kerahasiaan keamanan pesan tersebut karena sudah teracak.

## *ABSTRACT*

*Kaur 2 Public High School is one of the State Senior High Schools in Kaur District, Bengkulu Province. Communication between teachers or teachers and students or students and students has so far been carried out through text message applications that are already available on users' smartphones so that they exchange information. However, the information sent has not been fully implemented by security, where the message sent is the original message, and the recipient of the original message can read it immediately. This of course makes it easier for certain parties who intend to get the message. An android-based text message encryption and decryption application using the Advanced Encrytion Standard algorithm was created to help maintain security of communication between senders and recipients so that confidentiality is*

*maintained. This application was created using Android Studio and has installed the JSON web service, so that it can be accessed by Android smartphone devices with the internet. Messages that have been sent will be stored in the MySQL database in the form of scrambled records, so it is necessary to do encryption to find out what the contents of the message are, where the Advanced Encryption Standard Algorithm is cryptography that uses symmetric keys (encryption and decryption keys must be the same). Based on the results of the tests that have been carried out, the functionality of the android-based text message encryption and decryption application at SMA Negeri 2 Kaur runs well as expected and the message sent between the recipient and the sender is kept confidential because the message is encrypted.*

## PENDAHULUAN

Perkembangan teknologi informasi khususnya pada bidang komunikasi antar manusia sudah sangat mudah dilakukan melalui telepon genggam dan fiturnya sangat bervariasi. Komunikasi merupakan salah satu kegiatan dasar dalam kehidupan manusia yang memungkinkan manusia saling dapat bertukar informasi. Pertukaran informasi jarak jauh ini menuntut keamanan terhadap kerahasiaan informasi yang dipertukarkan.

Salah satu media komunikasi yang umum sering digunakan adalah SMS (Short Message Service). SMS dapat membantu pengguna untuk mengirim pesan dan menerima pesan masuk yang berupa teks sehingga lebih fleksibel dan pada sistem komunikasinya nirkabel. Dikarenakan kemudahan komunikasi tersebut, bukan berarti tidak terdapat celah keamanan bagi yang berniat untuk mendapatkan informasi. Hal ini tentunya dapat dihindari dengan merahasiakan informasi yang hanya dapat dimengerti oleh orang yang berwenang.

Kriptografi sudah banyak digunakan oleh banyak bidang khususnya bidang informatika, seperti membuat penyandian data teks password yang digunakan pengguna untuk login ke sistem berbasis digital agar tidak dapat dimengerti oleh orang yang tidak berkepentingan. Kriptografi sendiri memiliki 2 konsep yakni enkripsi dan dekripsi, dimana enkripsi mengubah informasi asli menjadi informasi yang tidak dapat dikenali, sedangkan dekripsi kebalikannya mengubah informasi yang tidak dapat dikenali menjadi informasi asli sehingga dapat dibaca oleh penerima pesan tersebut.

SMA Negeri 2 Kaur merupakan salah satu Sekolah Menengah Atas Negeri yang terdapat di Kabupaten Kaur Provinsi Bengkulu. Komunikasi antar guru atau guru dengan siswa atau siswa dengan siswa selama ini dilakukan melalui aplikasi pesan teks yang telah tersedia di smartphone pengguna sehingga saling bertukar informasi. Namun informasi yang dikirim tersebut belum sepenuhnya diterapkan keamanan, dimana pesan yang dikirim adalah pesan asli, dan langsung terbaca penerima pesan asli tersebut. Hal ini tentunya mempermudah pihak-pihak tertentu yang berniat untuk mendapatkan pesan tersebut.

Oleh karena itu, diperlukan suatu keamanan terhadap informasi tersebut sebelum informasi dikirim ke penerima. Dalam penelitian ini, dibangun aplikasi pesan teks yang dapat mengamankan informasi tersebut melalui salah satu algoritma kriptografi yaitu Advanced Encyption Standard. Selain itu, aplikasi pesan teks menyimpan data guru dan siswa sehingga mempermudah memilih penerima pesan teks tersebut.

## LANDASAN TEORI

### Kriptografi

Pada umumnya kriptografi (cryptography) merupakan ilmu dan seni untuk menjaga pesan agar aman. “Cryptography is the art and science of keeping messages secure”. “Crypto” berarti

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

"secret" (rahasia) dan "graphy" berarti "writing" (tulisan). Para pelaku atau praktisi kriptografi disebut Cryptographers. Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher dan merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi (Rudiyanto & Amini, 2018).

Kriptografi merupakan seni dan ilmu dalam menciptakan sebuah sistem kripto yang mampu menyediakan keamanan informasi. Kriptografi berkaitan erat dengan pengamanan data digital. Ilmu ini terdiri dari mekanisme-mekanisme perancangan yang didasarkan pada algoritma-algoritma matematik yang menawarkan sejumlah layanan keamanan informasi fundamental (Siahaan & Sianipar, 2019)

Kriptografi adalah bidang ilmu yang mempelajari tentang cara untuk menjaga keamanan pesan dalam proses pengiriman dengan menggunakan metode penyandian tertentu, dengan tujuan agar informasi dalam pesan tersebut tidak disalahgunakan oleh orang yang bukan penerima aslinya. Kriptografi memiliki beragam metode untuk menyandikan pesan atau informasi yang ingin kita sembunyikan, seperti Caesar Cipher, Affine, Monoalphabetic, Polyalphabetic, Vigenere, Transposisi, dan banyak lagi metode-metode dalam kriptografi ini (Permana, 2018).

## Algoritma Advanced Encryption Standard

Algoritma AES adalah algoritma kritografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Awal proses enkripsi, input yang telah disalin ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut dengan round function. Round terakhir agak berbeda dengan round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns (Handoyo & Subakti, 2020).

## Android

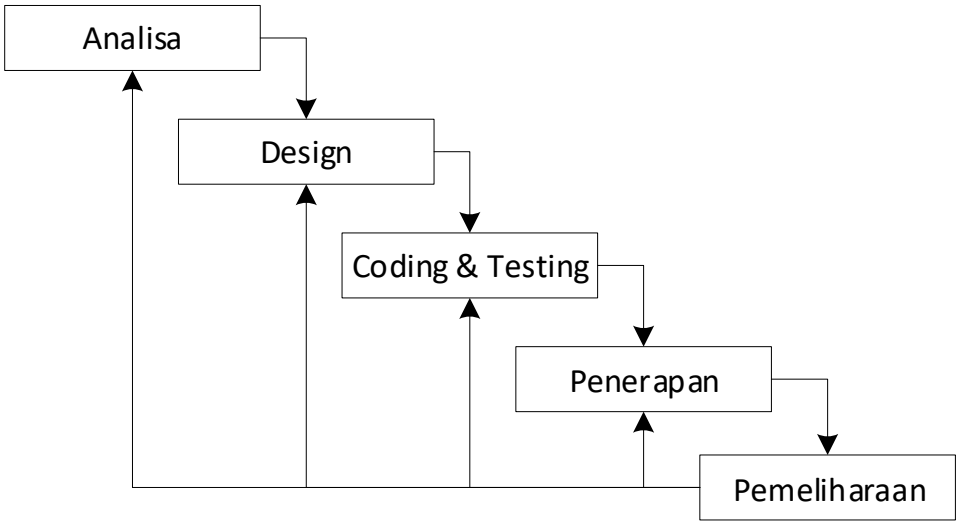
Android adalah sistem operasi (Operating System) yang umumnya digunakan pada perangkat dengan navigasi full touch screen yang biasa dimiliki oleh smartphone dan komputer tablet. Android sudah diambil alih oleh perusahaan Google Inc yang telah membelinya pada tahun 2005 dari Android Inc. Google menyediakan software/tools yang dikembangkan khusus untuk dijadikan alat pengembang aplikasi android yang diberi nama "Android Studio". Android Studio dikembangkan dengan menggunakan bahasa Java dengan menambahkan library-library khusus yang diperuntukan untuk membuat aplikasi android. Android studio menggunakan metode native code yang memisahkan antara view dan controll (Permana, 2018).

Android adalah sistem operasi berfungsi untuk perangkat mobile berbasis linux. Android juga menyediakan berbagai macam platform terbuka bagi para developer dalam membuat aplikasi sederhana. Pada awalnya, Google Inc. membeli Android Inc. yang merupakan pendatang baru dalam piranti smartphone. Untuk mengembangkan android, maka saat itu dibentuklah sebuah organisasi yang sekitar 34 perusahaan piranti keras, perangkat lunak maupun telekomunikasi, didalamnya termasuk Google, HTC, Intel, Motorola, Qualcomm, TMobile dan Nvidia. Android dirilis pertama kalinya pada tanggal 05 November 2007, yang dikenal sebagai android bersama Open Handset Alliance yang mengesahkan android dikembangkan sebagai open source pada perangkat mobile. Kemudian pada sekitar September 2007, Google kembali mengenalkan Nexus One, sebagai salah satu jenis smartphone yang menggunakan android sebagai sistem operasinya. Telepon seluler dibuat dan dikembangkan oleh HTC Corporation. Kemudian pada tanggal 09 Desember 2008, telah diumumkan anggota baru yang bergabung dalam sebuah perusahaan untuk menciptakan versi-versi baru android. Dengan seiring pembentukan OHA (Open Handset Alliance), OHA mengumumkan produk perdana android mereka yang merupakan hasil modifikasi dari kernel Linux 2.6. Sejak android dirilis, maka dari itu juga banyak pembaharuan dan penambahan fitur-fitur yang

mendukung berjalannya android tersebut, sehingga android dapat berjalan dengan sempurna dan tidak memiliki kekurangan apapun itu (Fachri & Sembiring, 2020).

## METODE PENELITIAN

Metode penelitian yang diterapkan pada penelitian ini adalah dengan pengembangan metode waterfall. Metode Waterfall memiliki tahapan-tahapan terlihat pada Gambar 1.




Gambar 1. Tahapan Metode *Waterfall*

1. Analisa
   Pada tahap ini akan dilakukan analisis terhadap algoritma kriptografi dalam mengamankan teks.
2. Design
   Pada tahap ini akan dilakukan perancangan sistem berdasarkan hasil analisis. Tahap ini akan menggambarkan rancangan proses penerapan algoritma kriptografi dalam mengamankan data.
3. *Coding* dan *Testing*
   Pada tahap ini akan dilakukan proses pembuatan aplikasi serta uji coba aplikasi, dimana pada aplikasi tersebut sudah diintegrasikan algoritma kriptografi untuk proses enkripsi dan dekripsi.
4. Penerapan
   Pada tahap ini akan dilakukan penerapan dari aplikasi yang telah dibuat dengan menguji coba aplikasi.
5. Pemeliharaan
   Pada tahap ini akan dilakukan pemeliharaan secara berkala dari aplikasi, jika suatu saat terjadinya eror.

## HASIL DAN PEMBAHASAN

Pengujian aplikasi enkripsi dan dekripsi pesan teks berbasis android di SMA Negeri 2 Kaur dilakukan menggunakan Metode Black Box dengan mengidentifikasi fungsionalitas dari aplikasi melalui data yang benar dan data yang salah. Adapun hasil pengujian black box yang telah dilakukan, tampak pada tabel 1.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Tabel 1. Hasil Pengujian Blackbox

| No | Skenario Pengujian | Hasil Pengujian | Keterangan |
|---|---|---|---|
| 1. | Mengosongkan semua isian data pada form login, lalu klik tombol login | Sistem menolak akses login tersebut dan menampilkan pesan kesalahan | Sesuai Harapan |
| 2 | Mengosongkan isian data password pada form login, lalu klik tombol login | Sistem menolak akses login tersebut dan menampilkan pesan kesalahan | Sesuai Harapan |
| 3 | Mengosongkan isian data username pada form login, lalu klik tombol login | Sistem menolak akses login tersebut dan menampilkan pesan kesalahan | Sesuai Harapan |
| 4. | Memasukkan isian data pada form login yang benar, lalu klik tombol login. | Sistem menerima akses login tersebut dan menampilkan pesan berhasil | Sesuai Harapan |
| 5 | Menulis pesan dengan memilih penerima pesan | Sistem berhasil mengirim pesan ke penerima pesan yang telah dipilih | Sesuai Harapan |
| 6. | Melihat pesan pada kotak masuk | Sistem berhasil menampilkan isi pesan pada kotak masuk | Sesuai Harapan |

Berdasarkan hasil pengujian yang telah dilakukan, fungsional dari aplikasi enkripsi dan dekripsi pesan teks berbasis android di SMA Negeri 2 Kaur berjalan dengan baik sesuai yang diharapkan dan pesan yang dikirim antara penerima dan pengirim terjaga kerahasiaan keamanan pesan tersebut karena sudah teracak.

## KESIMPULAN DAN SARAN

### Kesimpulan

1. Aplikasi enkripsi dan dekripsi pesan teks berbasis android menggunakan algoritma Advanced Encrytion Standard dibuat untuk membantu menjaga keamanan berkomunikasi antara pengirim dan penerima sehingga terjaga kerahasiaannya.
2. Aplikasi ini dibuat menggunakan android studio dan sudah dipasang web service JSON, sehingga dapat diakses oleh perangkat smartphone android dengan internet.
3. Pesan yang telah dikirim akan tersimpan ke dalam database MySQL dalam bentuk record yang telah diacak, sehingga perlu dilakukan penyandian untuk mengetahui apa isi pesan tersebut, dimana Algoritma Advanced Encryption Standard merupakan kriptografi yang menggunakan kunci simetris (kunci enkripsi dan dekripsi harus sama).
4. Berdasarkan hasil pengujian yang telah dilakukan, fungsional dari aplikasi enkripsi dan dekripsi pesan teks berbasis android di SMA Negeri 2 Kaur berjalan dengan baik sesuai yang diharapkan dan pesan yang dikirim antara penerima dan pengirim terjaga kerahasiaan keamanan pesan tersebut karena sudah teracak.

### Saran

Berdasarkan penelitian yang penulis lakukan, maka penulis menyarankan agar dapat menggunakan aplikasi ini untuk dijadikan alternatif dalam bertukar informasi antara kedua belah pihak, khususnya disekolah

## DAFTAR PUSTAKA

Andriyani, S., 2016. Aplikasi Akademik Online Berbasis Mobile Android Pada Universitas Tama Jagakarsa. Jurnal Sains dan Teknologi Utama , Volume Vol.XI No.1 ISSN :1978-001X.

Budiarto, E., 2017. Pembuatan Aplikasi Web Berbasis SMS Sebagai Media Penyalur Informasi dan Komunikasi Antara Sekolah Dengan Orang Tua Siswa. Junal Ilmiah Pendidikan Teknik Kejuruan (JIPTEK) Vol.X No.1 Januari 2017.

Enterprise, J., 2019. PHP Untuk Programmer Pemula. Jakarta: PT. Elex Media Komputindo.

Fachri, B. & Sembiring, R. M., 2020. Pengamanan Data Teks Menggunakan Algoritma DES Berbasis Android. Jurnal Media Informatika Budidarma, Volume Vol.4 No.1 e-ISSN:2548-8368.

Firman, A., 2019. Analisis dan Perancangan Sistem Informasi. Surabaya: Penerbit Qiara Media.

Handoyo, J. & Subakti, Y. M., 2020. Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (AES). Jurnal Sistem Informasi dan Teknologi, Volume Vol.3 No.2 e-ISSN:2622-2973.

Indrajani., 2017. Database Design Theory, Practice, and Case Study. Jakarta: PT. Elex Media Komputindo.

Irawan, C. & Winarno, A., 2020. Kombinasi Algoritma Kriptografi AES dan DES Untuk Enkripsi File Dokumen Proposal. Semarang, Proceeding Sendiu ISBN:978-979-3649-72-6.

Lasminiasih, 2016. Perancangan Sistem Informasi Kredit Mikro Mahasiswa Berbasis Web. Jurnal Sistem Informasi (JSI) Vol.8 No.1 April 2016 ISSN : 2085-1588.

Pamungkas, C. A., 2017. Pengantar dan Implementasi Basis Data. Yogyakarta: Penerbit Deepublish.

Permana, A. A., 2018. Penerapan Kriptografi Pada Teks Pesan Dengan Menggunakan Metode Vigenere Cipher Berbasis Android. Jurnal Al-Azhar Indonesia Seri Sains dan Teknologi, Volume Vol.4 No.3.

Rachmawati, A., 2017. Desain Aplikasi Mobile Informasi Pemetaan Jalur Batik Solo Trans Berbasis Android Menggunakan Location Based Service. Jurnal Geodesi Undip , Volume Vol.6 No.2 ISSN : 2337-845X.

Rudiyanto & Amini, S., 2018. Implementasi Kriptografi Untuk Pengamanan Pesan Teks Pada Aplikasi Chatting Berbasis Android Dengan Metode Vigenere Cipher Pada SMK Negeri 7 Kota Tangerang. Skanika, Volume Vol.1 No.2.

Santoso & Nurmalina, R., 2017. Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). Jurnal Integrasi, Volume Vol.9 No.1 April 2017 e-ISSN : 2548-9828.

Sari, I. Y. et al., 2020. Keamanan Data dan Informasi. Medan: Yayasan Kita Menulis.

Siahaan, V. & Sianipar, R. H., 2019. Database Dan Kriptografi Menggunakan Java/MySQL. Yogyakarta: Sparta Publishing.

Suprapto, U., 2021. Pemodelan Perangkat Lunak (C3) Kompentesi Keahlian : Rekayasa Perangkat Lunak Untuk SMK/MAK Kelas XI. Jakarta: Grasindo.

.