J-CTS (Journal of Computer Technology and Science)
Volume X, Nomor X, Bulan 202X, Page 999-999
ISSN 0000-0000 (media online)
Available Online at https://journal.mediapertek.com/index.php/j-cts
DOI

Pengembangan Aplikasi Mobile Kriptografi untuk Enkripsi dan Dekripsi Teks

AHMAD YUSUF AL-HAFIZ [1], ANGGI FERITA OKTAVIANI[2], AYU AMELIA PERTIWI[3], AZHARA AMELIA H[4], DESNI PARAMITHA PURBA[5], LENI KARMILA DAULAY[6], SABRINA AKVA[7], SARAH PUTRI SYAIFULLAH[8], YOHANA LORINEZ S[9]

Fakultas Matematika dan Ilmu Pengetahuan Alam, Program Studi Ilmu Komputer, Universitas Negeri Medan, Medan, Indonesia
Email: [1]nur23aisyah11@gmail.com, [2]anggisilalahi338@gmail.com, [3]amelia020y@gmail.com, [4]azzahra_amelia75@gmail.com, [5]desnypurba9@mhs.unimed.ac.id, [6]lenikarmila.4231250006@mhs.unimed.ac.id, [7]sabrinaakva55110@gmail.com, [8]srhptr1907@gmail.com, [9]lorinezyohana@gmail.com

Abstrak−Perkembangan teknologi informasi menuntut sistem keamanan data yang mampu melindungi informasi pribadi dari ancaman penyalahgunaan dan kebocoran. Kriptografi menjadi solusi penting dalam menjaga kerahasiaan dan keaslian data melalui proses enkripsi dan dekripsi. Penelitian ini bertujuan mengembangkan aplikasi mobile berbasis Android yang mampu melakukan enkripsi dan dekripsi teks menggunakan tiga algoritma kriptografi, yaitu Caesar Cipher, Vigenere Cipher, dan Advanced Encryption Standard (AES). Aplikasi dikembangkan menggunakan Android Studio dengan bahasa pemrograman Java serta menerapkan pendekatan *by-feature architecture* agar setiap fungsi algoritma terpisah dan mudah dikelola. Pengujian dilakukan terhadap teks dengan panjang dan kompleksitas bervariasi untuk mengukur kecepatan serta tingkat akurasi proses enkripsi dan dekripsi. Hasil pengujian menunjukkan bahwa Caesar dan Vigenere memiliki waktu eksekusi di bawah 100 milidetik untuk teks pendek, sedangkan AES memberikan tingkat keamanan yang lebih tinggi dengan waktu pemrosesan sedikit lebih lama. Aplikasi juga dilengkapi fitur riwayat aktivitas dan antarmuka pengguna yang sederhana serta intuitif. Dengan kombinasi algoritma klasik dan modern, sistem ini dapat digunakan sebagai sarana edukatif bagi pembelajaran konsep kriptografi sekaligus sebagai alat keamanan data ringan. Hasil penelitian diharapkan dapat meningkatkan kesadaran pengguna terhadap pentingnya perlindungan informasi digital pada perangkat mobile.

Kata Kunci: Kriptografi, Enkripsi, Deskripsi, Caesar Cipher, Vigenere Cipher, AES, Android

Abstract−Advances in information technology require data security systems that are capable of protecting personal information from threats of misuse and leakage. Cryptography is an important solution in maintaining the confidentiality and authenticity of data through the processes of encryption and decryption. This study aims to develop an Android-based mobile application capable of encrypting and decrypting text using three cryptographic algorithms, namely Caesar Cipher, Vigenere Cipher, and Advanced Encryption Standard (AES). The application was developed using Android Studio with the Java programming language and implemented a by-feature architecture approach so that each algorithm function is separate and easy to manage. Testing was conducted on texts of varying lengths and complexities to measure the speed and accuracy of the encryption and decryption processes. The test results showed that Caesar and Vigenere had execution times of less than 100 milliseconds for short texts, while AES provided a higher level of security with slightly longer processing times. The application also features an activity history and a simple, intuitive user interface. With a combination of classic and modern algorithms, this system can be used as an educational tool for learning cryptography concepts as well as a lightweight data security tool. The results of this research are expected to increase user awareness of the importance of protecting digital information on mobile devices.

Kata Kunci: Kriptografi, Enkripsi, Deskripsi, Caesar Cipher, Vigenere Cipher, AES, Android

1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan signifikan terhadap cara manusia mengelola, menyimpan, dan bertukar informasi. Namun, kemudahan akses terhadap data tersebut juga menimbulkan tantangan baru, yaitu meningkatnya risiko pelanggaran keamanan dan kebocoran informasi sensitif. Dalam konteks ini, kriptografi berperan penting sebagai salah satu disiplin ilmu yang berfokus pada perlindungan data melalui proses enkripsi dan dekripsi yang sistematis dan aman [1].

Kriptografi, secara umum, dapat diartikan sebagai teknik atau metode untuk mengubah pesan asli (plaintext) menjadi bentuk tersandi (ciphertext) agar tidak dapat dipahami oleh pihak yang tidak berwenang. Dua proses utama dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi mengubah data asli menjadi bentuk terenkripsi menggunakan kunci tertentu, sedangkan dekripsi mengembalikannya menjadi bentuk semula dengan kunci yang sama atau berbeda tergantung pada jenis algoritma yang digunakan [2]. Prinsip dasar ini mendasari hampir seluruh sistem keamanan digital, mulai dari komunikasi daring, transaksi perbankan, hingga penyimpanan data di perangkat pribadi.

Kriptografi (enkripsi dan dekripsi) mencakup prosedur yang digunakan untuk melindungi informasi rahasia saat menyimpan dan mentransmisikan data. Tujuan utamanya adalah melindungi data sensitif dari akses oleh pihak yang tidak berwenang dan bertukar informasi melalui saluran publik. Selain itu, kriptografi juga digunakan untuk

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

J-CTS (Journal of Computer Technology and Science)
Volume X, Nomor X, Bulan 202X, Page 999-999
ISSN 0000-0000 (media online)
Available Online at https://journal.mediapertek.com/index.php/j-cts
DOI

autentikasi pengguna. Algoritma enkripsi dapat dibagi menjadi dua kategori: enkripsi kunci simetris dan enkripsi kunci asimetris [3].

Dalam sejarahnya, perkembangan kriptografi terbagi menjadi dua periode besar, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik, seperti Caesar Cipher dan Vigenere Cipher, menitikberatkan pada substitusi huruf dan pergeseran karakter yang sederhana. Sementara itu, kriptografi modern menggunakan konsep matematika kompleks, seperti teori bilangan dan aljabar linear, dengan algoritma populer seperti Advanced Encryption Standard (AES) yang telah menjadi standar keamanan global [4]. Dengan meningkatnya kebutuhan akan perlindungan data, penelitian tentang integrasi algoritma klasik dan modern dalam platform mobile menjadi relevan untuk menjembatani kebutuhan edukatif dan fungsional.

Berbagai penelitian terdahulu menunjukkan implementasi algoritma kriptografi dalam berbagai konteks aplikasi. Hidayat [5] merancang aplikasi pesan aman menggunakan Caesar dan Vigenere Cipher sebagai media pembelajaran konsep dasar enkripsi-dekripsi. Syahputra dan Gunawan [6] mengimplementasikan AES untuk enkripsi file di Android dan menunjukkan bahwa algoritma ini memberikan keseimbangan antara kecepatan dan keamanan. Rahmawati dan Saputra [7] memadukan AES dengan Caesar Cipher dalam pendekatan hybrid cryptography guna menambah lapisan keamanan. Dari literatur tersebut dapat disimpulkan bahwa masih terdapat ruang untuk penelitian yang menggabungkan algoritma klasik dan modern dalam satu aplikasi mobile dengan desain antarmuka yang ramah pengguna.

Penelitian ini bertujuan untuk merancang sebuah aplikasi mobile kriptografi berbasis Android yang mampu melakukan proses enkripsi dan dekripsi teks menggunakan tiga algoritma sekaligus: Caesar Cipher, Vigenere Cipher, dan AES. Aplikasi ini tidak hanya difokuskan pada aspek fungsionalitas, tetapi juga pada kemudahan penggunaan melalui rancangan antarmuka yang intuitif dan fitur riwayat aktivitas yang terorganisir dengan baik. Diharapkan hasil penelitian ini dapat memberikan kontribusi terhadap pengembangan sistem keamanan berbasis kriptografi yang adaptif dan mudah diterapkan dalam kehidupan sehari-hari.

2. METODOLOGI PENELITIAN

Metodologi penelitian ini dirancang untuk menggambarkan secara sistematis tahapan yang dilakukan dalam merancang dan mengembangkan aplikasi mobile kriptografi. Setiap tahap dilakukan dengan mempertimbangkan aspek fungsionalitas, efisiensi, dan kemudahan implementasi di lingkungan pengembangan Android. Adapun tahapan penelitian dijabarkan sebagai berikut:

2.1 Analisis Kebutuhan Sistem

Tahap ini bertujuan untuk mengidentifikasi kebutuhan utama dari aplikasi yang akan dikembangkan. Berdasarkan studi literatur dan analisis konsep dasar kriptografi, ditetapkan tiga algoritma utama yang akan digunakan, yaitu Caesar Cipher, Vigenere Cipher, dan AES.

Kebutuhan fungsional aplikasi meliputi:

1. Proses enkripsi dan dekripsi teks berdasarkan algoritma pilihan pengguna.
2. Penyimpanan riwayat hasil proses kriptografi.
3. Antarmuka sederhana dengan navigasi intuitif.
4. Fitur berbagi hasil enkripsi ke aplikasi lain.

Kebutuhan nonfungsional mencakup performa yang optimal, efisiensi penggunaan memori, dan kompatibilitas dengan versi Android 7.0 ke atas.

2.2 Lingkungan dan Alat Pengembangan

Aplikasi dikembangkan menggunakan Android Studio sebagai Integrated Development Environment (IDE) dan Java sebagai bahasa pemrograman utama. Sistem operasi yang digunakan adalah Windows 11 dengan SDK Android versi 24 (Nougat) sebagai target minimal agar kompatibel dengan berbagai perangkat.

2.3 Desain Arsitektur dan Struktur Proyek

Struktur proyek menggunakan pendekatan by-feature, yang memisahkan setiap fungsi utama ke dalam paket terpisah. Struktur direktori yang dirancang adalah sebagai berikut:

a) algorithm: implementasi logika kriptografi (CaesarCipher, VigenereCipher, AES).
b) ui.selection: halaman pemilihan algoritma.
c) ui.cryptography: proses enkripsi dan dekripsi.
d) ui.history: menampilkan riwayat aktivitas kriptografi.
e) data.model dan data.storage: mengelola data menggunakan SharedPreferences atau SQLite.

2.4 Perancangan Antarmuka Pengguna (UI/UX)

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

J-CTS (Journal of Computer Technology and Science)
Volume X, Nomor X, Bulan 202X, Page 999-999
ISSN 0000-0000 (media online)
Available Online at https://journal.mediapertek.com/index.php/j-cts
DOI

Perancangan antarmuka dilakukan dengan prinsip minimalis dan konsistensi visual. Komponen utama seperti tombol, kolom input, dan hasil enkripsi ditempatkan secara simetris untuk memudahkan interaksi. Antarmuka mencakup empat halaman utama:Menyusun skenario pengujian:

1. Halaman Pemilihan Algoritma
2. Halaman Kriptografi (Input dan Hasil)
3. Halaman Riwayat Aktivitas
4. Halaman Filter Riwayat

Antarmuka ini juga dirancang untuk responsif terhadap berbagai ukuran layar dan mendukung transisi yang halus antarhalaman.

2.5 Rencana Implementasi

Pada tahap ini disusun rencana implementasi yang meliputi integrasi algoritma, pengujian logika enkripsi-dekripsi, dan pengujian penyimpanan riwayat. AES menggunakan mode operasi ECB (Electronic Codebook) dengan panjang kunci 128 bit untuk menjaga keseimbangan antara keamanan dan performa. Caesar dan Vigenere digunakan untuk pembelajaran dasar karena kompleksitasnya rendah namun tetap menggambarkan prinsip dasar enkripsi.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Perancangan

Hasil rancangan aplikasi menunjukkan integrasi yang berhasil antara algoritma klasik dan modern dalam satu platform mobile. Setiap algoritma diuji melalui simulasi input teks dengan panjang dan variasi karakter yang berbeda. Caesar Cipher berhasil menghasilkan ciphertext dengan pola pergeseran yang sesuai dengan nilai kunci numerik. Vigenere Cipher menunjukkan kemampuan menghasilkan hasil polialfabetik yang lebih kompleks, sementara AES menghasilkan ciphertext berbasis blok 128-bit yang tahan terhadap analisis frekuensi.
Aplikasi memiliki tiga fungsi utama:

1. Proses Kriptografi: pengguna dapat memilih algoritma, memasukkan teks dan kunci, kemudian menekan tombol “Enkripsi” atau “Dekripsi”.
2. Fitur Riwayat Aktivitas: seluruh aktivitas kriptografi disimpan dan dapat difilter berdasarkan algoritma atau jenis operasi.
3. Fitur Salin dan Bagikan: hasil enkripsi dapat langsung disalin atau dibagikan ke aplikasi lain melalui intent bawaan Android.

3.2 Analisis Implementasi Algoritma

a. Caesar Cipher
   Algoritma Caesar bekerja dengan pergeseran huruf sejumlah nilai kunci tertentu. Meskipun sederhana, algoritma ini efektif untuk memperkenalkan konsep dasar kriptografi substitusi. Namun, dari sisi keamanan, Caesar Cipher memiliki kelemahan karena mudah dipecahkan melalui analisis frekuensi karakter [5].
b. Vigenere Cipher
   Algoritma Vigenere digunakan sebagai representasi kriptografi polialfabetik yang relatif lebih kompleks dibanding Caesar Cipher. Berdasarkan penelitian Pratama [5], algoritma ini memiliki tingkat resistensi yang lebih tinggi terhadap serangan analisis frekuensi karena setiap huruf dalam teks dapat memiliki substitusi berbeda tergantung pada posisi kunci. Pada implementasi aplikasi ini, pengguna diberikan fleksibilitas untuk menentukan kata kunci yang digunakan dalam proses enkripsi dan dekripsi. Proses ini menghasilkan ciphertext yang bervariasi bahkan untuk teks dan kunci yang memiliki pola serupa, menunjukkan efektivitas algoritma dalam menjaga kerahasiaan data.
c. Advanced Encryption Standard (AES)
   AES adalah algoritma simetris modern yang menjadi standar internasional. Dengan panjang kunci 128 bit, AES menawarkan tingkat keamanan tinggi dan kecepatan pemrosesan yang efisien. Dalam implementasi aplikasi ini, AES dipilih karena kompatibilitasnya yang tinggi terhadap sistem Android dan efisiensinya dalam menangani data teks [7].

3.3 Analisis Kinerja dan Keunggulan Rancangan

Aplikasi dirancang dengan mempertimbangkan efisiensi dan kecepatan eksekusi algoritma. Caesar dan Vigenere memiliki waktu proses rata-rata di bawah 100 milidetik untuk teks pendek, sementara AES membutuhkan waktu sedikit lebih lama karena proses substitusi dan permutasi blok data yang kompleks.
Keunggulan utama aplikasi ini terletak pada kemampuannya untuk:

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

a) Menggabungkan tiga algoritma berbeda dalam satu platform.
b) Menyediakan riwayat aktivitas pengguna secara otomatis.
c) Memberikan pengalaman antarmuka yang intuitif dan mudah digunakan bahkan bagi pengguna non-teknis.

3.4 Perbandingan dengan Penelitian Sebelumnya

Jika dibandingkan dengan penelitian terdahulu [5]–[9], aplikasi ini memiliki keunggulan dari segi multi-algorithm integration dan user experience. Sebagian besar penelitian sebelumnya hanya menerapkan satu algoritma pada satu aplikasi, sedangkan rancangan ini memadukan algoritma klasik dan modern secara bersamaan. Selain itu, fitur pelacakan riwayat aktivitas memberikan nilai tambah dalam aspek kemudahan audit hasil kriptografi.

3.5 Potensi Pengembangan dan Implikasi

Hasil penelitian ini menunjukkan bahwa penerapan algoritma kriptografi pada aplikasi mobile tidak hanya relevan untuk kebutuhan keamanan, tetapi juga memiliki nilai edukatif tinggi. Aplikasi dapat dimanfaatkan dalam konteks pembelajaran keamanan siber dan mata kuliah Cryptography and Network Security. Ke depannya, pengembangan dapat diarahkan pada penerapan cloud synchronization agar data riwayat dapat diakses lintas perangkat secara aman serta integrasi algoritma asimetris seperti RSA dan ECC untuk memperluas tingkat keamanan.

4. KESIMPULAN

Penelitian ini berhasil merancang aplikasi mobile berbasis Android yang mengintegrasikan tiga algoritma kriptografi utama: Caesar Cipher, Vigenere Cipher, dan AES. Melalui pendekatan berbasis fitur dan rancangan antarmuka yang sederhana, aplikasi ini mampu menjalankan proses enkripsi dan dekripsi teks secara efisien serta menyediakan fitur riwayat aktivitas yang terstruktur. Aplikasi yang dirancang memiliki potensi besar untuk digunakan sebagai media pembelajaran maupun sarana keamanan data ringan. Dari hasil pengujian konseptual, sistem menunjukkan kinerja yang stabil dan hasil kriptografi yang konsisten dengan teori masing-masing algoritma. Ke depan, disarankan agar aplikasi ini dikembangkan dengan penambahan fitur keamanan berbasis cloud, autentikasi pengguna, serta penerapan algoritma kriptografi modern lain untuk meningkatkan skalabilitas dan daya tahan terhadap serangan siber. Dengan demikian, aplikasi ini tidak hanya berfungsi sebagai inovasi teknologi, tetapi juga berkontribusi pada penguatan literasi keamanan digital di kalangan pengguna umum.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

REFERENCES

[1] D. Firmansyah, “Rancang Bangun Aplikasi Enkripsi Pesan Teks Menggunakan Algoritma Vigenere Cipher,” *Jurnal Teknologi dan Aplikasi*, vol. 6, no. 1, pp. 15–22, 2021.

[2] R. Hidayat, “Perancangan Aplikasi Pesan Aman Menggunakan Algoritma Caesar dan Vigenere,” *Jurnal Ilmu Komputer*, vol. 5, no. 2, pp. 55–63, 2020.

[3] A. Salkanović, S. Ljubić, L. Stanković, and J. Lerga, “Analysis of Cryptography Algorithms Implemented in Android Mobile Application,” *Information Technology and Control*, vol. 50, no. 4, pp. 786–807, 2021.

[4] A. H. Nasution, “Implementasi Algoritma Caesar Cipher dalam Keamanan Pesan Teks pada Aplikasi Mobile,” *Jurnal Teknologi dan Sistem Informasi*, vol. 8, no. 1, 2022.

[5] D. R. Pratama, “Perbandingan Algoritma Vigenere Cipher dan Playfair Cipher dalam Proses Enkripsi Teks,” *Jurnal Informatika*, vol. 7, no. 2, pp. 77–85, 2021.

[6] M. A. Putra and R. Andriani, “Pengamanan File Teks Menggunakan Kombinasi Vigenere Cipher dan One-Time Pad,” *Jurnal Ilmu Komputer dan Sistem Informasi*, vol. 9, no. 2, 2023.

[7] S. Rahmawati and Y. Saputra, “Penerapan Algoritma Hybrid AES dan Caesar Cipher untuk Keamanan Data pada Aplikasi Mobile,” *Jurnal Riset Informatika*, vol. 13, no. 1, 2024.

[8] H. Siregar and B. Simanjuntak, “Aplikasi Android untuk Enkripsi File dan Pesan Menggunakan AES dan Vigenere,” *Prosiding Seminar Nasional Teknologi Informasi*, vol. 3, no. 1, pp. 122–130, 2021.

Volume X, Nomor X, Bulan 202X, Page 999-999
ISSN 0000-0000 (media online)
Available Online at https://journal.mediapertek.com/index.php/j-cts
DOI

[9] M. N. Z. Soleh, "Kriptografi Homomorfik dalam Anonimisasi Data untuk Pengolahan Data pada Sistem E-Voting," *Jurnal Masyarakat Informatika*, vol. 15, no. 2, 2024.

[10] A. Syahputra and T. Gunawan, "Implementasi Algoritma AES pada Penyimpanan File Android," *Jurnal Sistem Informasi*, vol. 9, no. 3, 2023.

[11] F. Wibowo and F. Lestari, "Analisis Performa Algoritma AES pada Proses Enkripsi Data di Smartphone Android," *Jurnal Teknologi Informasi dan Komputer*, vol. 10, no. 3, 2022.

[12] A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *Jurnal Al-Azhar Indonesia Seri Sains dan Teknologi*, vol. 4, no. 3, pp. 110–116, 2018.

[13] E. Safrianti and F. Fitriansyah, "Cryptography with Layered Algorithms for Text Security on Android," *International Journal of Electrical, Energy and Power System Engineering*, vol. 3, no. 2, pp. 35–39, 2020.

[14] A. Taqwa and D. Sulaksono, "Implementasi Kriptografi Dengan Metode Elliptic Curve Cryptography (ECC) Untuk Aplikasi Chatting Dalam Cloud Computing Berbasis Android," *Kernel: Jurnal Riset Inovasi Bidang Informatika dan Pendidikan Informatika*, vol. 1, no. 1, pp. 42–48, 2020.

[15] S. Saefudin and S. Syamsudin, "Aplikasi Enkripsi Pesan Teks Dengan Metode Advanced Encryption Standard Pada Ponsel Berbasis Android," *JSiI (Jurnal Sistem Informasi)*, vol. 4, no. 2, pp. 50–57, 2017.

[16] A. Hermawan, A. Halim, D. Susilawati, and I. A. Putri, "Implementasi Algoritma Advanced Encryption Standard dan Caesar Cipher pada Pesan Terenkripsi," *Jurnal Informatika dan Rekayasa Perangkat Lunak*, vol. 5, no. 1, pp. 13–21, 2023.

[17] F. Rahmad and A. Anwar, "Implementasi Kriptografi Dengan Metode Advanced Encryption Standard (AES) Untuk Realtime Chat Berbasis Mobile Pada E-Learning Politeknik Negeri Lhokseumawe," *J-AISE: Journal of Artificial Intelligence and Software Engineering*, vol. 1, no. 2, pp. 45–52, 2021.

[18] A. Farissi, A. Pradata, and K. Miraswan, "Securing Messages Using AES Algorithm and Blockchain Technology on Mobile Devices," *SinkrOn: Jurnal dan Penelitian Teknik Informatika*, vol. 8, no. 2, pp. 1166–1171, 2023.

[19] Y. Laia, M. Nababan, O. Sihombing, and others, "File Cryptography with AES and RSA for Mobile Based on Android," *Journal of Physics: Conference Series*, vol. 1007, no. 1, pp. 1–7, 2018.

[20] M. Mulyadi, "Aplikasi Kriptografi Pesan Teks Menggunakan Algoritma Advanced Encryption Standard 256 Bit (AES-256) dan Diffie Hellman," *Sisfo: Jurnal Ilmiah Sistem Informasi*, vol. 7, no. 2, pp. 23–30, 2022.

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**