Neptunus: Jurnal Ilmu Komputer dan Teknologi Informasi
Volume 3, Nomor 4, November 2025
e-ISSN: 3031-898X; p-ISSN: 3031-8998, Hal 119-127
DOI: https://doi.org/10.61132/neptunus.v3i4.1203
Tersedia: https://journal.arteii.or.id/index.php/Neptunus

Implementasi Kriptografi Menggunakan Metode Permutasi pada Pesan Berbasis Android

Ratih Adinda Destari
Fakultas Teknik dan Ilmu Komputer, Sistem Informasi, Universitas Potensi Utama, Indonesia
**Penulis Korespondensi: adindaalkarim0384@gmail.com*

Abstract. *The exchange of information in the digital era has become a general need for society. However, the information sent often has a public or confidential nature. Therefore, security is needed so that confidential information remains safe. Cryptography is a field of knowledge used to secure information using encryption and decryption processes. One of the cryptographic methods used is the permutation method, which changes the layout, sequence, or structure of data into a form that is difficult to understand without knowledge of the exact key. Implementing cryptography using the permutation method in Android-based applications can increase the security and privacy of user data, as well as protect sensitive information from unauthorized access. This research aims to implement permutation method cryptography in Android-based applications to protect the confidentiality or privacy of user data. By using the permutation method, the sequence of bits or characters in the data is scrambled so that it is difficult for unauthorized parties to understand. The research results show that the implementation of permutation method cryptography in Android applications can provide a higher level of security in maintaining data confidentiality. However, it is worth considering that simple permutation methods may not be secure enough to deal with more sophisticated attacks. Therefore, choosing a stronger cryptographic method needs to be considered to achieve a higher level of security. In conclusion, implementing cryptography using the permutation method in Android-based applications can increase the security and privacy of user data. The permutation method is able to randomize the sequence of bits or characters in the data so that it is difficult for unauthorized parties to understand. However, for a higher level of security, it is necessary to consider stronger cryptographic methods.*

Keywords: *Android System; Cryptography; Data Security; Information; Permutation Methods.*

Abstrak. Pertukaran informasi dalam era serba digital telah menjadi kebutuhan umum masyarakat. Namun, informasi yang dikirimkan seringkali memiliki sifat publik maupun rahasia. Oleh karena itu, diperlukan pengamanan agar informasi yang bersifat rahasia tetap aman. Kriptografi merupakan bidang pengetahuan yang digunakan untuk mengamankan informasi dengan menggunakan proses enkripsi dan dekripsi. Salah satu metode yang digunakan dalam penelitian ini adalah metode permutasi, yang mana mengubah tata letak, urutan, atau struktur data menjadi bentuk yang sulit dipahami tanpa pengetahuan kunci yang tepat. Implementasi kriptografi menggunakan metode permutasi pada aplikasi berbasis Android dapat meningkatkan keamanan dan privasi data pengguna, serta melindungi informasi sensitif dari akses yang tidak sah. Penelitian ini bertujuan untuk mengimplementasikan kriptografi metode permutasi pada aplikasi berbasis Android guna melindungi kerahasiaan atau privasi data pengguna. Adapun data yang digunakan dalam penelitian ini adalah data pesan melalui media WhatsApp. Hasil dari penelitian menunjukkan bahwa implementasi kriptografi metode permutasi pada aplikasi Android dapat memberikan tingkat keamanan yang lebih tinggi dalam menjaga kerahasiaan data. Namun, perlu dipertimbangkan bahwa metode permutasi sederhana mungkin tidak cukup aman untuk menghadapi serangan yang lebih canggih. Oleh karena itu, pemilihan metode kriptografi yang lebih kuat perlu dipertimbangkan untuk mencapai tingkat keamanan yang lebih tinggi. Kesimpulannya, implementasi kriptografi menggunakan metode permutasi pada aplikasi berbasis Android dapat meningkatkan keamanan dan privasi data pengguna. Metode permutasi mampu mengacak urutan bit atau karakter dalam data sehingga sulit dipahami oleh pihak yang tidak berwenang.

Kata kunci: Informasi; Keamanan Data; Kriptografi; Metode Permutasi; Sistem Android.

1. LATAR BELAKANG

Pada era digital saat ini, pertukaran informasi menjadi kebutuhan yang tidak terpisahkan dari aktivitas masyarakat. Informasi dikirimkan melalui berbagai perangkat elektronik seperti komputer, ponsel pintar, dan sistem berbasis internet. Data yang ditransmisikan dapat berupa teks, gambar, maupun multimedia yang bersifat publik maupun sangat rahasia. Kondisi ini

Naskah Masuk: 22 September 2025; Revisi: 25 Oktober 2025; Diterima: 28 November 2025; Terbit: 30 November 2025

menuntut adanya sistem keamanan data yang andal untuk memastikan bahwa informasi sensitif terlindungi dari pihak yang tidak berwenang (Abdala et al., 2017; Dewanto & Suharso, 2022).

Kriptografi merupakan teknik fundamental dalam menjaga kerahasiaan data dengan mengubah informasi asli menjadi bentuk terenkripsi menggunakan proses matematika tertentu (Nurdin, 2017; Stallings, 2017). Proses enkripsi dan dekripsi memastikan bahwa hanya pihak yang memiliki kunci yang tepat yang dapat membaca isi data. Berbagai algoritma kriptografi modern telah dikembangkan, di antaranya adalah DES, AES, IDEA, serta algoritma berbasis substitusi dan permutasi (Alasi et al., 2021; Liesdiani, 2017; Schneier, 2015).

Salah satu pendekatan kriptografi yang banyak digunakan adalah metode permutasi, yaitu teknik yang mengubah urutan, posisi, atau struktur elemen data untuk menghasilkan ciphertext yang sulit dipahami tanpa kunci tertentu. Metode permutasi efektif digunakan dalam berbagai implementasi dasar maupun sebagai bagian dari algoritma kriptografi yang lebih kompleks, seperti pada Feistel Structure dan block cipher (Menezes et al., 2018; Katz & Lindell, 2020).

Dalam konteks aplikasi berbasis Android, kebutuhan keamanan semakin mendesak karena tingginya intensitas pertukaran data melalui jaringan dan penyimpanan lokal perangkat. Keamanan Android yang bersifat terbuka membuat aplikasi rentan terhadap serangan seperti sniffing, reverse engineering, dan penyadapan data (Enck et al., 2009; Shabtai et al., 2010). Oleh karena itu, penerapan kriptografi, termasuk metode permutasi, menjadi langkah strategis untuk menjaga integritas dan kerahasiaan data pengguna (Patil & Waghmare, 2020).

Implementasi metode permutasi dalam aplikasi Android dapat mengacaukan struktur bit atau karakter sehingga data tidak mudah dibaca oleh pihak yang tidak berwenang. Meski demikian, metode permutasi sederhana sering dianggap kurang aman terhadap serangan kriptanalisis modern. Untuk itu, pemilihan algoritma harus mempertimbangkan tingkat ancaman serta kebutuhan keamanan (Khan et al., 2018; William & Brown, 2019).

Dengan semakin meningkatnya risiko keamanan digital, diperlukan penelitian komprehensif untuk mengkaji penerapan metode permutasi pada aplikasi Android agar dapat menghasilkan sistem keamanan yang efektif, efisien, dan mudah diimplementasikan.

2. KAJIAN TEORITIS

Jenis Penelitian

Jenis penelitian yang dilakukan adalah penelitian terapan, yaitu penelitian yang bertujuan untuk menyelesaikan masalah yang ada dengan menerapkan teori-teori yang mendasari penelitian yang dikaji dengan terlebih dahulu menyusun konsep-konsep yang berkaitan dengan kriptografi secara matematis.

Metode yang digunakan dalam penelitian ini. Metode penelitian ini meliputi penentuan model enkripsi, penyelesaian algoritma enkripsi, pembuatan simulasi enkripsi dan analisa hasil dari simulasi enkripsi.

Metode pengembangan sistem

Metode pengembangan sistem yang penulis gunakan dalam penelitian ini adalah metode Extreme Programming. Extreme Programming yaitu sebuah metode dalam pengembangan sistem yang dilakukan untuk :

1. Planning/Perencanaan Pada tahap perencanaan ini dimulai dari pengumpulan kebutuhan yang membantu tim teknikal untuk memahami konteks bisnis dari sebuah aplikasi. Selain itu pada tahap ini juga mendefinisikan output yang akan dihasilkan, fitur yang dimiliki oleh aplikasi dan fungsi dari aplikasi yang dikembangkan.
2. Design/Perancangan Metode ini menekankan desain aplikasi yang sederhana, bagaimana sebuah aplikasi bisa berjalan dengan baik.
3. Coding/Pengkodean

   Konsep utama dari tahapan pengkodean pada extreme programming adalah bagaimana menyusun kode yang sederhana sehingga mudah dipahami.
4. Testing/Pengujian Pada tahapan ini lebih fokus pada pengujian fitur dan fungsionalitas dari aplikasi.

3. METODE

Kriptografi

Kriptografi dalam dunia komputer itu sangat mempunyai peran penting, karena di media media komputer terdapat banyak informasi rahasia penting yang tidak boleh di ketahui oleh orang yang tidak berhak untuk mengakses informasi tersebut. Jadi dengan menerapkan kriptografi ini kita bisa lebih mudah dan tidak perlu takut untuk mengirimkan informasi yang bersifat rahasia dan hanya penerima yang bisa menghapus penyamaran dan pembacaan pesan atau menguraikan nya[4]. Kriptografi ini termasuk ilmu yang mempelajari teknik teknik matematika yang berhubungan dengan keamanan informasi, dan biasanya informasi atau pesan

yang di sampaikan dari satu pihak ke pihak lain itu bisa berupa pesan teks, pesan gambar, maupun pesan suara.

Permutasi

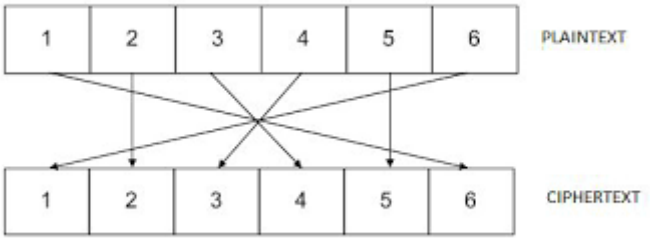
Permutasi merupakan salah satu teknik dasar dalam kriptografi yang bekerja dengan melakukan pengacakan urutan bit, karakter, kata maupun blok dari plaintext ke chipertext. Proses permutasi memindahkan posisi dari data asli berdasarkan aturan atau kunci tertentu kedalam tabel permutasi sehingga menghasilkan chipertext. Maka dari itu teknik permutasi ini juga salah satu teknik enkripsi dalam kriptografi karena teknik ini memindahkan karakter dengan mempunyai aturan tertentu.

4. HASIL DAN PEMBAHASAN

Berdasarkan pembahasan yang ada maka di dapatkan hasil dari implementasi kriptografi menggunakan metode permutasi pada aplikasi berbasis android, yaitu aplikasi berbasis android untuk pengamanan informasi. Selain itu itu penerapan kriptografi dengan metode permutasi memiliki cara pengerjaan secara manual dan juga menggunakan aplikasi berbasis android .

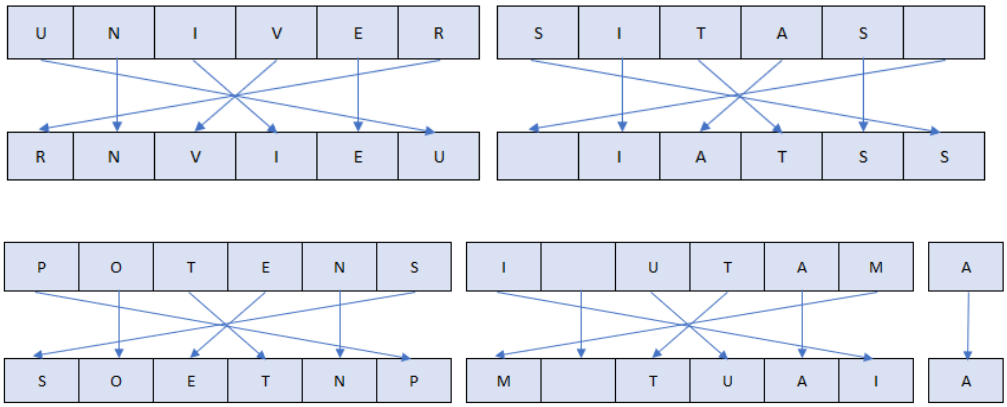
Metode Permutasi Secara Manual

Prinsip metode permutasi dalam kriptografi adalah mengubah urutan karakter dalam teks yang akan dienkripsi. Sebelum melakukan permutasi, maka plaintext akan dibagi menjadi blok-blok dengan panjang yang sama sesuai aturan permutasi



Gambar 1. Aturan Permutasi.

Diketahui pengirim memiliki pesan informasi dengan plaintext “UNIVERSITAS POTENSI UTAMA” yang akan dikirimkan ke penerima. Maka masukan setiap kata kedalam blok-blok sesuai dengan aturan permutasi, kemudian ubah urutan karakter dalam plaintext tersebut sesuai dengan aturan permutasi. Yang dimana untuk karakter pertama menyilang dengan karakter terakhir, karakter kedua dan kelima tetap berada di posisi awal, dan karakter ke tiga dan ke empat saling menyilang. Maka didapatkan chipertext pada gambar 2. Berdasarkan gambar 2 maka chipertext pada pesan informasi “ UNIVERSITAS POTENSI UTAMA” yaitu “RNVIEU IATSSSOETNPM TUAAIA”

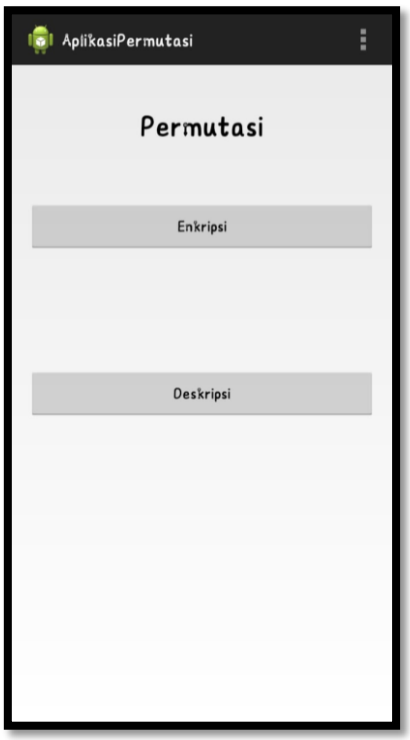


Gambar 2. Proses Enkripsi.

Metode Permutasi Menggunakan Aplikasi Berbasis Android

Tampilan Pengguna Android

Pada bagian ini, aplikasi yang telah dibangun dengan teknik yang disarankan ditunjukkan pada Gambar 3 yang menunjukkan tampilan awal dengan dua tombol yaitu tombol enkripsi dan tombol dekripsi, dengan mengklik tombol enkripsi akan menuju ke halaman enkripsi, dan sebaliknya.



Gambar 3. Menu Utama.

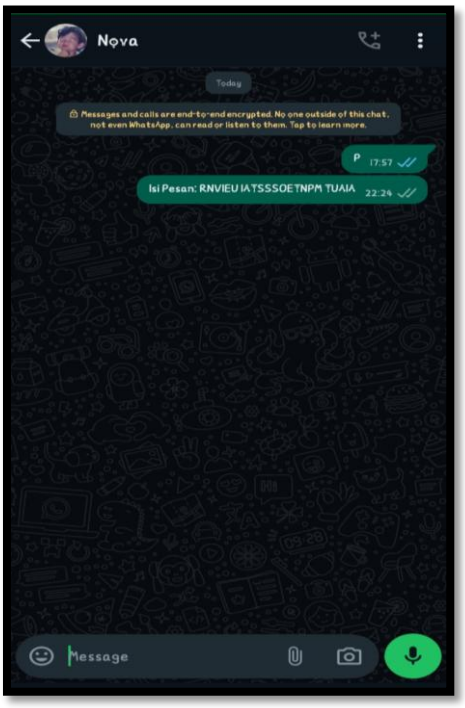
Selanjutnya, gambar 4 menunjukkan tampilan proses enkripsi dari sisi pengirim yang menggunakan Android.

Gambar 4. Proses Enkripsi Sisi Pengirim.

Kemudian, gambar 5 menunjukan tampilan pengiriman pesan enkripsi ke WhatsApp dari sisi pengirim menggunakan Android.

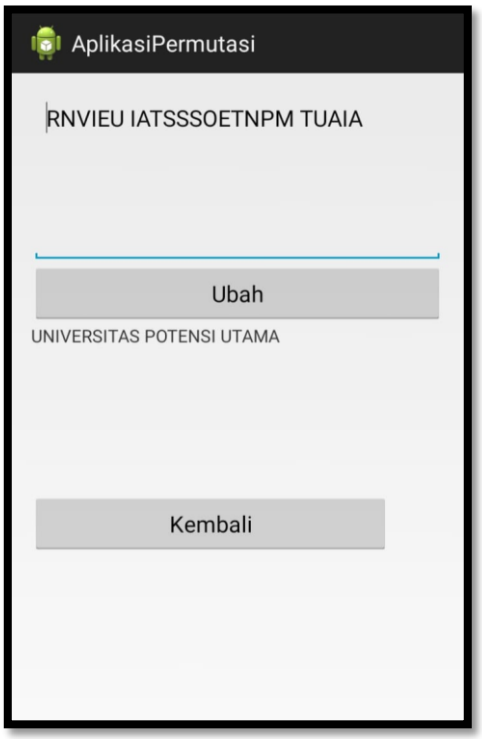
Gambar 5. Pengiriman Pesan Enkripsi.

Kemudian, gambar 6 menunjukan tampilan pesan Enkripsi yang sudah di kirim melalui WhatsApp.



Gambar 6. Pesan Enkripsi.

Setelah itu pada gambar 7 menampilkan proses deskripsi dari sisi penerima.



Gambar 7. Proses Deskripsi Sisi Penerima.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil dan pembahasan yang ada, dapat disimpulkan bahwa implementasi kriptografi menggunakan metode permutasi pada pesan berbasis Android dapat membantu meningkatkan keamanan dan privasi pesan pengguna. Pada penelitian ini maka dihasilkan pesan enkripsi yang akan dikirim melalui media WhatsApp

Dalam konteks aplikasi berbasis Android, penggunaan metode permutasi dapat memberikan tingkat keamanan yang lebih tinggi dalam melindungi pesan yang akan dikirimkan melalui media WhatsApp. Dengan cara merubah pesan yang akan dikirimkan melalui aplikasi berbasis android tersebut yang memungkinkan pihak yang tidak berwenang sulit untuk memahami pesan tersebut. Namun, perlu diingat bahwa metode permutasi yang sederhana mungkin tidak cukup aman untuk menghadapi serangan yang lebih canggih. Tergantung pada tingkat keamanan yang diinginkan, mungkin diperlukan implementasi kriptografi yang lebih canggih lagi yang dimana dapat menggabungkan 2 metode kriptografi sekaligus tidak hanya metode permutasi saja.

UCAPAN TERIMA KASIH

Ucapkan terima kasih kepada semua orang yang terlibat dalam pembuatan jurnal ini

DAFTAR REFERENSI

Abdala, P., Budiman, M. A., & Herriyance, H. (2017). Implementasi algoritma kriptografi Vernam Cipher dan DES (Data Encryption Standard) pada aplikasi chatting berbasis Android. *Jurnal Ilmiah CORE IT, 5*(1), 1–19. http://core-it.org/index.php/coreit/article/view/27

Alasi, T. S., Wanto, R., & Sitanggang, V. H. (2021). Implementasi kriptografi algoritma IDEA pada keamanan data teks berbasis Android. *Jurnal Informatika Komputer dan Logika, 2*(1), 1–4.

Dewanto, R. A., & Suharso, A. (2022). Analisis teknik-teknik kriptografi terhadap serangan jaringan lokal. *Jurnal Ilmiah Wahana Pendidikan, 8*(16), 467–476. https://doi.org/10.5281/zenodo.7068003

Enck, W., Ongtang, M., & McDaniel, P. (2009). Understanding Android security. *IEEE Security & Privacy, 7*(1), 50–57. https://doi.org/10.1109/MSP.2009.26

Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography* (3rd ed.). CRC Press. https://doi.org/10.1201/9781351133036

Khan, A., Khan, M. J., & Ali, F. (2018). Performance evaluation of classical and modern cryptography techniques. *International Journal of Computer Applications, 179*(44), 1–7.

Liesdiani, M. (2017). Sistem kriptografi pada citra digital menggunakan metode substitusi dan permutasi. *Prosiding SNATIKA*, *4*, 24–31. https://jurnal.stiki.ac.id/SNATIKA/article/view/140

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC Press. https://doi.org/10.1201/9780429466335

Nurdin, A. P. N. (2017). Analisa dan implementasi kriptografi pada pesan rahasia. *Jurnal JESIK*, *3*(1), 1–11.

Patil, A., & Waghmare, S. (2020). Data security enhancement in Android applications using hybrid cryptography. *International Journal of Computer Science Trends and Technology*, *8*(2), 12–18.

Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (2nd ed.). Wiley. https://doi.org/10.1002/9781119183471.ch10

Shabtai, A., Fledel, Y., & Elovici, Y. (2010). Securing Android-powered mobile devices using SELinux. *IEEE Security & Privacy*, *8*(3), 36–44. https://doi.org/10.1109/MSP.2009.144

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

William, P., & Brown, K. (2019). A comparative study of encryption techniques for mobile applications. *International Journal of Mobile Computing*, *7*(2), 45–53.

Zhou, Y., & Jiang, X. (2012). Dissecting Android malware: Characterization and evolution. *IEEE Symposium on Security and Privacy*, 95–109. https://doi.org/10.1109/SP.2012.16