

Artikel 3:

Implementasi Metode Triple DES pada Aplikasi Keamanan Pesan Berbasis Mobile

Sitasi (APA Style):

Alda, M., & Rifki, M. I. (2022). *Implementasi Metode Triple DES pada Aplikasi Keamanan Pesan Berbasis Mobile*. JOINTTECS: Journal of Information Technology and Computer Science, 7(1), 17–26.

Review:

Artikel ini membahas penggunaan *Triple Data Encryption Standard* (Triple DES) dalam aplikasi pesan berbasis Android. Topiknya penting karena komunikasi melalui smartphone sering tidak aman dan berisiko disadap. Penelitian ini berkontribusi dengan merancang aplikasi yang mampu mengenkripsi pesan menjadi *ciphertext* dan mendekripsinya kembali ke *plaintext*. Keunggulan Triple DES adalah enkripsi dilakukan tiga kali sehingga lebih kuat dibanding DES biasa. Namun, penelitian terbatas pada platform Android dan belum dibandingkan dengan algoritma modern lain seperti AES yang lebih populer saat ini.

Ringkasan Ilmiah:

Latar & Tujuan:

Pesan teks yang tidak terenkripsi rentan dicuri atau dimodifikasi. Penelitian ini bertujuan membangun aplikasi mobile berbasis Android yang memanfaatkan algoritma Triple DES untuk meningkatkan keamanan dan kerahasiaan komunikasi pengguna.

Metode:

Pengembangan aplikasi dilakukan dengan model *waterfall* melalui tahapan analisis kebutuhan, perancangan, implementasi, dan pengujian. Algoritma Triple DES dengan kunci 168-bit (efektif 112-bit) digunakan untuk proses enkripsi dan dekripsi. Uji coba dilakukan dengan *black box testing* untuk memverifikasi fungsi utama aplikasi, yakni pengiriman, enkripsi, dan dekripsi pesan.

Hasil/Temuan Kunci:

Aplikasi mampu mengenkripsi pesan menjadi *ciphertext* yang tidak dapat dibaca tanpa kunci, dan berhasil mendekripsi kembali menjadi pesan asli. Dari survei terhadap 50 responden, mayoritas (86%) menilai aplikasi bermanfaat untuk menjaga kerahasiaan pesan, sedangkan 68% pernah mengalami masalah keamanan sebelum memakai aplikasi ini. Hal ini membuktikan bahwa penggunaan Triple DES dapat meningkatkan rasa aman dalam komunikasi sehari-hari.

Kontribusi & Keterbatasan:

Penelitian ini berkontribusi dengan menyediakan aplikasi Android sederhana namun efektif untuk mengamankan pesan teks. Keterbatasannya adalah hanya menguji algoritma Triple DES tanpa perbandingan dengan algoritma lain, serta belum diimplementasikan pada platform di luar Android.

Takeaway:

Triple DES terbukti dapat meningkatkan keamanan pesan pada aplikasi mobile dan memberi rasa aman bagi pengguna. Meski demikian, penelitian lanjutan diperlukan untuk menguji algoritma kriptografi lain agar didapatkan solusi yang lebih cepat dan efisien.