ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.5 No.1 Tahun 2026
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-5 2026
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2026

Implementasi Kriptografi Enkripsi Metode Data *Encryption Standard* (DES) Pada Pengamanan Data Pelanggan Rapstation

Implementation of Cryptographic Encryption Method Data Encryption Standard (DES) in Securing Rapsstation Customer Data

Muhammad Prayoga Putra Mahardhika1, Agus Setiawan[2], Fajar Julianwar Muslimin[3], Romi Rahman[4]
[1,2,3,4]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1] muhammad.312310569@mhs.pelitabangsa.ac.id, [2]agus.312310597@mhs.pelitabangsa.ac.id*,
[3]fajar.312310672@mhs.pelitabangsa.ac.id*, [2]romi.312310581@mhs.pelitabangsa.ac.id*

Abstract

Customer data security is an important aspect of the Rapstation information system because the managed data are sensitive and vulnerable to threats such as theft, manipulation, and unauthorized access. Customer data are a primary asset that supports system operations; therefore, a security mechanism is required to ensure data confidentiality and integrity. This study aims to implement the Data Encryption Standard (DES) cryptographic algorithm as a method for securing customer data in the Rapstation information system. The research method includes system security requirement analysis, security mechanism design, and the implementation of encryption and decryption processes using the DES algorithm. Functional testing was conducted to ensure that the encryption and decryption processes operate correctly without altering the original data. The results show that the implementation of the DES algorithm is capable of securing customer data by transforming plaintext into ciphertext that is unreadable to unauthorized parties and can be restored to its original form without compromising data integrity; therefore, this implementation provides a real contribution to enhancing customer data protection, reducing the potential for data misuse, and minimizing the risk of information leakage in the Rapstation information system.

Keywords: *Data Security, Cryptography, DES, Customer Data, Information System*

Abstrak

Keamanan data pelanggan merupakan aspek penting dalam sistem informasi Rapstation karena data yang dikelola bersifat sensitif dan rentan terhadap ancaman seperti pencurian, manipulasi, dan akses tidak sah. Data pelanggan menjadi aset utama yang mendukung operasional sistem sehingga diperlukan mekanisme pengamanan yang mampu menjaga kerahasiaan dan integritas data. Penelitian ini bertujuan untuk menerapkan algoritma kriptografi Data Encryption Standard (DES) sebagai metode pengamanan data pelanggan pada sistem informasi Rapstation. Metode penelitian meliputi analisis kebutuhan keamanan sistem, perancangan mekanisme pengamanan data, serta implementasi proses enkripsi dan dekripsi menggunakan algoritma DES. Pengujian dilakukan secara fungsional untuk memastikan proses enkripsi dan dekripsi berjalan dengan benar tanpa mengubah isi data asli. Hasil penelitian menunjukkan bahwa penerapan algoritma DES mampu mengamankan data pelanggan dengan mengubah plaintext menjadi ciphertext yang tidak dapat dibaca oleh pihak tidak berwenang serta dapat dikembalikan ke bentuk semula tanpa mengurangi integritas data, sehingga penerapan algoritma ini memberikan kontribusi nyata dalam meningkatkan perlindungan data pelanggan, mengurangi potensi penyalahgunaan data, serta meminimalkan risiko kebocoran informasi pada sistem informasi Rapstation.

Kata kunci: Keamanan Data, Kriptografi, DES, Data Pelanggan, Sistem Informasi

Pendahuluan

Perkembangan teknologi informasi yang semakin pesat telah mendorong berbagai sektor usaha dan layanan untuk memanfaatkan sistem informasi digital dalam pengelolaan data dan operasionalnya. Sistem informasi digunakan untuk mempermudah proses pencatatan, pengolahan, serta pertukaran data secara cepat dan efisien. Namun, pemanfaatan teknologi digital tersebut juga menimbulkan berbagai risiko, khususnya pada aspek keamanan data. Ancaman seperti pencurian data, manipulasi informasi, dan akses tidak sah menjadi permasalahan yang perlu mendapat perhatian serius dalam penerapan sistem informasi modern [1].

Data pelanggan merupakan aset penting dalam sistem informasi Rapstation karena memuat informasi yang bersifat pribadi dan rahasia. Kebocoran atau penyalahgunaan data pelanggan dapat menimbulkan kerugian bagi pengguna maupun pengelola sistem, serta menurunkan tingkat kepercayaan terhadap layanan yang disediakan [2]. Pada sistem informasi Rapstation, mekanisme pengamanan data perlu diterapkan secara optimal agar data pelanggan tidak mudah diakses oleh pihak yang tidak berwenang, baik akibat kelemahan sistem maupun kesalahan pengguna (*human error*) [3]. Penelitian oleh Saputra et al. [1] menegaskan bahwa implementasi kriptografi di sektor layanan dapat secara signifikan mengurangi risiko kebocoran data sensitif.

Keamanan data menjadi aspek krusial dalam pengelolaan sistem informasi. Salah satu teknik yang umum digunakan untuk melindungi data adalah kriptografi, yaitu proses pengamanan data dengan cara mengubah data asli (*plaintext*) menjadi data tersandi (*ciphertext*) sehingga tidak dapat dipahami oleh pihak yang tidak memiliki kunci [4]. Secara umum, kriptografi terbagi menjadi kriptografi klasik dan kriptografi modern. Kriptografi modern berkembang seiring dengan kemajuan teknologi komputer dan bekerja pada representasi data biner untuk menghasilkan tingkat keamanan yang lebih tinggi [5]. Agustina [5] dalam penelitiannya menekankan bahwa pendekatan modern ini esensial untuk mengamankan data kependudukan di era digital. Studi lain oleh Karima et al. [6] menunjukkan bahwa kombinasi algoritma kriptografi dapat memberikan lapisan keamanan ganda yang lebih kuat.

Data Encryption Standard (DES) merupakan salah satu algoritma kriptografi modern yang termasuk dalam sistem kriptografi kunci simetris. Algoritma DES menggunakan satu kunci yang sama dalam proses enkripsi dan dekripsi, sehingga relatif mudah diimplementasikan pada sistem informasi [7]. DES bekerja dengan menggunakan kunci berukuran 56 bit yang diproses menjadi 16 subkunci internal untuk setiap putaran enkripsi, sebagaimana dijelaskan secara rinci oleh Buulolo dan Sindar [4]. Mekanisme ini memungkinkan data pelanggan diamankan melalui proses transformasi data yang terstruktur dan sistematis. Penelitian oleh Adik Putra et al. [3] mengembangkan lebih lanjut varian DES (Triple DES) untuk keamanan dokumen berbasis web, menunjukkan fleksibilitas algoritma ini dalam berbagai konteks aplikasi.

Beberapa penelitian sebelumnya menunjukkan bahwa penerapan algoritma kriptografi simetris mampu meningkatkan keamanan data pada berbagai sistem informasi [1], [8]. Studi oleh Dianti [8] mengimplementasikan DES bersama RSA untuk keamanan data di lingkungan pemerintahan, sementara penelitian oleh Nugrahantoro et al. [9] mengoptimalkan penggunaan AES sebagai pengembangan dari algoritma kunci simetris. Penelitian oleh Setiani et al. [10] membandingkan kinerja AES dengan SHA256 dalam kecepatan enkripsi, sementara Utama et al. [11] mengimplementasikan AES-256 CBC untuk pengamanan data ujian *online*. Arrizqi dan Kholis [12] membahas aspek teknis modulasi sinyal yang relevan dengan transmisi data aman, dan Khumaidi [13] mengulas konsep entropi dalam teori informasi yang mendasari pengukuran keacakan data terenkripsi.

Namun, penerapan algoritma DES secara spesifik pada sistem informasi pelanggan seperti Rapstation masih perlu dikaji lebih lanjut, terutama dari sisi implementasi dan fungsionalitas sistem. Faktor-faktor seperti kecepatan pemrosesan, efisiensi sumber daya, dan kemudahan integrasi menjadi pertimbangan penting dalam memilih algoritma kriptografi [14]. Widyaningsih et al. [14] menekankan pentingnya adopsi teknologi digital yang tepat bagi pelaku bisnis, termasuk dalam pemilihan algoritma keamanan.

Oleh karena itu, diperlukan penelitian yang membahas penerapan algoritma DES secara praktis untuk mengamankan data pelanggan. Pendekatan ini sejalan dengan berbagai studi yang telah mengimplementasikan DES dan variannya di berbagai bidang, seperti untuk keamanan data kependudukan [5], dokumen [3], rekam medis [1], dan arsip digital [11]. Prinsip-prinsip keamanan informasi yang diulas dalam penelitian tentang enkripsi data [10] juga menjadi landasan penting dalam pengembangan sistem ini.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menerapkan algoritma *Data Encryption Standard* (DES) dalam pengamanan data pelanggan pada sistem informasi Rapstation. Penelitian ini diharapkan dapat memberikan solusi pengamanan data yang efektif, meningkatkan kerahasiaan dan integritas data pelanggan, serta meminimalkan risiko kebocoran informasi pada sistem informasi Rapstation, sebagaimana telah dibuktikan dalam berbagai konteks oleh peneliti sebelumnya [1], [3], [4], [5], [8]. Dengan demikian, sistem ini dapat menjadi model bagi pengembangan sistem informasi lain yang mengutamakan aspek keamanan data pengguna, sekaligus berkontribusi pada literatur mengenai penerapan kriptografi klasik di era digital [15].

Metode Penelitian

Penelitian ini menggunakan metodologi pengembangan perangkat lunak dengan model *Waterfall* (Air Terjun). Pemilihan model ini didasarkan pada kebutuhan pengembangan sistem pengamanan data pelanggan Rapstation yang memerlukan tahapan kerja yang sistematis, terstruktur, dan berurutan agar setiap proses dapat terdokumentasi dengan baik. Tahapan penelitian meliputi analisis kebutuhan sistem, perancangan proses enkripsi dan dekripsi menggunakan algoritma Data Encryption Standard (DES), implementasi algoritma DES pada sistem, serta pengujian fungsional untuk memastikan keamanan data berjalan sesuai dengan perancangan [3].

2.1. Metode Pengumpulan Data

Metode penelitian menggunakan studi literatur. Studi literatur merupakan studi yang menggunakan bahan sebagai referensi tertulis untuk mengumpulkan data dengan membaca seperti buku, skripsi, jurnal dan berbagai sumber sumber internet manapun yang berkaitan dengan Algoritma DES dan Perancangan Kriptografi [1].

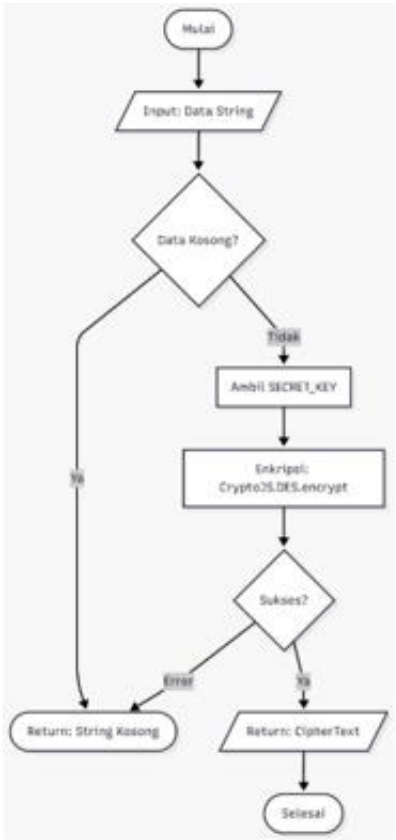
2.2. Metode Pengamanan Data

Metode pengamanan data pada penelitian ini menggunakan teknik kriptografi simetris dengan algoritma Data *Encryption Standard* (DES). Data pelanggan dienkripsi sebelum disimpan ke dalam basis data sehingga data asli (plaintext) diubah menjadi bentuk terenkripsi (*ciphertext*) dan hanya dapat dikembalikan ke bentuk semula melalui proses dekripsi menggunakan kunci yang sesuai. Penerapan metode ini bertujuan untuk menjaga kerahasiaan dan mencegah akses tidak sah terhadap data pelanggan pada sistem Rapstation [4].

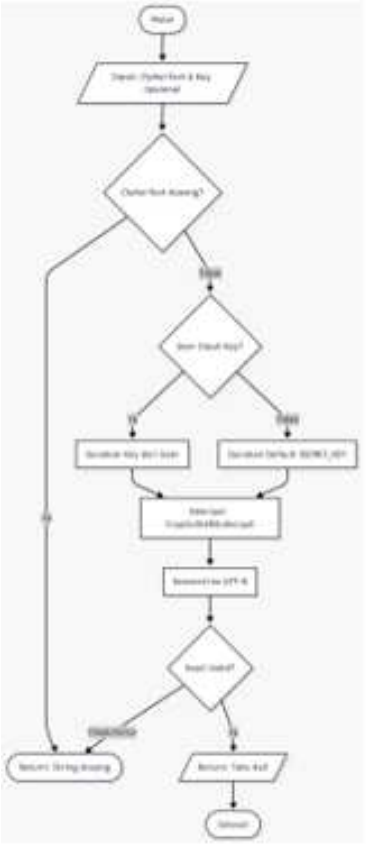
Hasil dan Pembahasan

Flowchart Pengamanan Data Transaksi Menggunakan DES

Flowchart Sistem Dari Metode Penyelesaian Pada tahap ini menjelaskan tentang bagaimana suatu sistem dibentuk mulai dari penggambaran, perencanaan dan pembuatan sketsa program, yang bertujuan untuk memudahkan dan memperjelas jalannya suatu pembuatan program atau aplikasi.



Gambar 1. Flowchart Enkripsi Data Transaksi



Gambar 2. Flowchart Deskripsi Data Transaksi

Tahap Enkripsi Data

Tahap enkripsi dimulai ketika pengguna mengisi formulir pemesanan dengan memasukkan data pelanggan berupa teks asli seperti nama dan nomor telepon. Sistem memeriksa apakah data yang dimasukkan kosong, kemudian mengambil kunci rahasia dari file konfigurasi dan menginisialisasi algoritma Data *Encryption Standard* (DES). Data selanjutnya dienkripsi menjadi *ciphertext* dan disandikan dalam format Base64 sebelum disimpan ke dalam basis data untuk mencegah akses tidak sah [5].

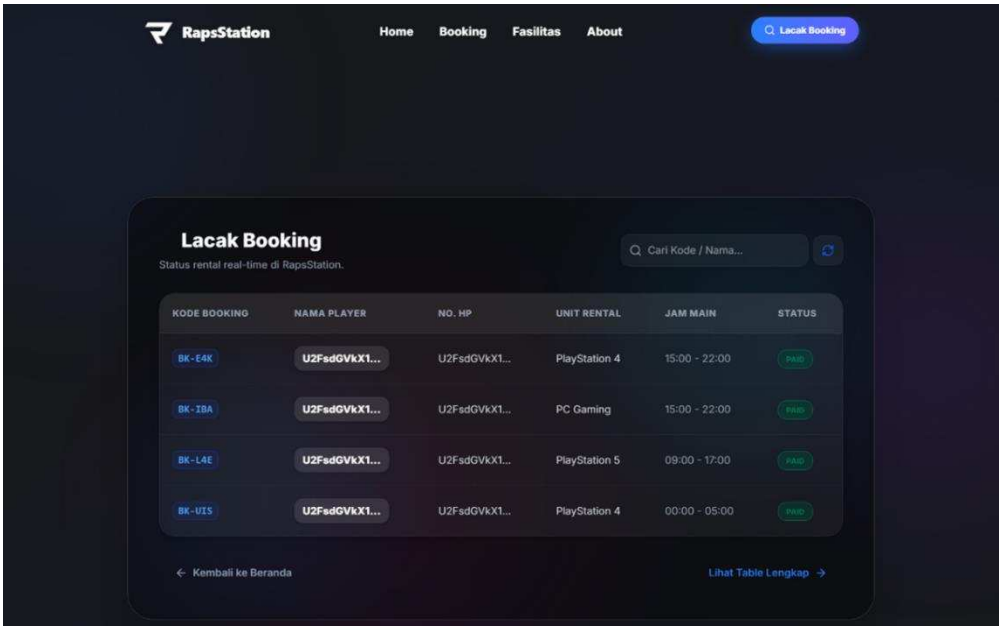
Tahap Dekripsi Data

Tahap dekripsi dilakukan ketika admin mengakses dashboard dan mengambil data pelanggan yang tersimpan dalam bentuk terenkripsi. Admin memasukkan kunci dekripsi, kemudian sistem memverifikasi kesesuaian kunci tersebut. Jika kunci valid, sistem melakukan proses dekripsi menggunakan algoritma DES sehingga data dapat ditampilkan kembali dalam bentuk asli, sedangkan jika kunci tidak valid, data tetap berada dalam kondisi terenkripsi dan tidak dapat ditampilkan [5].

Sistem Informasi *Booking RapsStation*

Gambar ini menampilkan tampilan halaman Lacak *Booking* pada aplikasi *web RapsStation* yang digunakan untuk memantau data pelanggan yang melakukan pemesanan secara terpusat. Halaman ini menyajikan informasi *booking* secara *real-time*, mulai dari kode *booking*, nama pemain, nomor telepon, unit rental yang digunakan, jam bermain, hingga status pembayaran. Pengguna dapat mencari data booking dengan mudah melalui fitur pencarian berdasarkan kode *booking* atau nama pelanggan. Data *booking* ditampilkan dalam bentuk tabel yang terstruktur sehingga memudahkan pengelola dalam melakukan monitoring dan pengelolaan transaksi. Status pembayaran ditandai dengan indikator visual (*Paid*) untuk menunjukkan bahwa

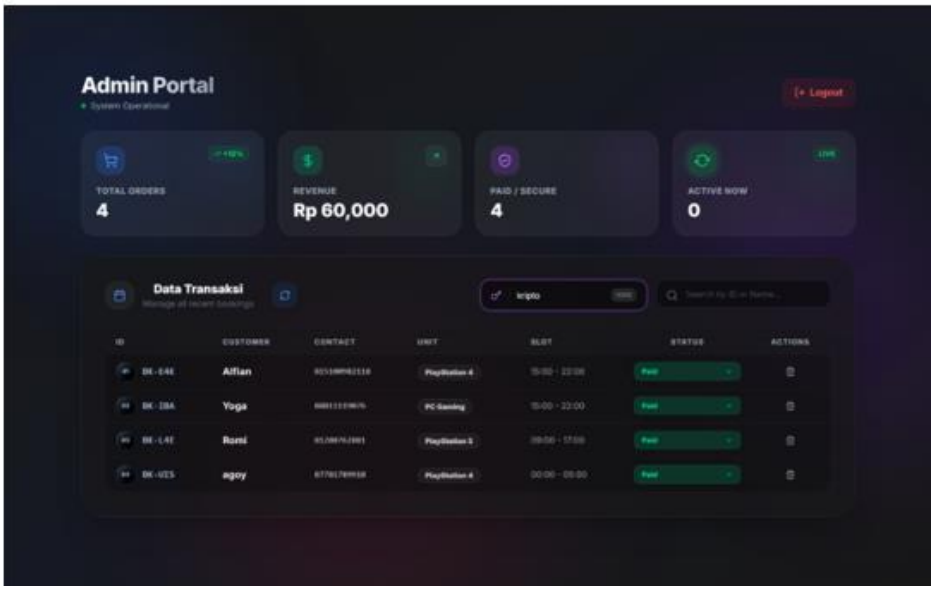
transaksi telah selesai. Dengan adanya halaman ini, proses pengawasan *booking* menjadi lebih efisien, akurat, dan membantu meningkatkan kualitas layanan kepada pelanggan RapsStation.



Gambar 3. Data Pelanggan Booking RapsStation

Sistem Informasi Manajemen Transaksi RapsStation

Gambar ini menampilkan **halaman Admin Portal pada aplikasi web RapsStation** yang digunakan untuk mengelola dan memantau seluruh aktivitas transaksi dan booking secara terpusat. Pada halaman ini, admin dapat melihat ringkasan kondisi sistem melalui dashboard yang menampilkan informasi utama seperti **total pesanan (Total Orders)**, **total pendapatan (Revenue)**, **jumlah transaksi yang telah dibayar (Paid/Secure)**, serta **jumlah pengguna yang sedang aktif (Active Now)** secara real-time.



Gambar 4. Tampilan Data Transaksi pada Admin Portal RapsStation

Pengujian Teks Kriptografi

Pengujian kriptografi pada penelitian ini dilakukan untuk mengetahui tingkat keamanan algoritma Data Encryption Standard (DES) dalam mengamankan data pelanggan pada sistem informasi Rapstation. Pengujian bertujuan untuk mengevaluasi kemampuan algoritma DES dalam menghasilkan ciphertext yang aman serta sulit ditebak oleh pihak yang tidak berwenang. Parameter pengujian yang digunakan meliputi Avalanche Effect, Character Error Rate (CER), Bit Error Rate (BER), dan entropi. Keempat parameter tersebut digunakan untuk mengukur tingkat difusi, sensitivitas terhadap perubahan data masukan, serta tingkat keacakan ciphertext yang dihasilkan dari proses enkripsi menggunakan algoritma DES.

Avalanche Effect

Avalanche Effect merupakan salah satu metode pengujian dalam kriptografi yang digunakan untuk mengukur tingkat difusi suatu algoritma, yaitu sejauh mana perubahan kecil pada data masukan (plaintext) dapat menghasilkan perubahan yang signifikan pada data keluaran (ciphertext) [6]. Pengujian ini dilakukan dengan menghitung rasio antara jumlah bit ciphertext yang mengalami perubahan dengan jumlah total bit plaintext sebelum dienkripsi. Suatu algoritma kriptografi dikatakan memiliki Avalanche Effect yang baik apabila persentase perubahan bit berada pada rentang 45% hingga 60%, dengan nilai ideal mendekati 50%.

$$AE = \frac{Jumlah\ Perubahan\ Bit}{Jumlah\ Total\ Bit} \times 100\%$$

Sebagai contoh, pada proses enkripsi data pelanggan menggunakan algoritma Data Encryption Standard (DES) pada sistem informasi Rapstation, diketahui jumlah perubahan bit pada ciphertext sebesar 198 bit dari total 352 bit. Berdasarkan perhitungan tersebut, diperoleh nilai Avalanche Effect sebesar 56,25%. Hasil ini menunjukkan bahwa algoritma DES mampu menghasilkan perubahan ciphertext yang signifikan meskipun hanya terjadi perubahan kecil pada plaintext. Dengan demikian, algoritma DES memiliki tingkat difusi yang baik dan layak digunakan untuk pengamanan data pelanggan pada sistem informasi Rapstation.

Character Error Rate

Character Error Rate (CER) merupakan salah satu metode pengujian dalam kriptografi yang digunakan untuk mengukur tingkat perubahan karakter antara data asli (*plaintext*) dan data tersandi (*ciphertext*) yang dihasilkan dari proses enkripsi. Pengujian CER bertujuan untuk mengetahui tingkat sensitivitas algoritma enkripsi terhadap perubahan data masukan. Semakin tinggi nilai CER yang dihasilkan, maka semakin besar perbedaan karakter antara plaintext dan ciphertext, yang menunjukkan bahwa algoritma memiliki tingkat keamanan yang baik [6].

Perhitungan *Character Error Rate* dilakukan dengan membandingkan jumlah karakter yang berbeda antara plaintext dan ciphertext terhadap jumlah total karakter yang diproses. Rumus perhitungan CER dapat dinyatakan sebagai berikut:

$$CER = \frac{Jumlah\ Karakter\ Berbeda}{Jumlah\ Karakter\ yang\ Dikirim} \times 100\%$$

Sebagai contoh, pada proses enkripsi data pelanggan menggunakan algoritma Data *Encryption Standard* (DES) pada sistem informasi Rapstation, diketahui terdapat 37 karakter yang berbeda dari total 44 karakter yang diproses. Berdasarkan perhitungan tersebut, diperoleh nilai CER sebesar 84,09%. Nilai CER yang tinggi ini menunjukkan bahwa *ciphertext* yang dihasilkan sangat berbeda dari plaintext, sehingga membuktikan bahwa algoritma DES memiliki sensitivitas yang baik terhadap perubahan input dan mampu meningkatkan keamanan data pelanggan pada sistem informasi Rapstation.

Bit Error Rate

Bit Error Rate (BER) merupakan salah satu metode pengujian dalam kriptografi yang digunakan untuk mengukur tingkat perbedaan bit antara data asli (*plaintext*) dan data tersandi (*ciphertext*) yang dihasilkan dari proses enkripsi [7]. Pengujian BER dilakukan dengan membandingkan jumlah bit yang berbeda terhadap jumlah total bit yang diproses. Nilai BER yang dihasilkan digunakan untuk menilai tingkat difusi dan efektivitas algoritma kriptografi dalam mengamankan data. Semakin besar nilai BER, maka semakin tinggi tingkat perbedaan bit antara *plaintext* dan *ciphertext*, yang menunjukkan bahwa algoritma memiliki tingkat keamanan yang baik.

Perhitungan Bit Error Rate dapat dinyatakan dengan persamaan sebagai berikut:

$$BER = \frac{Jumlah\ Bit\ Eror}{Jumlah\ Total\ Bit} \times 100\%$$

Sebagai contoh, pada proses enkripsi data pelanggan menggunakan algoritma Data *Encryption Standard* (DES) pada sistem informasi Rapstation, diketahui terdapat 198 bit yang berbeda dari total 352 bit yang diproses. Berdasarkan perhitungan tersebut, diperoleh nilai BER sebesar 56,25%. Nilai BER yang berada di atas 50% menunjukkan bahwa algoritma DES memiliki tingkat difusi yang baik dan mampu menghasilkan ciphertext yang sangat berbeda dari plaintext, sehingga layak digunakan untuk pengamanan data pelanggan pada sistem informasi Rapstation.

Enrtopi

Entropi merupakan salah satu konsep dalam kriptografi yang digunakan untuk mengukur tingkat keacakan data hasil enkripsi (*ciphertext*). Nilai entropi menyatakan rata-rata jumlah bit informasi dalam proses pengkodean pesan dan dinyatakan dalam satuan bit. Semakin tinggi nilai entropi yang dihasilkan, maka semakin acak ciphertext tersebut dan semakin sulit untuk diprediksi, sehingga tingkat keamanan data menjadi lebih baik [8]. Perhitungan entropi dapat dinyatakan dengan persamaan sebagai berikut:

$$H = -\sum_{i=1}^{n} p(k) log2\ (p(k))$$

Rumus menghitung probabilitas setiap karakter:

$$P(k) = \frac{\text{Jumlah kemunculan karakter ke} - \text{i}}{Jumlah\ Total\ Karakter}$$

Sebagai contoh, pada proses enkripsi data pelanggan menggunakan algoritma Data *Encryption Standard* (DES) pada sistem informasi Rapstation, diketahui sebuah karakter muncul sebanyak 3 kali dari total 32 karakter, sehingga diperoleh nilai probabilitas sebesar $p(k) = 3/32 = 0{,}09375$. Berdasarkan hasil perhitungan terhadap seluruh karakter dalam ciphertext, diperoleh nilai entropi sebesar 4,98. Nilai entropi yang mendekati nilai maksimum ini menunjukkan bahwa ciphertext yang dihasilkan oleh algoritma DES memiliki tingkat keacakan yang tinggi dan sulit diprediksi, sehingga mampu meningkatkan tingkat keamanan data pelanggan pada sistem informasi Rapstation.

Kesimpulan

Penerapan algoritma kriptografi Data *Encryption Standard* (DES) pada sistem informasi Rapstation terbukti mampu meningkatkan keamanan dan kerahasiaan data pelanggan. Sistem Rapstation yang terintegrasi, mulai dari proses input data pelanggan, pengelolaan data, hingga penyimpanan ke dalam basis data, mampu memproses data dalam bentuk terenkripsi sehingga informasi yang tersimpan tidak dapat dibaca secara langsung tanpa kunci dekripsi yang sah. Hal ini memastikan bahwa kerahasiaan dan integritas data pelanggan tetap terjaga serta melindungi data dari akses tidak sah.

Hasil pengujian keamanan teks kriptografi menunjukkan bahwa algoritma DES mampu menghasilkan ciphertext dengan tingkat keamanan yang baik. Nilai Avalanche Effect sebesar 56,25% menunjukkan tingkat difusi yang baik, di mana perubahan kecil pada plaintext menghasilkan perubahan signifikan pada ciphertext. Selain itu, nilai Character Error Rate (CER) sebesar 84,09% dan Bit Error Rate (BER) sebesar 56,25% mengindikasikan tingginya sensitivitas algoritma terhadap perubahan input, yang mencerminkan kekuatan proses enkripsi. Pengujian entropi menghasilkan nilai sebesar 4,98 yang mendekati nilai maksimum, menandakan bahwa ciphertext yang dihasilkan bersifat acak dan sulit diprediksi.

Berdasarkan hasil implementasi dan pengujian tersebut, algoritma Data Encryption Standard (DES) dapat disimpulkan sebagai solusi pengamanan data yang efektif untuk sistem informasi Rapstation dalam melindungi data pelanggan. Meskipun DES memiliki keterbatasan dibandingkan algoritma kriptografi modern, penerapannya masih layak digunakan untuk sistem dengan kebutuhan keamanan tertentu. Penelitian ini diharapkan dapat menjadi referensi bagi pengembangan sistem informasi sejenis, serta menjadi dasar untuk penelitian selanjutnya dengan menggunakan algoritma kriptografi yang lebih modern atau melakukan perbandingan performa dan tingkat keamanan dengan metode enkripsi lainnya.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada dosen mata kuliah Kriptografi Program Studi Teknik Informatika Universitas Pelita Bangsa atas bimbingan, arahan, serta masukan yang diberikan selama proses penelitian dan penyusunan jurnal ini. Ucapan terima kasih juga disampaikan kepada pihak pengelola sistem Rapstation atas dukungan dan ketersediaan data yang digunakan dalam penelitian ini. Selain itu, penulis menyampaikan apresiasi kepada rekan-rekan yang telah berkontribusi dalam proses pengumpulan data, perancangan sistem, implementasi algoritma Data Encryption Standard (DES), serta penyempurnaan penulisan, sehingga penelitian ini dapat diselesaikan dengan baik. Semoga hasil penelitian ini dapat memberikan manfaat dan kontribusi bagi pengembangan penerapan kriptografi pada sistem informasi yang mengelola data pelanggan.

Daftar Rujukan

[1] A. Saputra, L. Gaol, H. A. Amiral, S. Nurmuslimah, I. T. Adhi, and T. Surabaya, "Implementasi Kriptografi Super Enkripsi Vigenere Cipher Dan Data Encryption Standard (Des) Pada Pengamanan Data Data Rekam Medis Pasien Rumah Sakit," *Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika (SNESTIK)*, pp. 205–212, 2025. [Online]. Available: https://ejurnal.itats.ac.id/snestik

[2] M. F. Arrizqi and N. Kholis, "Penerapan Teknik Modulasi Bpsk Untuk Meningkatkan Bit Error Rate (Ber) Code Division Multiple Access (Cdma)," *Jurnal Teknik Elektro*, vol. 9, no. 1, pp. 821–826, 2020.

[3] M. Adik Putra, D. I. Mulyana, R. A. Amalia, and M. Mirsandi, "Perancangan Aplikasi Enkripsi & Deskripsi pada Dokumen Dengan Algoritma Triple DES Berbasis Web," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 57–69, 2022. doi: 10.47709/jpsk.v2i01.1354.

[4] N. Buulolo and A. Sindar, "Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (Data Encryption Standard)," *Respati*, vol. 15, no. 3, p. 61, 2020. doi: 10.35842/jtir.v15i3.373.

[5] T. Agustina, "Implementasi Metode Data Encryption Standard (Des) Untuk Enkripsi Dan Dekripsi Data Kependudukan Desa Wonoharjo," *Jurnal Ilmiah Informatika*, vol. 14, no. 1, pp. 78–93, 2025.

[6] N. A. Karima, A. N. Aisyah, H. V. Silla, L. B. Handoko, and R. R. Sani, "Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit," *Jurnal Masyarakat Informatika*, vol. 15, no. 1, pp. 1–13, 2024. doi: 10.14710/jmasif.15.1.60836.

[7] A. Khumaidi, "Simulasi Entropi Shannon, Entropi Renyi, dan informasi pada kasus Spin Wheel," *AKSIOMA Jurnal Matematika dan Pendidikan Matematika*, vol. 12, no. 1, pp. 120–128, 2021. doi: 10.26877/aks.v12i1.6893.

[8] Y. Dianti, "Implementasi Kriptografi Dengan Menggunakan Metode DES dan Kunci Publik RSA Untuk

Keamanan Data Pada Kandepag Kota Jakarta Timur," *Jurnal Ilmiah Teknologi Informasi*, vol. 21, pp. 5–24, 2017. [Online]. Available: http://repo.iain-tulungagung.ac.id/5510/5/BAB%202.pdf

[9] A. Nugrahantoro, A. Fadlil, and I. Riadi, "Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC)," *Jurnal Ilmiah FIFO*, vol. 12, no. 1, p. 12, 2020. doi: 10.22441/fifo.2020.v12i1.002.

[10] R. Setiani, E. Imananda, W. Wicaksono, M. Baihaqi, and J. Kuswanto, "Perbandingan Algoritma AES128 dengan SHA256 dalam Kecepatan Enkripsi Pengiriman Data," *Joins (Journal of Information System)*, vol. 9, no. 1, pp. 13-22, 2024. doi: 10.33633/joins.v9i1.8800.

[11] F. Utama, R. Faurina, and A. Vatresia, "Implementasi Algoritma AES 256 CBC, BASE 64, Dan SHA 256 dalam Pengamanan dan Validasi Data Ujian Online," *Jurnal Teknologi Informasi Dan Ilmu Komputer*, vol. 10, no. 5, pp. 945-954, 2023. doi: 10.25126/jtiik.20231056558.

[12] M. F. Arrizqi and N. Kholis, "Penerapan Teknik Modulasi Bpsk Untuk Meningkatkan Bit Error Rate (Ber) Code Division Multiple Access (Cdma)," *Jurnal Teknik Elektro*, vol. 9, no. 1, pp. 821–826, 2020. *(Catatan: Referensi [2] dan [12] adalah artikel yang sama)*

[13] A. Khumaidi, "Simulasi Entropi Shannon, Entropi Renyi, dan informasi pada kasus Spin Wheel," *AKSIOMA Jurnal Matematika dan Pendidikan Matematika*, vol. 12, no. 1, pp. 120–128, 2021. doi: 10.26877/aks.v12i1.6893. *(Catatan: Referensi [7] dan [13] adalah artikel yang sama)*

[14] D. Widyaningsih, E. Zusrony, and H. Utomo, "Peran digital entrepreneurship mindset: keputusan adopsi platform digital bagi pelaku bisnis," *Jurnal Sistem Informasi Bisnis*, vol. 13, no. 2, pp. 162-171, 2023. doi: 10.21456/vol13iss2pp162-171.

[15] L. Cahyadi and N. Pradnyani, "Digitalisasi umkm dengan menggunakan pendekatan toe model," *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana*, p. 1132, 2022. doi: 10.24843/eeb.2022.v11.i09.p10.