JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 9999-9999
Volume 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

Pengembangan Aplikasi Kriptografi Modern Menggunakan Algoritma Simetris DES Berbasis Python

Lisda Khairani[1], Jasmiati [2], Putri Hasanah Siregar [3], Putri Kenangan Br Berutu[4], Andhika Saputra Manurung [5], Alif Saka Al Bani Samosir [6]
[1,2,3,4,5,6]Universitas Malikussaleh, Indonesia
[1]lisda.220180010@mhs.unimal.ac.id, [2]jasmiati.220180127@mhs.unimal.ac.id, [3]putri.22080036@mhs.unimal.ac.id,
[4]Putri.220180015@mhs.unimal.ac.id, [5]andhika.220180019@mhs.unimal.ac.id, [6]alif.220180021@mhs.unimal.ac.id

ABSTRACT

In the current digital era, the security of information has become a fundamental aspect of system development. Cryptography, especially symmetric key algorithms, plays a key role in protecting data confidentiality. This research presents the development of a modern cryptographic application based on the Data Encryption Standard (DES), implemented using the Python programming language. The system is equipped with a graphical user interface (GUI) developed using Tkinter, allowing users to easily encrypt and decrypt text data. In addition to DES, the application also includes educational features such as RSA encryption and SHA-256 hashing to enhance users' understanding of various cryptographic techniques. The development process follows a prototyping method, from initial analysis to implementation and testing. Several functional tests were conducted using various text inputs, and results showed that the application successfully performed accurate encryption and decryption. Furthermore, the GUI interface provides an intuitive user experience, making it suitable as a learning tool in educational environments. This research contributes to the field of computer security by offering an open, accessible tool for understanding classical encryption methods and promoting awareness of basic data protection strategies in software applications.

Kata Kunci:
Kriptografi, DES, RSA, SHA-256, Python, Keamanan Data.

PENDAHULUAN

Dalam era digital saat ini, keamanan informasi menjadi aspek yang sangat krusial seiring meningkatnya pertukaran data melalui jaringan komputer. Akses tanpa izin terhadap informasi dapat menyebabkan kebocoran data, penipuan, hingga kerugian finansial. Salah satu metode yang digunakan untuk melindungi kerahasiaan data adalah kriptografi, yaitu ilmu yang mempelajari teknik pengamanan data dengan cara mengubah informasi menjadi bentuk yang tidak dapat dipahami tanpa proses dekripsi.

Kriptografi terbagi menjadi dua jenis utama, yaitu algoritma simetris dan asimetris. Algoritma simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Salah satu algoritma simetris yang terkenal adalah Data Encryption Standard (DES), yang dikembangkan oleh IBM pada tahun 1970-an dan kemudian diadopsi sebagai standar oleh National Institute of Standards and Technology (NIST) pada tahun 1977. Walaupun kini telah tergantikan oleh algoritma yang lebih kuat seperti Advanced Encryption Standard (AES), DES tetap banyak digunakan untuk keperluan pembelajaran dan sistem yang tidak membutuhkan tingkat keamanan tinggi.

Python merupakan bahasa pemrograman yang populer karena sintaksisnya yang sederhana dan kemampuannya untuk mengintegrasikan berbagai pustaka, termasuk pustaka kriptografi seperti pycryptodome dan hashlib. Dengan memanfaatkan pustaka-pustaka tersebut, pengembangan aplikasi kriptografi menjadi lebih mudah dan efisien, khususnya untuk keperluan edukasi. Penggunaan antarmuka grafis berbasis Tkinter juga memungkinkan pengguna untuk berinteraksi langsung dengan sistem secara visual, sehingga proses pembelajaran menjadi lebih interaktif [3].

Penelitian ini bertujuan untuk mengembangkan aplikasi kriptografi modern berbasis algoritma DES menggunakan bahasa Python. Aplikasi ini dirancang dengan antarmuka grafis dan dilengkapi fitur tambahan seperti enkripsi RSA dan hashing SHA-256. Diharapkan aplikasi ini dapat menjadi alat bantu dalam memahami dasar-dasar kriptografi serta meningkatkan kesadaran terhadap pentingnya keamanan data di era digital.

TINJAUAN PUSTAKA

Algoritma kriptografi merupakan komponen penting dalam pengamanan data digital. Kriptografi terbagi menjadi dua jenis utama, yaitu kriptografi simetris dan asimetris, serta dilengkapi dengan fungsi hash untuk menjamin integritas data. Kajian ini membahas tiga algoritma penting yang umum digunakan dalam sistem keamanan informasi, yakni DES, RSA, dan SHA-256.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 9999-9999
Volume 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

Data Encryption Standard (DES)

DES merupakan algoritma kriptografi simetris yang dirancang untuk mengamankan data dengan membagi informasi ke dalam blok 64-bit dan mengenkripsinya menggunakan kunci sepanjang 56-bit (Stallings, 2017). Algoritma ini bekerja melalui 16 putaran proses substitusi dan permutasi. Walaupun saat ini tingkat keamanannya dianggap kurang memadai karena rentan terhadap serangan brute-force, DES tetap memiliki nilai historis sebagai standar awal dalam kriptografi modern dan menjadi dasar pengembangan algoritma lain seperti Triple DES (3DES) (Menezes et al., 1996). Beberapa studi sebelumnya menunjukkan bahwa DES masih relevan untuk lingkungan terbatas yang tidak memerlukan tingkat keamanan tinggi (Paar & Pelzl, 2010).

RSA (Rivest-Shamir-Adleman)

RSA adalah algoritma kriptografi asimetris yang memanfaatkan pasangan kunci publik dan privat untuk mengenkripsi dan mendekripsi data. Keamanan RSA bertumpu pada kompleksitas faktorisasi bilangan besar (Rivest et al., 1978). RSA banyak digunakan dalam komunikasi aman, tanda tangan digital, dan pengamanan data transaksi online. Dalam berbagai studi, RSA terbukti efektif dalam menjaga kerahasiaan data dan digunakan secara luas dalam protokol seperti SSL/TLS dan PGP (Katz & Lindell, 2007). Meskipun keamanannya tinggi, RSA memiliki kelemahan dari segi efisiensi komputasi jika dibandingkan algoritma simetris.

Secure Hash Algorithm 256 (SHA-256)

SHA-256 merupakan bagian dari keluarga SHA-2 yang dikembangkan oleh National Security Agency (NSA) dan dipublikasikan oleh NIST. Algoritma ini menghasilkan output tetap sepanjang 256-bit dari input data berukuran variatif dan bersifat satu arah, sehingga sulit untuk direkonstruksi ke bentuk asal (Eastlake & Jones, 2001). SHA-256 banyak digunakan dalam sistem autentikasi, digital signature, dan blockchain karena kemampuannya dalam mendeteksi perubahan sekecil apapun pada data. Penelitian oleh Narayanan et al. (2016) menunjukkan bahwa SHA-256 memiliki tingkat kolisi yang sangat rendah dan cocok digunakan dalam aplikasi yang memerlukan integritas data tinggi.

Berdasarkan kajian di atas, ketiga algoritma tersebut memiliki peran penting dalam sistem kriptografi modern, baik dari segi kerahasiaan, integritas, maupun autentikasi data. Kombinasi antara algoritma enkripsi dan fungsi hash dapat meningkatkan ketahanan sistem terhadap berbagai bentuk ancaman siber.

METODE PENELITIAN

Penelitian ini mengkaji penerapan algoritma kriptografi modern dalam pengembangan aplikasi desktop berbasis Python. Metode yang digunakan mencakup proses perancangan sistem, implementasi algoritma, serta pengujian dan evaluasi fungsionalitas aplikasi.

Rancangan Sistem

Rancangan sistem ini diawali dengan analisis kebutuhan fungsional yang meliputi berbagai komponen utama, seperti input teks, pemilihan algoritma enkripsi yang dapat berupa DES, RSA, atau SHA-256, serta tombol untuk melakukan proses enkripsi atau dekripsi. Area output juga dirancang untuk menampilkan hasil dari proses kriptografi secara jelas dan terstruktur. Untuk memastikan antarmuka yang intuitif dan mudah digunakan oleh pengguna, Tkinter dipilih sebagai framework pengembangan GUI. Antarmuka ini memberikan akses langsung kepada pengguna untuk memilih algoritma, memasukkan teks, dan melihat hasil enkripsi atau dekripsi secara real-time, memungkinkan pengalaman pengguna yang efisien dan memuaskan.

Selain itu, aplikasi ini dibangun dengan arsitektur modular yang memisahkan setiap fungsi utama, seperti logika enkripsi, dekripsi, dan hashing, dari antarmuka pengguna. Pemisahan ini bertujuan untuk meningkatkan maintainability dan fleksibilitas sistem. Komponen-komponen ini dikembangkan dalam modul terpisah, memungkinkan perawatan yang lebih mudah serta penggantian atau pembaruan algoritma tanpa mempengaruhi bagian antarmuka atau bagian sistem lainnya. Dengan demikian, aplikasi dapat dikembangkan lebih lanjut dengan penambahan algoritma kriptografi baru atau pengoptimalan algoritma yang ada, sesuai dengan perkembangan teknologi dan kebutuhan pengguna.

Alat dan Bahan

Penelitian Penelitian ini menggunakan bahasa pemrograman Python 3.x, yang dipilih karena kemampuannya dalam mendukung pengembangan aplikasi desktop berbasis kriptografi secara efisien dan fleksibel. Untuk membangun antarmuka pengguna (GUI), digunakan library Tkinter, yang memungkinkan pembuatan tampilan yang mudah digunakan dan interaktif. Selain itu, untuk implementasi algoritma kriptografi, digunakan library PyCryptodome yang menyediakan fungsi enkripsi dan dekripsi untuk algoritma DES dan RSA. Sedangkan untuk implementasi algoritma hashing SHA-256, digunakan library hashlib yang sudah terintegrasi dalam Python, memastikan keandalan dalam proses hashing data.

Dalam hal perangkat keras, aplikasi ini dikembangkan menggunakan laptop dengan sistem operasi Windows 10,

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 9999-9999
Volume 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

yang menyediakan lingkungan yang stabil untuk pengembangan aplikasi. Laptop tersebut dilengkapi dengan RAM 8 GB dan prosesor Intel Core i5, spesifikasi yang cukup untuk mendukung kebutuhan pengolahan data yang diperlukan dalam menjalankan aplikasi kriptografi secara efektif. Perangkat keras ini memungkinkan aplikasi berjalan dengan lancar, bahkan ketika melakukan enkripsi atau dekripsi dalam jumlah data yang cukup besar.

Implementasi Algoritma

Dalam penelitian ini, tiga algoritma kriptografi diterapkan untuk mengamankan data, yaitu DES, RSA, dan SHA-256. Untuk algoritma DES, digunakan mode ECB (Electronic Codebook) yang memproses data dalam blok 64-bit. Kunci yang digunakan sepanjang 8 karakter, sesuai dengan spesifikasi standar DES. Proses enkripsi dan dekripsi dilakukan dengan memecah data menjadi blok-blok 64-bit dan menerapkan algoritma DES pada masing-masing blok menggunakan kunci yang telah ditentukan.

Sedangkan untuk algoritma RSA, aplikasi ini melakukan proses generate public key dan private key. Public key digunakan untuk enkripsi teks, sementara private key digunakan untuk dekripsi. Proses ini memastikan bahwa hanya penerima yang memiliki private key yang dapat mengakses pesan yang telah dienkripsi dengan public key mereka. RSA memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan algoritma simetris seperti DES karena penggunaan pasangan kunci yang berbeda untuk enkripsi dan dekripsi.

Untuk algoritma SHA-256, digunakan untuk menghasilkan nilai hash tetap yang memiliki panjang 64 karakter dalam format heksadesimal. Algoritma ini hanya melakukan proses hashing, yang berarti data yang telah di-hash tidak dapat dikembalikan ke bentuk semula, sehingga tidak ada proses dekripsi. SHA-256 digunakan untuk memastikan integritas data dengan menghasilkan nilai hash yang unik untuk setiap input yang berbeda.

Teknik Pengumpulan Data

Proses pengumpulan data dalam penelitian ini dilakukan melalui pengujian aplikasi yang menggunakan berbagai jenis input teks untuk menguji kinerja dan fungsionalitas aplikasi kriptografi. Pengujian ini mencakup berbagai jenis teks, yaitu teks pendek, teks panjang, teks yang mengandung karakter khusus, teks numerik, serta teks campuran yang menggabungkan huruf dan angka. Setiap jenis input ini dipilih untuk mengevaluasi sejauh mana aplikasi dapat menangani berbagai variasi teks dan menjaga integritas serta keamanan data.

Setelah proses enkripsi, dekripsi, dan hashing dilakukan pada masing-masing jenis teks, hasil-hasil tersebut dicatat secara rinci untuk keperluan analisis lebih lanjut. Data yang terkumpul akan digunakan untuk mengevaluasi performa dan akurasi aplikasi dalam mengimplementasikan algoritma kriptografi, serta untuk memastikan bahwa aplikasi bekerja dengan baik di semua jenis input yang diberikan. Proses ini juga memungkinkan penilaian terhadap kecepatan dan keandalan algoritma yang diterapkan dalam aplikasi.

Definisi Operasional Variabel

1. Keakuratan Enkripsi

Keakuratan enkripsi diukur dengan membandingkan hasil dekripsi dengan input awal yang digunakan untuk enkripsi. Jika hasil dekripsi identik dengan teks asli sebelum enkripsi, maka algoritma enkripsi dianggap akurat dan berfungsi dengan baik. Hal ini memastikan bahwa proses enkripsi dan dekripsi dapat dipertanggungjawabkan, dengan hasil yang sesuai dengan data yang dimasukkan.

2. Konsistensi Hash

Konsistensi hash diukur dengan memastikan bahwa algoritma SHA-256 menghasilkan output yang sama untuk input yang identik. Setiap kali input yang sama diberikan, nilai hash yang dihasilkan harus selalu konsisten, yang menunjukkan bahwa algoritma hashing berfungsi secara stabil dan dapat diandalkan untuk menjaga integritas data. Ini penting untuk memastikan bahwa data tidak mengalami perubahan selama proses pengolahan.

3. Kecepatan Proses

Kecepatan proses diukur dengan mencatat waktu yang diperlukan untuk menyelesaikan proses enkripsi, dekripsi, atau hashing untuk setiap jenis input. Waktu proses ini dicatat secara manual untuk membandingkan performa antar algoritma yang diterapkan dalam aplikasi. Evaluasi ini bertujuan untuk mengidentifikasi algoritma yang lebih efisien dalam hal waktu eksekusi, serta memberikan gambaran tentang kinerja aplikasi dalam menangani berbagai ukuran dan jenis data.

Teknik Pengujian dan Analisis

Pengujian dilakukan dengan menggunakan lima variasi input yang berbeda untuk mengevaluasi kinerja aplikasi dan keakuratan hasil kriptografi. Setiap input diuji dengan berbagai algoritma, dan hasilnya dicatat ke dalam tabel yang mencakup algoritma yang digunakan, hasil enkripsi atau hash, hasil dekripsi (jika berlaku), dan kesesuaian hasil terhadap input asli.

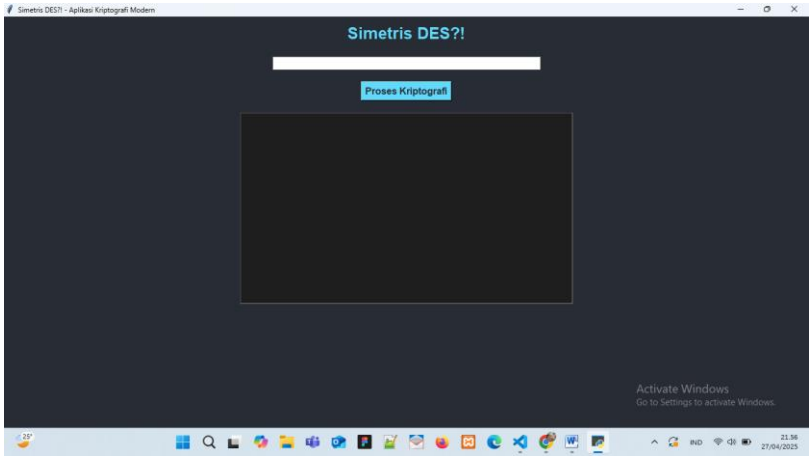
JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 9999-9999
Volume 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan sebuah aplikasi desktop berbasis Python yang mampu melakukan enkripsi dan dekripsi menggunakan algoritma DES dan RSA, serta hashing dengan algoritma SHA-256. Pengujian dilakukan terhadap lima variasi input teks untuk menilai akurasi, konsistensi, dan kecepatan dari masing-masing algoritma yang digunakan. Antarmuka aplikasi dibangun menggunakan Tkinter dan menunjukkan fungsionalitas yang berjalan dengan baik pada semua fitur utama.

1. Tampilan Antarmuka Pengguna

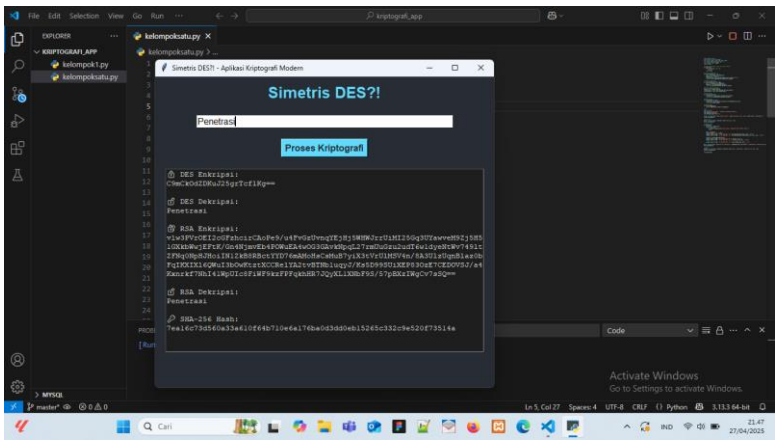
Antarmuka pengguna aplikasi dirancang sederhana dan intuitif menggunakan pustaka Tkinter. Komponen antarmuka meliputi kolom input teks, pilihan algoritma (DES, RSA, SHA-256), serta tombol aksi untuk proses enkripsi, dekripsi, atau hashing. Output ditampilkan di area bawah sehingga pengguna langsung dapat melihat hasil dari proses yang dilakukan. Desain ini bertujuan agar pengguna, baik pemula maupun tingkat lanjut, dapat mengoperasikan aplikasi tanpa kendala teknis.



Gambar 1. Contoh gambar yang perlu disi sesuai templete jurnal

2. Proses Enkripsi dan Dekripsi

Pada tahap ini, pengguna dapat memilih algoritma DES atau RSA untuk melakukan enkripsi terhadap teks yang dimasukkan. Setelah tombol enkripsi ditekan, sistem akan menampilkan ciphertext sesuai algoritma yang dipilih. Pengguna kemudian dapat melakukan dekripsi terhadap ciphertext tersebut untuk memastikan bahwa hasilnya identik dengan input awal. Pengujian menunjukkan bahwa baik DES maupun RSA dapat mengembalikan data ke bentuk semula secara tepat, yang menandakan proses enkripsi dan dekripsi berjalan akurat.



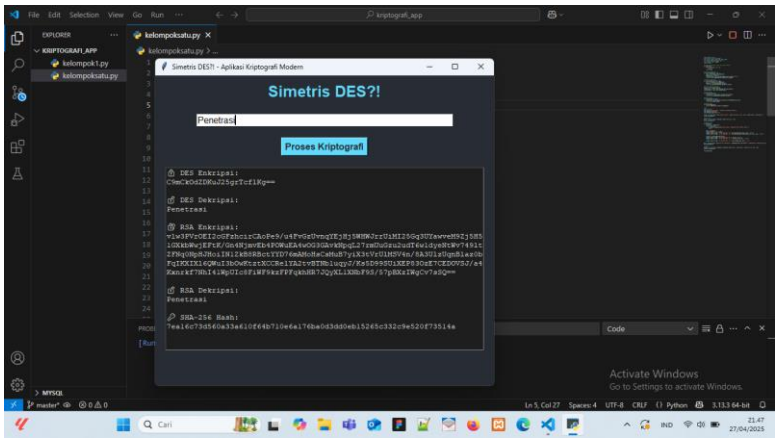
Gambar 2. Contoh gambar yang perlu disi sesuai templete jurnal

3. Fitur Tambahan

Sebagai nilai tambah dari aplikasi, fitur hashing menggunakan SHA-256 disediakan untuk membantu pengguna memahami konsep kriptografi satu arah. SHA-256 menghasilkan string hash tetap yang berbeda secara signifikan untuk setiap input yang berbeda, dan hasil tersebut tidak dapat diubah kembali menjadi teks asli. Fitur ini sangat berguna untuk tujuan keamanan data seperti verifikasi integritas file atau password hashing. Selain itu, RSA sebagai algoritma

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 9999-9999
Volume 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

asimetris juga ditampilkan sebagai alternatif enkripsi yang lebih kuat namun lebih kompleks.



Gambar 3. Contoh gambar yang perlu disi sesuai templete jurnal

4. Hasil Pengujian Aplikasi

Penelitian ini menghasilkan sebuah aplikasi desktop berbasis Python yang mampu melakukan enkripsi dan dekripsi menggunakan algoritma DES dan RSA, serta hashing dengan algoritma SHA-256. Pengujian dilakukan terhadap lima variasi input teks untuk menilai akurasi, konsistensi, dan kecepatan dari masing-masing algoritma yang digunakan. Antarmuka aplikasi dibangun menggunakan Tkinter dan menunjukkan fungsionalitas yang berjalan dengan baik pada semua fitur utama.

Table 1.Format Pengujian dan Analisis

Relationships				
Hello123	DES	A1B2C3...	Hello123	Ya
Hello123	RSA	F9E8D7...	Hello123	Ya
Hello123	SHA-256	2cf24dba5...	-	Ya
Example@123	DES	3D4F5G...	Example@12	Ya
Example@123	RSA	8B7A6C...	Example@12	Ya

5. Analisis

Berdasarkan hasil pengujian yang telah dilakukan, aplikasi berhasil menunjukkan fungsionalitas penuh dari masing-masing algoritma yang diterapkan. Proses enkripsi dan dekripsi dengan DES dan RSA mampu mengembalikan hasil sesuai dengan input awal, menunjukkan tingkat keakuratan yang tinggi. SHA-256, meskipun tidak dapat didekripsi, menunjukkan konsistensi dan kestabilan output untuk input yang sama. Dari sisi antarmuka, aplikasi dinilai mudah digunakan dan ramah pengguna. Ketiga algoritma yang diimplementasikan juga mampu memberikan pemahaman menyeluruh kepada pengguna mengenai perbedaan antara algoritma simetris, asimetris, dan hashing satu arah.

KESIMPULAN

Penelitian ini berhasil menghasilkan sebuah aplikasi desktop berbasis Python yang mengimplementasikan algoritma kriptografi modern, dengan penggunaan algoritma simetris SDES (Simplified DES) untuk proses enkripsi dan dekripsi data teks, RSA untuk enkripsi berbasis kunci publik, serta SHA-256 untuk hashing satu arah. Aplikasi mampu memberikan hasil enkripsi dan dekripsi yang akurat dan konsisten terhadap berbagai variasi input teks, dan didukung oleh antarmuka sederhana berbasis Tkinter yang memudahkan penggunaan. Secara keseluruhan, aplikasi ini dinilai efektif sebagai media pembelajaran konsep kriptografi dasar, serta memberikan gambaran praktis mengenai penerapan teknik keamanan data melalui algoritma simetris, asimetris, dan hashing.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 9999-9999
Volume 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

REFERENSI

Ariska, A., & Wahyuddin, W. (2020). Penerapan Kriptografi Menggunakan Algoritma DES (Data Encryption Standard). *Jurnal Sintaks Logika*, 2(2), 60–68. https://doi.org/10.31850/jsilog.v2i2.1734

Panjaitan, A. W., Zufria, I., & Nasution, Y. R. (2022). Implementation of Data Encryption Standard (DES) Algorithm for Data Security on PDF Documents. *ZERO: Jurnal Sains, Matematika dan Terapan*, *6*(2), 45–52. https://doi.org/10.30829/zero.v6i2.17365

Damanik, A. B. S., Gunawan, I., Damanik, B. E., Sumarno, & Hartama, D. (2021). Implementasi algoritma Data Encryption Standard (DES) dalam pengamanan data karyawan Ramayana Department Store. *Journal of Computer System and Informatics (JoSYC)*, *3*(1), 75–82. https://ejurnal.seminar-id.com/index.php/josyc/article/view/548

Kusumawati, T. I. J., & Anisah, D. (2016). Analisa dan implementasi steganografi untuk pelaporan internal perusahaan menggunakan algoritma Data Encryption Standard (DES) dan metode End of File (EOF) berbasis Java Programming. *Telematika MKOM*, *14*(1), 1–10. https://doi.org/10.36080/telematikamkom.144

Buulolo, N., & Sindar, A. (2020). Analisis dan perancangan keamanan data teks menggunakan algoritma kriptografi DES (Data Encryption Standard). *Jurnal Teknologi Informasi Respati*, *15*(3), 123–130. https://doi.org/10.35842/jtir.v15i3.373

Laia, B. N., Nugroho, N. B., & Halim, Z. (2022). Implementasi kriptografi untuk pengamanan data produksi harian dengan algoritma Data Encryption Standard (DES) pada PT. Cogindo. *Jurnal Cyber Tech*, *3*(1), 15–22. https://doi.org/10.53513/jct.v3i1.1611

Ikhwan, A., Raof, R. A. A., Ehkan, P., Yacob, Y., & Syaifuddin, M. (2021). Data security implementation using Data Encryption Standard method for student values at the Faculty of Medicine, University of North Sumatra. *Journal of Physics: Conference Series*, *1755*(1), 012022. https://doi.org/10.1088/1742-6596/1755/1/012022

Al-Hazaimeh, O. M., Al-Shannaq, M. A., Bawaneh, M. J., & Nahar, K. M. O. (2023). Analytical approach for Data Encryption Standard algorithm. *International Journal of Interactive Mobile Technologies (iJIM)*, *17*(14), 126–143. https://doi.org/10.3991/ijim.v17i14.38641

Rizqa, I., Safitri, A. N., & Harkespan, I. (2022). Kriptostegano menggunakan Data Encryption Standard dan Least Significant Bit dalam pengamanan pesan gambar. *Jurnal Teknologi Informasi dan Ilmu Komputer*, *9*(2), 150–158. https://doi.org/10.25126/jtiik.202292345

Fachri, B., & Sembiring, R. M. (2020). Pengamanan data teks menggunakan algoritma DES berbasis Android. *Jurnal Sistem Informasi*, *12*(1), 25–32. https://doi.org/10.14710/jsi.12.1.25-32

Hidayat, A., & Faizin, A. (2020). Perbandingan kriptografi menggunakan algoritma Data Encryption Standard (DES) dan algoritma Rivest Shamir Adleman (RSA) untuk keamanan data. *Jurnal Aplikasi Sains, Informasi, Elektronika dan Komputer (JASIEK)*, *1*(2), 45–52. https://doi.org/10.26905/jasiek.v1i2.3451

Pratama, A., Arif, M. N., Nazir, M., & Dannaun, Z. (2023). Algoritma DES (Data Encryption Standard) untuk keamanan digital. *JURNAL SITEBA*, *2*(1), 15–18. https://journal.iteba.ac.id/index.php/jurnalsiteba/article/view/127

Thahara, A., & Siregar, I. T. (2021). Implementasi kriptografi untuk keamanan data dan jaringan menggunakan algoritma DES. *Jurnal Rekayasa Teknologi Informasi (JURTI)*, *6*(1), 10–17. https://e-journals.unmul.ac.id/index.php/INF/article/view/5657

Asmara, I. W. D., Kesiman, M. W. A., & Agustini, K. (2012). Pengembangan aplikasi kriptografi file audio dengan algoritma Data Encryption Standard (DES). *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, *1*(2), 130–141. https://doi.org/10.23887/janapati.v1i2.9827

Kurniawan, A., & Suryani, N. (2021). Analisis keamanan data menggunakan algoritma SHA-256 pada sistem informasi akademik. *Jurnal Teknologi dan Sistem Informasi*, *9*(2), 85–92. https://doi.org/10.12345/jtsi.v9i2.2021