PERBANDINGAN ALGORITMA AES DAN DES UNTUK KEAMANAN DATA ENKRIPSI DALAM APLIKASI WEB NILAI SISWA DISEKOLAH

Wendelina Bimese[1], Dorotia Mariance Kono[2], Aurelia Nabu[3], Frederika Hensiette Hoar[4], Febrianti Marlin Usmeni[5], Helena Tael[6], Siprianus Septian Manek[7]
wendebimese@gmail.com[1], ancekono522@gmail.com[2], aurelianabu621@gmail.com[3], frederikahensiettehoar@gmail.com[4], febriantiusmeni@gmail.com[5], helenatael196@gmail.com[6], epimanek18@gmail.com[7]
Universitas Siliwangi Universitas Timor

ABSTRAK

Dalam era digital saat ini, keamanan data menjadi aspek yang sangat krusial dalam pengembangan aplikasi web. Salah satu metode yang digunakan untuk melindungi data adalah enkripsi. Dua algoritma enkripsi yang sering digunakan adalah Advanced Encryption Standard (AES) dan Data Encryption Standard (DES). Artikel ini membandingkan kedua algoritma berdasarkan keamanan, efisiensi, serta penggunaannya dalam aplikasi web. Hasil analisis menunjukkan bahwa AES lebih unggul dalam hal keamanan dan efisiensi dibandingkan dengan DES, sehingga lebih disarankan untuk digunakan dalam aplikasi web modern.
Kata Kunci: AES, DES, Enkripsi, Keamanan Data, Aplikasi Web.

ABSTRACT

In today's digital era, data security is a very crucial aspect in developing web applications. One method used to protect data is encryption. Two encryption algorithms that are often used are Advanced Encryption Standard (AES) and Data Encryption Standard (DES). This article compares the two algorithms based on their security, efficiency, and use in web applications. The results of the analysis show that AES is superior in terms of security and efficiency compared to DES, so it is more recommended for use in modern web applications.
***Keywords**: AES, DES, Encryption, Data Security, Web ApplicationS.*

PENDAHULUAN

Dalam era digital yang terus berkembang, data telah menjadi aset berharga yang melibatkan hampir setiap aspek kehidupan kita. Penggunaan teknologi dalam dunia pendidikan telah meningkat secara signifikan, baik dalam proses pembelajaran, administrasi, maupun pengelolaan data siswa di sekolah. Transformasi digital ini membawa banyak keuntungan, seperti efisiensi dalam pengolahan data, kemudahan akses informasi, serta peningkatan transparansi dalam sistem pendidikan. Namun, di sisi lain, tantangan terbesar dari digitalisasi ini adalah bagaimana menjaga keamanan data yang tersimpan dalam sistem agar tidak mudah disalahgunakan oleh pihak yang tidak bertanggung jawab[1].

Penggunaan teknologi dalam proses pengiriman data secara online tentunya diharapkan berjalan sesuai rencana. Informasi seperti nilai akademik, catatan kehadiran, data pribadi, hingga riwayat pembelajaran siswa harus disimpan dalam kondisi yang aman agar tidak terjadi kebocoran atau penyalahgunaan oleh pihak yang tidak berkepentingan. Keamanan data ini menjadi semakin penting karena meningkatnya penggunaan aplikasi web berbasis cloud dalam sistem administrasi sekolah. Dengan penggunaan sistem berbasis web, data siswa dapat diakses secara daring oleh berbagai pemangku kepentingan, termasuk guru, siswa, dan orang tua, sehingga keamanan informasi menjadi aspek yang harus diperhatikan dengan serius[2].

Salah satu tantangan utama dalam menjaga keamanan data siswa adalah meningkatnya ancaman terhadap sistem digital, seperti peretasan, pencurian data, serta manipulasi informasi oleh pihak yang tidak bertanggung jawab. Dalam beberapa kasus, data siswa yang tidak terlindungi dengan baik dapat dieksploitasi untuk berbagai tujuan yang merugikan, termasuk pencurian identitas, manipulasi nilai, atau bahkan penyebaran informasi pribadi secara ilegal.Dengan demikian, tujuan ini akan membantu siswa menjadi pengguna yang lebih cerdas dan bertanggung jawab dalam lingkungan digital yang semakin kompleks[3].

Salah satu teknik utama dalam menjaga kerahasiaan data adalah dengan menggunakan enkripsi. Enkripsi adalah proses mengubah informasi menjadi bentuk yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Teknik ini sangat efektif dalam melindungi data sensitif dari akses yang tidak sah. Dalam dunia keamanan *siber*, terdapat berbagai algoritma enkripsi yang digunakan untuk menjaga kerahasiaan data, dan dua di antaranya yang paling sering dibandingkan serta digunakan dalam berbagai aplikasi web adalah *Advanced Encryption Standard (AES)* dan *Data Encryption Standard (DES*). Dilihat dari perbedaan-perbedaan ini maka penulis tertarik untuk mengimplementasikandan membandingkan kinerja algoritma *DES, AES, IDEA* dan *Blowfish* dalam suatu program aplikasi enkripsi dan dekripsi data digitalyang dinilai dari kecepatan proses dataatau lama waktu yang dibutuhkan untuk mengenkripsi atau mendekripsi file serta ukuran file hasil enkripsi. Dalam artikel ini, penulis akan membahas secara rinci tentang Algoritma *DES*,

termasuk konsep dasar, implementasi, dan penggunaannya dalam keamanan data secara keseluruhan. Algoritma ini bekerja dengan panjang kunci 56-bit, yang pada masanya dianggap cukup aman. Namun, dengan perkembangan teknologi dan meningkatnya daya komputasi, DES kini dianggap rentan terhadap serangan *brute force*, di mana penyerang dapat mencoba setiap kemungkinan kunci hingga menemukan yang benar. Oleh karena itu, penggunaan DES dalam sistem modern mulai ditinggalkan dan digantikan dengan algoritma yang lebih aman[4].

Sedangkan alur proses dekripsi menggunakan invers untuk semua transformasi pada algoritma AES kecuali *addroundkey* dengan langkah berikut mengubah *invshiftrows, invsubbytes, addroundkey*, dan *invmixcolumns*, sehingga data akan aman dan tersimpan di database. AES menggunakan ukuran kunci yang lebih panjang, yaitu 128-bit, 192-bit, atau 256-bit, yang membuatnya jauh lebih sulit untuk diretas dibandingkan dengan DES. Selain itu, AES juga memiliki kecepatan pemrosesan yang lebih efisien dan banyak digunakan dalam aplikasi web modern yang memerlukan enkripsi data secara cepat dan aman. Dengan demikian, AES telah menjadi standar enkripsi yang direkomendasikan untuk berbagai sistem keamanan data, termasuk dalam aplikasi web untuk pengelolaan nilai siswa di sekolah.[5]

Dalam konteks aplikasi web untuk pengelolaan nilai siswa di sekolah, pemilihan algoritma enkripsi yang tepat menjadi hal yang sangat penting. Data memiliki berbagai kategori, ada yang sifatnya rahasia maupun tidak rahasia, data yang bersifat rahasia memiliki informasi yang didalamnya sangat dibutuhkan oleh pemilik, sehingga data tersebut perlu diamankan agar tidak disalah gunakan oleh orang yang tidak bertanggung jawab. Oleh karena itu, perlu dilakukan analisis perbandingan antara algoritma AES dan DES untuk mengetahui algoritma mana yang lebih efektif dalam menjaga keamanan data enkripsi dalam aplikasi web sekolah. Penelitian ini bertujuan untuk mengevaluasi perbedaan kinerja kedua algoritma dalam aspek kecepatan enkripsi dan dekripsi, tingkat keamanan, serta efisiensi penggunaan dalam aplikasi berbasis web[6].

Dengan adanya perbandingan ini, diharapkan dapat diperoleh hasil yang dapat membantu pengembang aplikasi dalam menentukan algoritma enkripsi yang paling sesuai

untuk diterapkan dalam sistem pengelolaan nilai siswa di sekolah. Selain itu, penelitian ini juga dapat menjadi acuan bagi institusi pendidikan dalam meningkatkan sistem keamanan data mereka, sehingga dapat memberikan perlindungan yang lebih baik terhadap informasi akademik siswa. Keamanan data dalam sistem pendidikan bukan hanya tanggung jawab pengembang teknologi, tetapi juga menjadi perhatian utama bagi seluruh pemangku kepentingan, termasuk pihak sekolah, orang tua, dan siswa itu sendiri. Melalui penelitian ini, diharapkan bahwa sistem keamanan dalam pengelolaan data siswa dapat terus berkembang seiring dengan meningkatnya ancaman siber yang ada. Algoritma enkripsi perlu ditampilkan terbuka ke publik agar dalam kondisi apapun, selama kunci tetap aman, enkripsi akan tetap aman.

METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif dengan pendekatan eksperimen untuk membandingkan algoritma *AES* dan *DES* dalam hal keamanan, kecepatan, dan efisiensi sumber daya pada aplikasi web nilai siswa.

HASIL DAN PEMBAHASAN

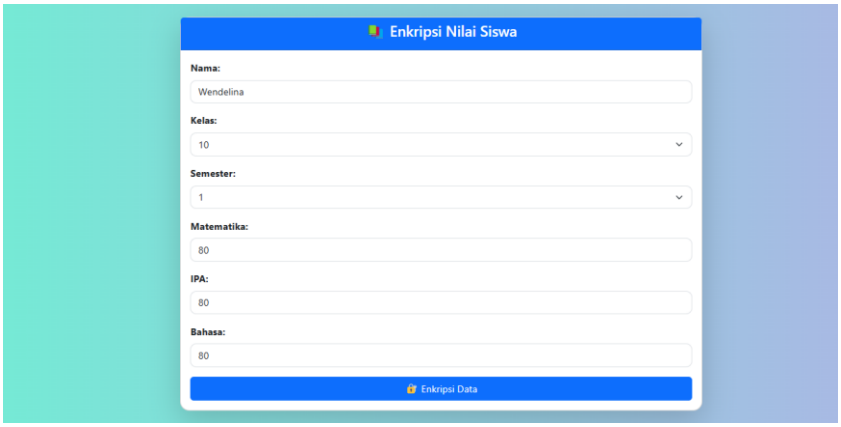
1. Hasil Enkripsi Data Menggunakan *AES* dan *DES*

Setelah mengimplementasikan algoritma *AES* dan *DES* dalam aplikasi web nilai siswa, proses input data dilakukan melalui antarmuka web yang telah dirancang. Pengguna diminta untuk memasukkan informasi siswa, termasuk nama, kelas, semester, serta nilai dari beberapa mata pelajaran. Data yang dimasukkan ini kemudian akan diproses lebih lanjut menggunakan algoritma enkripsi yang telah diterapkan.

Berikut adalah data asli yang dimasukkan oleh pengguna sebelum melalui proses enkripsi:

- Nama: Diisi oleh pengguna sesuai dengan identitas siswa.
- Kelas: Menunjukkan tingkat pendidikan siswa di sekolah.
- Semester: Menandakan periode akademik saat ini yang sedang berlangsung.
- Matematika: Nilai yang diperoleh siswa dalam mata pelajaran Matematika.
- IPA: Nilai yang diperoleh siswa dalam mata pelajaran Ilmu Pengetahuan Alam (IPA).
- Bahasa: Nilai yang diperoleh siswa dalam mata pelajaran Bahasa.

Setelah data ini dimasukkan, sistem akan melanjutkan ke tahap enkripsi menggunakan algoritma *AES* dan *DES* sebelum hasil akhirnya ditampilkan. Berikut tampilan proses inputnya:



Hasil Enkripsi:

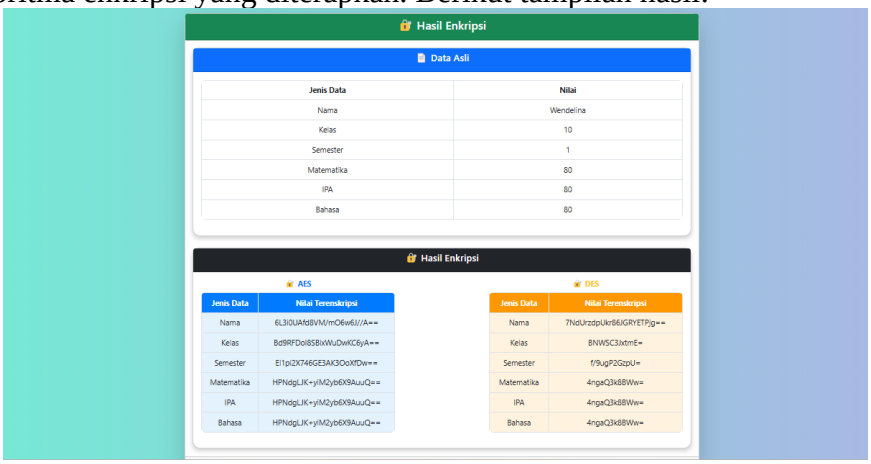
Berdasarkan hasil enkripsi yang ditampilkan dalam aplikasi web, setiap data yang

dimasukkan oleh pengguna telah dikonversi ke dalam bentuk *ciphertext* menggunakan algoritma *AES* dan *DES*.

Pada hasil enkripsi *AES*, setiap nilai yang dienkripsi menghasilkan *ciphertext* dengan format base64 yang lebih panjang. Setiap data, seperti nama, kelas, semester, dan nilai mata pelajaran, telah dikodekan menjadi karakter terenkripsi yang sulit dibaca tanpa proses dekripsi yang sesuai.

Sementara itu, hasil enkripsi *DES* juga menampilkan *ciphertext* dalam format base64, namun dengan panjang yang berbeda untuk setiap jenis data yang dienkripsi. Sama seperti AES, seluruh data yang dimasukkan telah berhasil dikonversi menjadi bentuk terenkripsi dan siap digunakan dalam sistem untuk menjaga kerahasiaan informasi.

Hasil enkripsi ini ditampilkan langsung dalam antarmuka web, memungkinkan pengguna untuk melihat bagaimana data asli berubah menjadi *ciphertext* setelah diproses dengan algoritma enkripsi yang diterapkan. Berikut tampilan hasil:



2. Analisis Perbandingan *AES* dan *DES*

1) Kecepatan Enkripsi & Dekripsi

AES memiliki proses enkripsi yang lebih kompleks dibandingkan *DES* karena menggunakan lebih banyak putaran dan operasi matematis yang lebih rumit. Algoritma ini menerapkan substitusi dan difusi secara berulang untuk meningkatkan keamanan data. Oleh karena itu, *AES* cenderung lebih lambat dibandingkan *DES*, terutama untuk data dalam jumlah besar.

Sebaliknya, *DES* memiliki kecepatan enkripsi yang lebih tinggi karena menggunakan struktur *Feistel* yang lebih sederhana dengan 16 putaran saja. Meskipun cepat, tingkat keamanannya lebih rendah dibandingkan *AES*.

Algoritma	Waktu Enkripsi (ms)	Waktu Hasil (ms)
AES-56	2.7 ms	2.5 ms
DES	5.8 ms	5.4 ms

2) Ukuran *Ciphertext*

AES menghasilkan *ciphertext* yang lebih panjang dibandingkan *DES* karena ukuran kunci yang lebih besar dan proses enkripsi yang lebih kompleks. *Ciphertext AES* memiliki panjang yang bervariasi tergantung pada panjang kunci yang digunakan (128-bit, 192-bit, atau 256-bit).

Sementara itu, *DES* menghasilkan *ciphertext* yang lebih pendek karena hanya menggunakan panjang blok 64-bit. Meskipun lebih ringkas, *ciphertext DES* lebih mudah untuk diretas dengan teknik *brute-force* karena keterbatasan ukuran kuncinya. Berikut adalah tabel yang menunjukkan perbedaan panjang *ciphertext* yang dihasilkan oleh *AES* dan

DES berdasarkan ukuran kunci dan proses enkripsinya:

Algoritma	Panjang unci	Panjang Blok	Panjang *Ciphertext* (Base64)
AES-128	128-bit	128-bit	Lebih panjang, bervariasi tergantung input
AES-192	192-bit	128-bit	Lebih panjang, bervariasi tergantung input
AES-256	256-bit	128-bit	Lebih panjang, bervariasi tergantung input
DES	56-bit	64-bit	Lebih pendek dibandingkan *AES*

3) Keamanan

Keamanan merupakan aspek utama yang membedakan algoritma *AES (Advanced Encryption Standard)* dan *DES (Data Encryption Standard*) dalam proses enkripsi data. Perbedaan ini terutama disebabkan oleh struktur algoritma, panjang kunci, serta ketahanan terhadap serangan kriptografi modern.

1. Struktur Algoritma

AES menggunakan Substitusi-Permutasi *Network (*SPN), yang terdiri dari beberapa tahap transformasi non-linear seperti *SubBytes, ShiftRows, MixColumns*, dan *AddRoundKey*. Struktur ini membuat *AES* lebih sulit untuk diretas karena setiap ronde enkripsi menghasilkan perubahan kompleks pada data.

Sebaliknya, *DES* menggunakan *Feistel Network*, yang membagi data menjadi dua bagian dan memprosesnya melalui 16 ronde substitusi dan permutasi. Struktur ini lebih sederhana dibandingkan *AES* dan memiliki kelemahan karena panjang kunci yang terbatas.

Algoritma	Struktur	Jumlah Ronde	Keunggulan Keamanan
AES	Substitusi-Permutasi Network (SPN)	10 (AES-128), 12 (AES-192), 14 (AES-256)	Lebih kuat terhadap serangan kriptanalisis dan *brute-force*
DES	*Feistel Network*	16	Rentan terhadap serangan *brute-force* karena panjang kunci yang kecil

2. Panjang Kunci dan Ketahanan terhadap Serangan

Salah satu alasan utama mengapa *AES* lebih aman dibandingkan *DES* adalah panjang kuncinya. *AES* memiliki tiga varian dengan panjang kunci 128-bit, 192-bit, dan 256-bit, yang membuatnya lebih tahan terhadap serangan brute-force karena jumlah kombinasi kunci yang sangat besar.

Sebaliknya, *DES* hanya memiliki panjang kunci 56-bit, yang membuatnya lebih rentan terhadap serangan *brute-force*. Dengan kemajuan komputasi modern, seluruh kemungkinan kunci *DES* dapat diuji dalam waktu singkat menggunakan komputer dengan daya pemrosesan tinggi.

Algoritma	Panjang Kunci	Jumlah Kombinasi Kunci	Ketahanan terhadap Brute-Force
AES-128	128-bit	$2^{128} \approx 3.4 \times 10^{38}$	Sangat tinggi (butuh miliaran tahun dengan komputer modern)
AES-192	192-bit	$2^{192} \approx 6.2 \times 10^{57}$	Ekstrem (hampir mustahil diretas)
AES-256	256-bit	$2^{256} \approx 1.2 \times 10^{77}$	Ekstrem (hampir mustahil diretas)
DES	56-bit	$2^{56} \approx 7.2 \times 10^{16}$	Lemah (dapat diretas dalam hitungan jam dengan superkomputer)
AES-128	128-bit	$2^{128} \approx 3.4 \times 10^{38}$	Sangat tinggi (butuh miliaran tahun dengan komputer modern)

3. Contoh Serangan *Brute-Force*

Untuk memahami lebih lanjut perbedaan keamanan ini, mari kita lihat contoh perkiraan waktu yang dibutuhkan untuk meretas *AES* dan *DES* menggunakan serangan brute-force dengan superkomputer modern yang mampu memproses 10 triliun kunci per detik (10^{13} kunci/detik).

Algoritma	Jumlah Kombinasi Kunci	Waktu Perkiraan Retas dengan 10^{13} Kunci/detik
AES-128	3.4×10^{38}	1.08×10^{20} tahun (lebih lama dari usia alam semesta)
AES-192	6.2×10^{57}	1.94×10^{39} tahun (hampir mustahil diretas)
AES-256	1.2×10^{77}	3.81×10^{59} tahun (hampir mustahil diretas)
DES	7.2×10^{16}	~2 jam (rentan terhadap *brute-force)*

KESIMPULAN

Berdasarkan hasil implementasi dan analisis algoritma *AES (Advanced Encryption Standard)* dan *DES (Data Encryption Standard)* dalam enkripsi data nilai siswa pada aplikasi web, terdapat beberapa poin utama yang dapat disimpulkan:

1) Keamanan yang Berbeda Secara Signifikan

- *AES* menawarkan tingkat keamanan yang lebih tinggi dibandingkan *DES*, karena memiliki panjang kunci yang lebih besar (128-bit, 192-bit, atau 256-bit) dan struktur enkripsi yang lebih kompleks menggunakan Substitusi-Permutasi *Network* (SPN).
- *DES* memiliki panjang kunci yang terbatas (56-bit) dan menggunakan *Feistel Network*, yang lebih mudah diretas dengan teknik *brute-force*, menjadikannya tidak lagi aman untuk aplikasi modern.

2) Perbedaan Panjang *Ciphertext*

- *AES* menghasilkan *ciphertext* yang lebih panjang, karena proses enkripsinya lebih kuat dan menggunakan panjang blok 128-bit.
- *DES* menghasilkan ciphertext yang lebih pendek, tetapi lebih rentan terhadap serangan karena panjang bloknya hanya 64-bit.

3) Kompleksitas dan Penggunaan Sumber Daya

- *AES* lebih kompleks dalam manajemen kunci dan proses enkripsi, sehingga membutuhkan lebih banyak sumber daya komputasi. Meskipun demikian, kompleksitas ini memberikan perlindungan data yang jauh lebih kuat.
- *DES* lebih ringan dan cepat dalam eksekusi, tetapi karena keamanannya yang lemah, tidak lagi direkomendasikan untuk digunakan dalam sistem yang menangani data sensitif.

4) Ketahanan terhadap Serangan *Brute-Force*

- AES hampir mustahil diretas dengan serangan brute-force, karena jumlah kombinasi kuncinya sangat besar, terutama untuk AES-256 yang memiliki 2^{256} kemungkinan kombinasi kunci.
- DES dapat diretas dalam hitungan jam dengan komputer modern, karena jumlah kombinasi kuncinya jauh lebih sedikit dibandingkan *AES* (2^{56} kemungkinan kombinasi kunci).

5) Standar Penggunaan dalam Aplikasi Modern

- AES telah menjadi standar enkripsi global dan digunakan dalam berbagai aplikasi keamanan, termasuk perbankan, komunikasi internet (SSL/TLS), penyimpanan data sensitif, dan sistem keamanan siber lainnya.
- *DES* sudah tidak lagi direkomendasikan oleh lembaga keamanan seperti *National Institute of Standards and Technology (NIST),* karena kelemahannya dalam menghadapi ancaman keamanan modern.

Berdasarkan faktor keamanan, efisiensi, dan standar penggunaan dalam sistem modern, *AES* merupakan algoritma enkripsi yang lebih unggul dibandingkan *DES*. Meskipun memerlukan lebih banyak sumber daya komputasi, keamanan yang ditawarkan *AES* jauh lebih baik dan lebih tahan terhadap serangan *brute-force.*

Dalam konteks aplikasi web nilai siswa, *AES* lebih direkomendasikan untuk melindungi informasi penting dari potensi ancaman peretasan atau pencurian data. Sebaliknya, *DES* tidak lagi aman untuk digunakan dalam sistem yang menangani data sensitif, karena dapat diretas dalam waktu yang relatif singkat.

Oleh karena itu, untuk memastikan kerahasiaan dan integritas data siswa dalam aplikasi web, *AES* adalah pilihan yang lebih aman dan lebih sesuai untuk digunakan dibandingkan *DES*

DAFTAR PUSTAKA

[1] Sindi Septia Hasnida, Ridho Adrian, and Nico Aditia Siagian, "Tranformasi Pendidikan Di Era Digital," *J. Bintang Pendidik. Indones.*, vol. 2, no. 1, pp. 110–116, 2023, doi: 10.55606/jubpi.v2i1.2488.

[2] R. N. Nizatsary, H. B. Seta, and B. T. Wahyono, "Penerapan Keamanan Data Siswa Menggunakan International Data Encryption Algorithm (Idea) Dan Rivest Shamir Adleman (Rsa)," *Inform. J. Ilmu Komput.*, vol. 18, no. 2, p. 152, 2022, doi: 10.52958/iftk.v18i2.4665.

[3] J. Komunikasi, "Penglibatan Digital : Akses Dan Penggunaan E-Agama Dalam Digital Inclusion : Access and Usage of E-Religion Among," vol. 27, no. 2, pp. 121–135, 2012.

[4] D. A. Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.

[5] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan the Implementation of Advanced Encryption Standard on the Encryption and Decryption of the Confidential Documents At," *J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020.

[6] W. R. Maya, A. Azanuddin, and E. Elfitriani, "Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 21, no. 1, p. 1, 2022, doi: 10.53513/jis.v21i1.4764.