Journal of Artificial Intelligence and Innovative Applications
Vol. 7, No. 1, Februari 2026
ISSN : 2716-1501 | E-ISSN : 2775-4057
https://doi.org/10.32493/joaiia.v7i1.54978 | Hal : 22-39

IMPLEMENTASI METODE ADVANCED ENCRYPTION STANDARD (AES) DALAM MENGAMANKAN DATA FILE SOAL UJIAN SMK MEDIA INFORMATIKA BERBASIS WEB

Mega Nur Utami[1], Bani[2]

[1,2]Teknik Informatika,. Fakultas Teknik, Universitas Pamulang, Jl Raya Puspitek, Buaran, Kec.Pamulang, Kota Tangerang Selatan, Banten 15310
e-mail: [1] lookatme.mega@gmail.com
e-mail: [2] dosen02381@unpam.ac.id

Info Artikel

Riwayat Artikel:

Received Nov 25, 2025
Revised Dec 23, 2025
Accepted Feb 21, 2026

Abstract *– The rapid development of information and communication technology has brought significant impacts, both positive and negative. One of the main challenges is data security. Organizations, educational institutions, and companies face high risks of data interception and information leaks that threaten privacy and system integrity. Although storing student exam files in softcopy form offers efficiency, weaknesses in security still pose risks of cyber-attacks such as hacking, malware, and data theft. In this context, SMK Media Informatika Jakarta places a high emphasis on the security of exam data, which is sensitive and must not be accessed before the exam schedule. Storage without adequate protection can lead to significant damage. Therefore, advanced digital security strategies are necessary. One recommended solution is the use of cryptography, specifically the Advanced Encryption Standard (AES) method. Cryptography secures data by encrypting files, making them accessible only to authorized parties. This study proposes the implementation of the AES method to secure web-based exam files at SMK Media Informatika Jakarta, providing an additional layer of protection and ensuring that sensitive information remains safe from unauthorized access, while also allowing secure and controlled access for authorized users.*

Keywords: *Data Security, AES, Exam Files, SMK Media Informatika*

Corresponding Author:
Mega Nur Utami
Email: *lookatme.mega@gmail.com*

This is an open access article under the CC BY 4.0 license.

Abstrak *– Perkembangan teknologi informasi dan komunikasi yang pesat membawa dampak signifikan, baik positif maupun negatif. Salah satu tantangan utamanya adalah keamanan data. Organisasi, lembaga pendidikan, dan perusahaan menghadapi risiko tinggi terhadap penyadapan data dan kebocoran informasi yang mengancam privasi serta integritas sistem. Meskipun penyimpanan file soal ujian siswa dalam bentuk softcopy menawarkan efisiensi, kelemahan dalam pengamanan tetap menimbulkan risiko serangan siber seperti peretasan, malware, dan pencurian data. Dalam konteks ini, SMK Media Informatika Jakarta sangat memperhatikan keamanan data ujian siswa, yang bersifat sensitif dan tidak boleh diakses sebelum jadwal ujian. Penyimpanan tanpa perlindungan yang memadai dapat menyebabkan kerusakan besar. Oleh karena itu, strategi keamanan digital yang canggih diperlukan. Salah satu solusi yang direkomendasikan adalah penggunaan kriptografi, khususnya metode Advanced Encryption Standard (AES). Kriptografi mengamankan data dengan mengenkripsi file, menjadikannya hanya dapat diakses oleh pihak berwenang. Penelitian ini mengusulkan implementasi metode AES untuk mengamankan file ujian berbasis web di SMK Media Informatika Jakarta, memberikan lapisan perlindungan tambahan dan memastikan bahwa informasi sensitif tetap aman dari akses tidak sah, sekaligus memungkinkan akses yang aman dan terkontrol bagi pengguna yang berwenang.*

Kata Kunci*: Keamanan Data, AES, File Ujian, SMK Media Informatika*

1. PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi membawa dampak signifikan dalam hal yang bersifat positif maupun negatif. Salah satu tantangan yang muncul adalah risiko keamanan data. Pentingnya menyimpan berbagai file dengan upaya perlindungan maksimal agar tidak mudah diakses oleh pihak yang tidak berkepentingan. Kekhawatiran ini pun menjadi perhatian khusus bagi beberapa organisasi, lembaga pendidikan, maupun perusahaan, terutama dalam aktivitas yang bergantung pada teknologi dan jaringan komunikasi. Teknologi telah menjadi satu kesatuan hampir di setiap aspek kehidupan manusia modern serta menjadi landasan yang tidak terpisahkan. Hampir seluruh populasi dunia kini sangat bergantung pada kemajuan teknologi yang tidak hanya mempermudah berbagai aktivitas tetapi juga mempercepat penyebaran informasi melintasi batas negara, budaya, bahkan zona waktu. Namun yang terjadi dari pesatnya perkembangan teknologi tersebut serta di balik segala kemudahan yang ditawarkan, muncul tantangan baru berupa penyadapan data dan kebocoran informasi, yang bisa membahayakan privasi dan integritas pihak-pihak terkait. Hal tersebut pun akhirnya menjadi titik permasalahan yang mulai serius menjadi perbincangan sehingga manusia mulai menyadari bahwa perkembangan teknologi informasi dan komunikasi tidak selalu membawa dampak positif ataupun menguntungkan. Penyadapan data menjadi ancaman nyata serta menjadikan aspek keamanan dalam pertukaran informasi sebagai prioritas utama. Hal ini disebabkan oleh kenyataan bahwa komunikasi data jarak jauh sering kali tidak memiliki jalur transmisi yang sepenuhnya aman dari penyusupan, sehingga menjaga keamanan informasi menjadi elemen krusial dalam dunia digital. Dengan kemajuan teknologi komputer dan komunikasi, semakin banyak individu yang mampu mencuri atau mendapatkan akses secara diam-diam ke data penting dan pribadi, meskipun langkah-langkah pengamanan sudah diterapkan dengan sangat ketat.

SMK Media Informatika Jakarta menjaga data dengan sangat hati-hati dan menyimpannya dengan rapi, terutama file-file yang berhubungan dengan soal ujian siswa. Data ini dianggap sangat sensitif karena tidak boleh sampai diketahui oleh siswa dan siswi sebelum jadwal ujian tiba. Menyimpan file soal ujian siswa dalam bentuk draft atau arsip softcopy di komputer memang memiliki kelebihan dalam hal aksesibilitas dan efisiensi. Namun, risiko kejahatan cyber tetap ada dikarenakan pengamanan data tidak memadai. File yang disimpan dalam softcopy rentan terhadap serangan cyber, seperti: peretasan, malware, dan pencurian data. Selain itu, tanpa enkripsi atau kode penyandian yang kuat terhadap file tersebut, maka file tersebut dalam status yang dapat diakses oleh pihak yang tidak berwenang, sehingga meningkatkan potensi kebocoran atau manipulasi data. Kejahatan cyber terus berkembang seiring dengan kemajuan teknologi dan pelaku kejahatan menggunakan metode yang semakin canggih untuk menembus sistem perlindungan data. Ketergantungan pada keamanan komputer standar, tanpa perlindungan yang memadai atau sistem backup data yang aman, dapat menyebabkan kerusakan besar jika file soal ujian berhasil diakses oleh pihak yang tidak bertanggungjawab. Oleh karena itu, penting untuk menganalisis kelemahan sistem penyimpanan file dan mengadopsi strategi keamanan digital yang komprehensif untuk melindungi informasi sensitif secara efektif juga penerapan teknik keamanan yang lebih canggih untuk melindungi data-data penting tersebut.

Salah satu teknik yang sangat direkomendasikan adalah penggunaan teknik kriptografi yang bertujuan untuk mengenkripsi file agar data hanya bisa diakses oleh pihak yang berwenang, sehingga memberikan lapisan perlindungan tambahan bagi data-data sensitif tersebut. Kriptografi menjadi salah satu teknik handal yang bertujuan memperkuat keamanan data atau informasi dengan mengubah cara akses terhadapnya. Dianggap sebagai perpaduan antara ilmu dan seni. Kriptografi bertujuan melindungi kerahasiaan pesan atau file yang sensitif. Dalam dunia digital yang semakin kompleks, sistem keamanan yang canggih menjadi keharusan untuk menjaga file penting dari akses yang tidak sah. Salah satu konsep kunci dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi bekerja dengan mengubah data asli menjadi bentuk yang tidak dapat dibaca oleh siapa pun kecuali pihak yang memiliki "kunci" khusus. Di sisi lain,

dekripsi adalah proses mengembalikan data terenkripsi ke bentuk aslinya, sehingga hanya mereka yang memiliki akses sah yang dapat memahami informasi tersebut. Kombinasi teknik ini memastikan data tetap terlindungi, sekaligus memungkinkan akses aman bagi mereka yang berhak mengaksesnya. Penelitian ini bertujuan untuk mengamankan data soal ujian siswa agar tidak dapat diakses oleh pihak yang tidak berwenang sebelum waktu ujian, serta untuk menguji efektivitas metode Advanced Encryption Standard (AES) dalam melindungi file ujian yang disimpan di komputer.

Dalam konteks dunia pendidikan, integritas dan kerahasiaan soal ujian merupakan aspek fundamental yang menentukan kualitas evaluasi pembelajaran. Kebocoran soal ujian sebelum waktu pelaksanaan dapat menimbulkan dampak serius, seperti menurunnya kredibilitas institusi, ketidakadilan dalam proses penilaian, serta terganggunya sistem akademik secara keseluruhan. Oleh karena itu, penelitian ini tidak hanya berorientasi pada implementasi teknis algoritma kriptografi, tetapi juga memiliki kontribusi praktis yang signifikan dalam mendukung tata kelola keamanan informasi di lingkungan sekolah.

Penelitian ini menawarkan solusi aplikatif yang dapat langsung diterapkan pada institusi pendidikan menengah, khususnya dalam pengamanan distribusi dan penyimpanan file soal ujian berbasis digital. Dengan menerapkan algoritma Advanced Encryption Standard (AES), sistem yang dikembangkan mampu memberikan perlindungan terhadap akses tidak sah sekaligus memastikan bahwa hanya pengguna dengan otorisasi yang tepat yang dapat melakukan proses dekripsi. Dengan demikian, penelitian ini relevan terhadap kebutuhan aktual lembaga pendidikan dalam menghadapi tantangan keamanan siber yang semakin kompleks.

2. PENELITIAN YANG TERKAIT

Penelitian ini bertumpu pada konsep keamanan data yang menekankan tiga aspek utama, yaitu kerahasiaan, integritas, dan ketersediaan data, khususnya dalam konteks penyimpanan file digital di lingkungan lembaga pendidikan. Data didefinisikan sebagai sekumpulan fakta yang setelah diolah menjadi informasi akan bernilai guna bagi pengambilan keputusan, sehingga akurasi dan cara pengelolaannya menjadi krusial dalam sistem informasi sekolah. Novianti & Hidayat (2023) mengimplementasikan kriptografi AES 128-bit untuk mengamankan data keuangan kas masjid, dan menunjukkan bahwa AES efektif menjaga kerahasiaan data keuangan dari pencurian atau manipulasi. Penelitian ini menjadi rujukan bahwa AES 128-bit dapat diadaptasi untuk konteks data lain yang juga sensitif, seperti soal ujian.

Landasan utama pengamanan menggunakan kriptografi, yaitu ilmu dan seni mengubah plainteks menjadi ciphertext melalui proses enkripsi dan mengembalikannya lagi melalui dekripsi dengan menggunakan kunci rahasia. Tujuan kriptografi yang diulas meliputi kerahasiaan (confidentiality), integritas, autentikasi, ketersediaan, dan pengendalian akses, yang kemudian dijadikan acuan dalam merancang mekanisme pengamanan file soal ujian. Tania dkk. (2024) menerapkan algoritma AES 128-bit pada sistem keamanan data digital berbasis web di Kantor Desa Aman Damai, difokuskan pada perlindungan dokumen penting seperti surat keterangan dan perizinan dari akses tidak sah. Hasilnya menguatkan bahwa integrasi AES dalam aplikasi web dapat meningkatkan keamanan dokumen administrasi publik.

Penelitian juga mengkaji secara khusus algoritma Advanced Encryption Standard (AES) sebagai metode kriptografi kunci simetris yang dipilih karena tingkat keamanan dan efisiensi komputasinya. Selain itu, dibahas pula konsep enkripsi–dekripsi, algoritma kunci simetris dan asimetris, serta teori pendukung lain seperti dokumen digital, web system, UML, pengujian black box dan white box sebagai dasar perancangan dan evaluasi sistem berbasis web untuk pengamanan file ujian. Indraka & Romli (2025) mengembangkan sistem keamanan arsip kelurahan berbasis web menggunakan AES-128 untuk mencegah kebocoran dan pencurian data arsip, dengan pengujian black box yang menunjukkan tingkat keberhasilan

99%. Temuan ini relevan karena membuktikan bahwa mekanisme enkripsi–dekripsi AES-128 dapat diimplementasikan secara praktis pada sistem arsip berbasis web.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan Research and Development (R&D) yang berfokus pada proses perancangan, pengembangan, dan pengujian sistem secara sistematis hingga menghasilkan produk perangkat lunak yang valid dan dapat digunakan. Metode R&D dipilih karena memungkinkan peneliti untuk tidak hanya melakukan analisis konseptual, tetapi juga menghasilkan implementasi sistem yang teruji secara fungsional maupun struktural.

Tahapan penelitian terdiri dari beberapa fase utama sebagai berikut:

1. Analisis Kebutuhan (Requirement Analysis)

   Tahap ini dilakukan untuk mengidentifikasi kelemahan sistem penyimpanan soal ujian yang berjalan serta menganalisis kebutuhan keamanan berdasarkan prinsip kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability).

2. Perancangan Sistem (System Design)

   Perancangan sistem dilakukan menggunakan pendekatan Unified Modeling Language (UML) yang meliputi:

   - Use Case Diagram
   - Activity Diagram
   - Sequence Diagram
   - Class Diagram

   Pendekatan ini digunakan untuk memastikan alur sistem terdokumentasi secara visual dan sistematis sehingga memudahkan proses implementasi serta evaluasi logika sistem.

3. Implementasi Algoritma AES

   Pada tahap ini dilakukan integrasi algoritma Advanced Encryption Standard (AES-128) ke dalam sistem berbasis web untuk menangani proses:

   - Enkripsi file soal ujian
   - Penyimpanan file terenkripsi
   - Dekripsi file oleh pengguna berwenang

4. Pengujian Sistem

Pengujian dilakukan melalui dua pendekatan utama:

a. Black Box Testing
   Untuk memastikan seluruh fitur sistem berjalan sesuai spesifikasi tanpa melihat struktur kode internal.

b. White Box Testing (Basis Path Testing)
   Untuk menganalisis logika internal sistem dengan menghitung nilai Cyclomatic Complexity pada modul:

   - Login
   - Proses Enkripsi
   - Proses Dekripsi
   - Logout

Pendekatan ini bertujuan untuk memastikan setiap jalur logika program telah diuji secara menyeluruh sehingga meminimalisir potensi kesalahan sistem.

4. HASIL DAN PEMBAHASAN

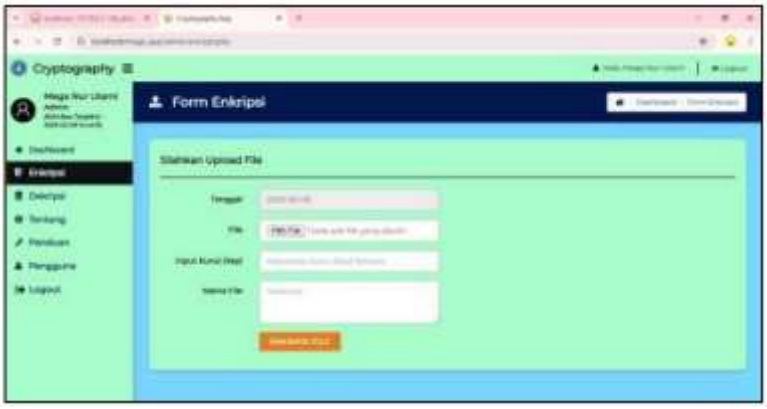
Spesifikasi perangkat keras untuk menjalankan aplikasi kriptografi keamanan dokumen file ujian siswa di SMK Media Informatika Jakarta menggunakan algoritma AES meliputi penggunaan notebook atau laptop dengan prosesor Intel Core i5 generasi ke-4, memori RAM sebesar 8 GB, penyimpanan SSD 256 GB, dan monitor berukuran 14 inci. Sedangkan untuk perangkat lunak, sistem ini berjalan pada sistem operasi Windows 10 64-bit, menggunakan XAMPP sebagai server yang mencakup Apache dan MySQL, editor program Visual Studio Code, serta browser Google Chrome sebagai media akses aplikasi. Spesifikasi ini telah disesuaikan untuk mendukung kinerja optimal aplikasi kriptografi dalam konteks keamanan dokumen ujian siswa.

Berikut ini adalah hasil beberapa rancangan program pada usulan sistem yang telah dibuat dapat dilihat pada gambar dibawah ini. Aplikasi sistem yang dibuat masih dijalankan pada localhost (server lokal). Untuk editor program menggunakan software Visual Studio Code dengan spesifikasi:

Version : 1.96.4 (user setup)
Electron : 32.2.6
ElectronBuildId : 10629634
Chromium : 128.0.6613.186
Node.js : 20.18.1
V8 : 12.8.374.38-electron.0
OS : Windows_NT x64 10.0.19045

Gambar 1. Form Login Pengguna

Pada Gambar 1 merupakan halaman aplikasi sistem berupa form login untuk akses pengguna Admin dan Guru yang menampilkan kolom Username dan Password yang perlu di-input agar pengguna dapat mengakses halaman utama (dashboard) pada aplikasi sistem.



Gambar 2. Form Enkripsi

Pada Gambar 2 merupakan form input yang berisikan data file yang akan dienkripsi. Pada halaman ini Admin dapat melakukan tindakan input data file melalui proses upload file. Untuk melakukan proses enkripsi dibutuhkan secret key yang nantinya key tersebut akan dikirimkan ke database beserta file yang telah di upload ke sistem.

Gambar 3. Gagal Login Kondisi Username dan Password Salah

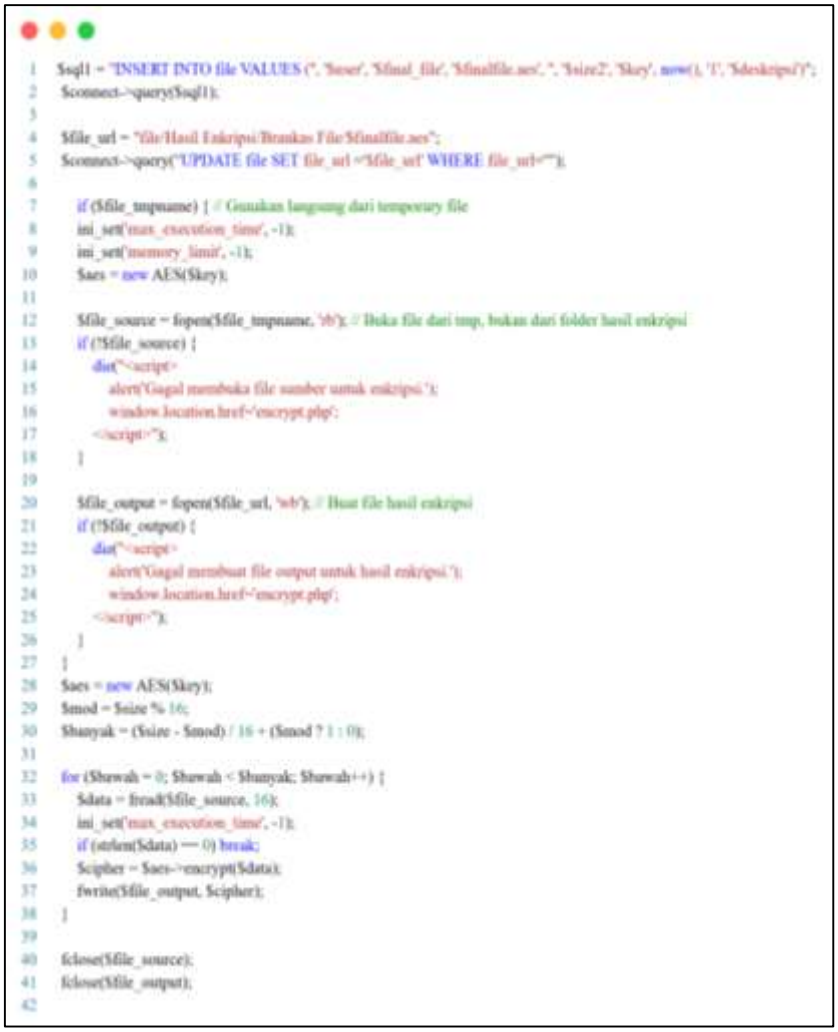
Pada tampilan Gambar 3 di bawah ini merupakan notifikasi pemberitahuan informasi yang ditampilkan oleh aplikasi sistem apabila pengguna yaitu Admin atau Guru pada saat melakukan tahap login dengan memasukkan username dan password yang tidak sesuai dan salah, maka menampilkan notifikasi.

Gambar 4. Notifikasi Berhasil Login Sebagai Admin

Pada tampilan Gambar 4 di bawah ini merupakan notifikasi pemberitahuan yang ditampilkan aplikasi sistem apabila pengguna Admin pada saat melakukan login dengan memasukkan username dan password yang sesuai.

Gambar 5. Output Hasil Enkripsi File

Berikut hasil rancangan program pada file ujian siswa yang telah dilakukan tahap enkripsi. Sistem hanya dapat memverifikasi file yang bisa dienkrip hanya file dengan ekstensi .docx dan .pdf serta file yang memiliki kapasitas atau ukuran file yang tidak bisa lebih besar dari 3 Mb. Pseudocode termasuk dalam representasi logis dan terstruktur dari suatu algoritma yang ditulis dalam format yang mudah dipahami, tanpa bergantung pada sintaks bahasa pemrograman tertentu. Tujuannya adalah untuk menggambarkan alur logika program sebelum diimplementasikan dalam kode sebenarnya.



```
$sql1 = "INSERT INTO file VALUES ('', '$user', '$final_file', '$finalfile.aes', '', '$size2', '$key', now(), '1', '$deskripsi')";
$connect->query($sql1);

$file_url = "file/Hasil Enkripsi/Brankas File/$finalfile.aes";
$connect->query("UPDATE file SET file_url ='$file_url' WHERE file_url=''");

  if ($file_tmpname) { // Gunakan langsung dari temporary file
  ini_set('max_execution_time', -1);
  ini_set('memory_limit', -1);
  $aes = new AES($key);

  $file_source = fopen($file_tmpname, 'rb'); // Buka file dari tmp, bukan dari folder hasil enkripsi
  if (!$file_source) {
    die("<script>
      alert('Gagal membuka file sumber untuk enkripsi.');
      window.location.href='encrypt.php';
    </script>");
  }

  $file_output = fopen($file_url, 'wb'); // Buat file hasil enkripsi
  if (!$file_output) {
    die("<script>
      alert('Gagal membuat file output untuk hasil enkripsi.');
      window.location.href='encrypt.php';
    </script>");
  }
}
$aes = new AES($key);
$mod = $size % 16;
$banyak = ($size - $mod) / 16 + ($mod ? 1 : 0);

for ($bawah = 0; $bawah < $banyak; $bawah++) {
  $data = fread($file_source, 16);
  ini_set('max_execution_time', -1);
  if (strlen($data) == 0) break;
  $cipher = $aes->encrypt($data);
  fwrite($file_output, $cipher);
}

fclose($file_source);
fclose($file_output);
```

Gambar 6. Source Code Proses Enkripsi

Tahapan Source Code dari struktur algoritma pada proses enkripsi yang terdapat pada sistem

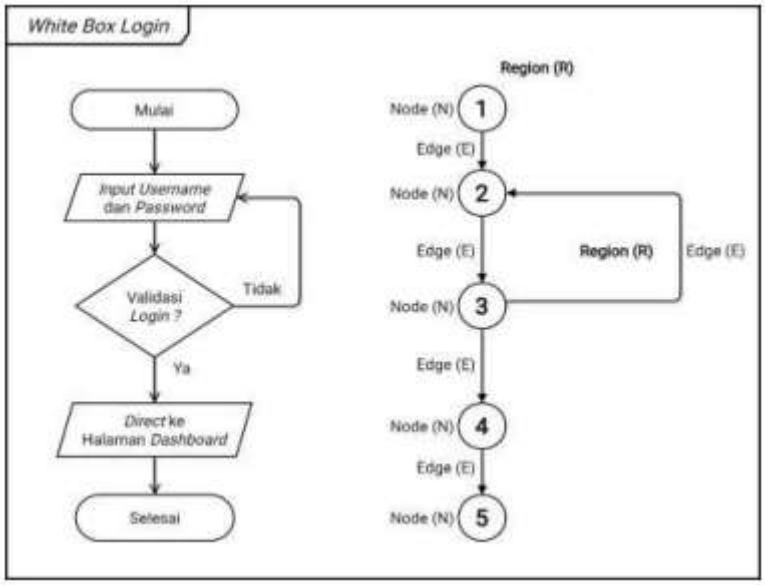
Tabel I. Hasil Skenario Pengujian Black Box Proses Login

Pengujian *Black Box* Halaman Proses *Login*				
No	**Skenario Pengujian**	***Test Case***	**Hasil yang Diharapkan**	**Kesimpulan**
1	Tidak mengisi *username* dan *password*, lalu selanjutnya mengklik tombol *login*	*Username*: (kosong) *Password*: (kosong)	Sistem akan menampilkan pesan *warning* “Harap isi bidang ini.” 	**Valid**
2	Mengisi *username* dengan benar dan tidak mengisi *password*, selanjutnya	*Username*: (Admin) *Password*: (kosong)	Sistem akan menampilkan pesan *warning* “Harap isi bidang ini.”	**Valid**

	mengklik tombol *login*			
3	Mengisi *password* dengan benar dan tidak mengisi *username*, selanjutnya mengklik tombol *login*	*Username*: (kosong) *Password*: (Admin)	Sistem akan menampilkan pesan *warning* "Harap isi bidang ini."	**Valid**
4	Mengisi *username* dan *password* dengan data yang salah, lalu mengklik tombol *login*	*Username*: (test) *Password*: (test)	Sistem akan menolak dan menampilkan pesan notifikasi peringatan "Username atau Password Salah !!!"	**Valid**
5	Mengisi *username* yang benar dan mengisi *password* dengan data yang salah, lalu mengklik tombol *login*	*Username*: (mega) *Password*: (test)	Sistem akan menolak dan menampilkan pesan notifikasi peringatan "Mohon Ulangi Proses Login ..!!! Data Username Atau Password Anda Salah ..."	**Valid**
6	Mengisi *username* dan *password* akun guru dengan data yang benar, lalu mengklik tombol *login*	*Username*: (nurhayati) *Password*: (guru)	Sistem akan menolak dan menampilkan pesan notifikasi peringatan "Status Akun Non-Aktif, Silakan Hubungi Administrator ..!!!"	**Valid**
7	Mengisi *username* dan *password* akun admin dengan data yang benar, lalu mengklik tombol *login*	*Username*: (mega) *Password*: (admin)	Sistem akan menerima akses *login* dan menampilkan pesan sukses berupa kotak dialog "Anda Berhasil Login sebagai Admin ..."	**Valid**

Pengujian menggunakan teknik black box testing yang dilakukan pada sisi fungsional sistem mulai dari skenario pengujian halaman akses login, skenario pengujian enkripsi file dan skenario pengujian dekripsi file sehingga hasil yang dicapai dapat dijadikan tolak ukur sistem berjalan dengan baik atau tidak sesuai dengan fungsinya. Dengan adanya pengujian ini, kualitas sistem dapat lebih terjamin serta meminimalisir kemungkinan terjadinya kesalahan saat digunakan oleh pengguna.

Tahap pengujian ini merupakan pengujian aplikasi atau software dengan teknik meneliti dan menganalisa kode dari program yang telah dibuat terdapat kesalahan atau tidak. Jika model telah menghasilkan berupa output yang tidak sesuai, maka akan dilakukan kompilasi ulang dan serta cek kembali kode-kode tersebut hingga sesuai dengan yang fungsi jalannya perintah pada sistem aplikasi kriptografi keamanan dokumen file ujian siswa pada SMK Media Informatika Jakarta. Pengujian white box yang dilakukan ini merupakan teknik untuk menganalisa kode program pada sistem sesuai dengan skenario pengujian yang dilakukan pada pengujian black box sebelumnya.



Gambar 6. Output Flowchart dan Flowgraph Login

Cyclomatic Complexity dari Edge dan Node pada Gambar 4.14, dimana nilai Edge (E) = 5 dan nilai Node (N) = 5, maka rumus Cyclomatic Complexity sebagai berikut ini:

V (G) = E - N + 2
= 5 - 5 + 2
= 2

Kesimpulannya, untuk jumlah jalur atau Path sebanyak 2.

Untuk Predicate Node (P) yang terdapat pada flowgraph Gambar 4.14 diatas, dimana P merupakan jumlah logika, P=1

V (G) = P + 1
= 1 + 1
= 2

Kesimpulannya, untuk jumlah Region (R) adalah 2.

Kemudian untuk keseluruhan independent path atau jumlah jalur independen pada flowgraph Gambar 4.14 diatas adalah sebagai berikut:

Path 1 = 1 – 2 – 3 – 4 – 5

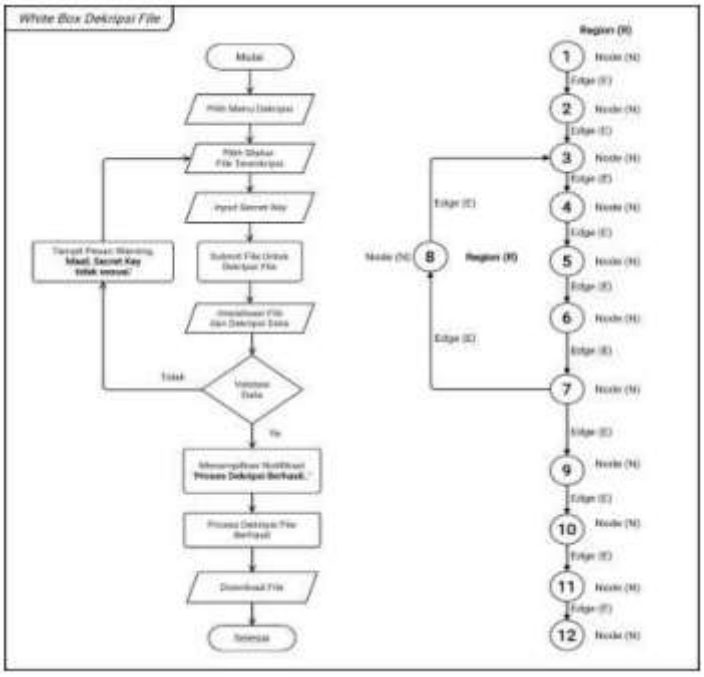
Path 2 = 1 – 2 – 3 – 2 – 3 – 4 – 5

Tabel 2. Test Case Pseudocode Login Path 1

Path	**1**
Jalur	**1 – 2 – 3 – 4 – 5**
Skenario	**1.** Mulai.
	2. Memasukkan data username dan password lalu submit.
	3. Kondisi berhasil login ke sistem.
	4. Proses direct ke halaman utama (dashboard).
	5. Selesai.
Hasil Pengujian	Berhasil

Tabel 3. Test Case Pseudocode Login Path 2

Path	**2**
Jalur	**1 – 2 – 3 – 2 – 3 – 4 – 5**
Skenario	**1.** Mulai.
	2. Memasukkan data username dan password lalu submit.
	3. Kondisi gagal login ke sistem.
	2. Memasukkan data username dan password lalu submit.
	3. Kondisi berhasil login ke sistem
	4. Proses direct ke halaman utama (dashboard).
	5. Selesai.
Hasil Pengujian	Berhasil



Gambar 7. Flowchart dan Flowgraph Enkripsi File

Cyclomatic Complexity dari Edge dan Node pada Gambar 7, dimana nilai Edge (E) = 12 dan nilai Node (N) = 12, maka rumus Cyclomatic Complexity sebagai berikut ini:

V (G) = E - N + 2
= 12 - 12 + 2
= 2

Kesimpulannya, untuk jumlah jalur atau Path sebanyak 2. 2.

Untuk Predicate Node (P) yang terdapat pada flowgraph Gambar 7 diatas, dimana P merupakan jumlah logika,

P =1 V (G) = P + 1
= 1 + 1
= 2

Kesimpulannya, untuk jumlah Region (R) adalah 2. 3.

Kemudian untuk keseluruhan Path atau jumlah jalur yang terdapat pada flowgraph Gambar 7 diatas adalah sebagai berikut:

Path 1 = 1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 - 3 – 4 – 5 – 6 – 7 – 9 – 10 – 11 – 12

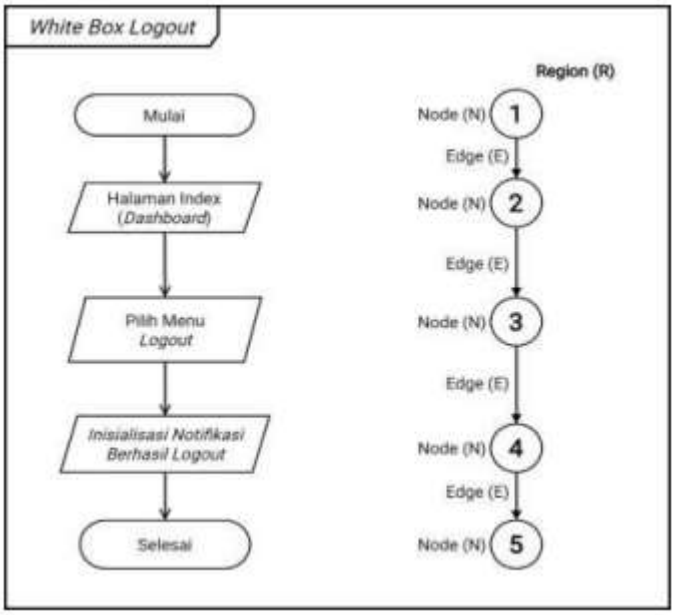
Path 2 = 1 – 2 – 3 – 4 – 5 – 6 – 7 – 8

Tabel 4. Test Case Pseudocode Dekripsi File Path 1

Path	**1**
Jalur	**1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 - 3 – 4 – 5 – 6 – 7 – 9 – 10 – 11 – 12**
Skenario	**1.** Mulai.
	2. Mengakses halaman menu dekripsi.
	3. Menampilkan status "Ter-Enkripsi" jika data ter-enkripsi.
	4. Masukkan secret key.
	5. Melakukan submit (proses dekripsi).
	6. Membaca data, mendekripsinya, dan menulis hasil dekripsi ke file.
	7. Validasi Data
	8. Proses gagal dan sistem menampilkan pesan alert yang memberi informasi bahwa secret key yang dimasukkan tidak sesuai.
	3. Menampilkan "Ter-Enkripsi" jika status data adalah 1.
	4. Menyimpan secret key dari data untuk dekripsi.
	5. Melakukan submit (proses dekripsi).
	6. Membaca data, mendekripsinya, dan menulis hasil dekripsi ke file.
	7. Validasi Data
	9. Menampilkan pesan bahwa dekripsi berhasil.
	10. Menyimpan lokasi file hasil dekripsi.
	11. Menyimpan file untuk diunduh, membaca file, dan menghapus session setelahnya.
	12. Selesai.
Hasil Pengujian	Berhasil

Tabel 5. Test Case Pseudocode Login Path 2

Path	**2**
Jalur	**1 – 2 – 3 – 4 – 5 – 6 – 7 – 9 – 10 – 11 – 12**
Skenario	**1.** Mulai.
	2. Mengakses halaman menu dekripsi
	3. Menampilkan status "Ter-Enkripsi" jika data ter-enkripsi.
	4. Masukkan secret key
	5. Melakukan submit (proses dekripsi).
	6. Membaca data, mendekripsinya, dan menulis hasil dekripsi ke file.
	7. Validasi Data
	8. Proses gagal dan sistem menampilkan pesan alert yang memberi informasi bahwa secret key yang dimasukkan tidak sesuai.
Hasil Pengujian	Berhasil



Gambar 8. Flowchart dan Flowgraph Logout

Cyclomatic Complexity dari Edge dan Node pada Gambar 8, dimana nilai Edge (E) = 4 dan nilai Node (N) = 5, maka rumus Cyclomatic Complexity sebagai berikut ini:

V (G) = E - N + 2
= 4 - 5 + 2
= 1

Kesimpulannya, untuk jumlah jalur atau Path sebanyak 1. 5.

Untuk Predicate Node (P) yang terdapat pada flowgraph Gambar 8 diatas, dimana P merupakan jumlah logika, P=0

V (G) = P + 1
= 0 + 1
= 1

Kesimpulannya, untuk jumlah Region (R) adalah 1. 6.

Kemudian untuk keseluruhan independent path atau jumlah jalur independen pada flowgraph Gambar 8 diatas adalah sebagai berikut:

Path 1 = 1 – 2 – 3 – 4 – 5

Tabel 6. Test Case Pseudocode Logout Path 1

Path	**1**
Jalur	**1 – 2 – 3 – 4 – 5**
Skenario	**1.** Mulai.
	2. Halaman sistem.
	3. Pilih menu logout
	4. Menampilkan kotak dialog informasi (alert) dan mengarahkan pengguna ke halaman index.php setelah berhasil keluar dari sistem.
	5. Selesai.
Hasil Pengujian	Berhasil

Analisis White Box dan Cyclomatic Complexity

Pengujian white box dilakukan untuk mengevaluasi kompleksitas logika internal sistem menggunakan pendekatan basis path testing. Nilai Cyclomatic Complexity dihitung dengan rumus:

$$V(G)=E-N+2$$

atau

$$V(G)=P+1$$

di mana:

- E = jumlah edge
- N = jumlah node
- P = jumlah predicate node

Hasil perhitungan menunjukkan bahwa modul login, enkripsi, dan dekripsi memiliki tingkat kompleksitas yang masih dalam kategori terkendali (low to moderate complexity), sehingga sistem dinilai memiliki struktur logika yang stabil dan dapat dipelihara dengan baik.

Pengujian ini memperkuat validitas sistem karena tidak hanya menguji keluaran program, tetapi juga memastikan seluruh jalur keputusan dalam kode telah dievaluasi secara menyeluruh.

Analisis Efektivitas Implementasi AES

Berdasarkan hasil pengujian yang telah dilakukan, implementasi algoritma Advanced Encryption Standard (AES-128) pada sistem keamanan file soal ujian menunjukkan tingkat efektivitas yang tinggi dalam menjaga kerahasiaan data. File yang telah melalui proses enkripsi berubah menjadi ciphertext yang tidak dapat dibaca tanpa penggunaan secret key yang sesuai.

Hasil pengujian Black Box menunjukkan bahwa seluruh fungsi utama sistem berjalan sesuai dengan spesifikasi, meliputi proses login, enkripsi file, dekripsi file, serta manajemen pengguna. Tidak ditemukan kegagalan fungsi pada skenario pengujian yang telah dirancang.

Sementara itu, hasil pengujian White Box melalui analisis Cyclomatic Complexity menunjukkan bahwa setiap modul memiliki jalur logika yang terkontrol dan tidak memiliki percabangan berlebihan yang dapat meningkatkan risiko kesalahan program. Dengan demikian, sistem tidak hanya valid dari sisi fungsionalitas, tetapi juga dari sisi struktur logika internalnya.

Dari sisi keamanan, penerapan AES memberikan perlindungan terhadap:

- Akses langsung terhadap file dalam server
- Upaya pembukaan file tanpa otorisasi
- Potensi manipulasi isi dokumen sebelum jadwal ujian

Hal ini menunjukkan bahwa sistem mampu meminimalisir risiko kebocoran soal ujian secara signifikan dibandingkan metode penyimpanan konvensional tanpa enkripsi.

Batasan Teknis Sistem

Meskipun sistem yang dikembangkan telah berjalan dengan baik dan memenuhi tujuan penelitian, terdapat beberapa batasan teknis yang perlu diperhatikan:

1. Sistem saat ini hanya mendukung file dengan ekstensi .docx dan .pdf.
2. Ukuran file yang dapat diproses dibatasi maksimal 3 MB.
3. Sistem masih berjalan pada lingkungan localhost (server lokal).
4. Manajemen kunci (key management) masih menggunakan secret key yang diinput secara manual oleh pengguna.

Pembatasan ukuran dan ekstensi file diterapkan untuk menjaga performa sistem serta menghindari beban proses enkripsi yang terlalu besar pada server dengan spesifikasi standar. Namun demikian, batasan ini berpotensi menjadi kendala apabila terdapat soal ujian berbasis gambar resolusi tinggi atau multimedia dengan ukuran file yang lebih besar. Oleh karena itu, pengembangan lanjutan diperlukan untuk meningkatkan skalabilitas sistem agar mampu menangani file dengan ukuran lebih besar dan format yang lebih beragam.

5. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa implementasi metode Advanced Encryption Standard (AES-128) pada sistem keamanan file soal ujian berbasis web di SMK Media Informatika Jakarta berhasil diterapkan dengan baik dan efektif.

Sistem yang dikembangkan mampu:

1. Menjaga kerahasiaan file soal ujian melalui proses enkripsi sehingga tidak dapat dibaca tanpa kunci yang sesuai.
2. Mengontrol akses pengguna melalui sistem login berbasis otorisasi.
3. Memastikan validitas sistem melalui pengujian Black Box dan White Box.
4. Menunjukkan struktur logika program yang stabil berdasarkan hasil perhitungan Cyclomatic Complexity.

Dengan demikian, penelitian ini membuktikan bahwa algoritma AES efektif dalam menjaga kerahasiaan data dan meminimalisir risiko penyalahgunaan akses oleh pihak yang tidak berwenang, khususnya dalam konteks pengamanan dokumen ujian di lingkungan pendidikan.

Secara praktis, sistem ini dapat menjadi solusi implementatif bagi institusi pendidikan dalam meningkatkan tata kelola keamanan informasi berbasis digital.

6. SARAN

Untuk pengembangan selanjutnya, beberapa rekomendasi yang dapat dilakukan antara lain:

1. Mengembangkan sistem agar mampu mendukung lebih banyak format file, termasuk gambar dan dokumen multimedia.
2. Meningkatkan batas kapasitas ukuran file agar lebih fleksibel.
3. Mengimplementasikan manajemen kunci otomatis dengan metode key derivation atau integrasi sistem otentikasi yang lebih kuat.
4. Mengembangkan sistem pada server berbasis cloud untuk meningkatkan skalabilitas dan aksesibilitas.

5. Menambahkan fitur audit log yang lebih detail untuk memantau aktivitas pengguna secara real-time.

Pengembangan lanjutan ini diharapkan dapat meningkatkan keamanan, fleksibilitas, serta kesiapan sistem dalam menghadapi tantangan keamanan siber yang lebih kompleks di masa mendatang.

DAFTAR PUSTAKA

[1] Adella, A. F., Pratama Putra, M. F., Taufiqurrahman, F., & Kaswar, A. B. (2020). Sistem Pintu Cerdas Menggunakan Sensor Ultrasonic Berbasis Internet of Things. Jurnal Media Elektrik, 17(3), 1–7.

[2] Alhamidi, L. A. (2022). Pengaruh Teaching Factory Dan Leadership Terhadap Kinerja Civitas Akademik Sekolah Menengah Kejuruan. Jurnal Pendidikan Manajemen Perkantoran, 7(1), 1–15. https://doi.org/10.17509/jpm.v7i1.41644

[3] Anamisa, D. R., & Mufarroha, F. A. (2020). Buku DASAR PEMROGRAMAN WEB Teori & Implementasi (HTML, CSS, Javascript, Bootstrap, Codeigniter). Malang: Media Nusa Creative.

[4] Berliana, S. Y., & Purtiningrum, S. W. (2023). Sistem Pendukung Keputusan Penilaian Ketidakdisiplinan Siswa Menggunakan Metode SAW Berbasis Web (Studi Kasus : MA Al-Muddatsiriyah). Jurnal IKRAITH-INFORMATIKA, 7(1), 16–23.

[5] Eriana, E. S., Subariah, R., & Farizy, S. (2022). Buku Testing & Implementasi Sistem. Pamulang: UNPAM Press.

[6] Fadillah, W. N., Al-areef, M. H., & Khatulistiwa, J. (2023). Sistem Pendukung Keputusan Untuk Memilih Laptop Ideal Dengan Metode SAW. Jurnal J-COM (Jurnal Informatika Dan Teknologi Komputer), 04(01), 7–13.

[7] Fadlullah, Tahir, M., Bintari, B. P., Dewi, M. L., & Ilmy, M. F. (2023). Implementasi Algoritma AES pada Autentikasi Login Sistem Informasi. Jurnal Bintang Pendidikan Indonesia (JUBPI), 1(2), 251–263.

[8] Fauzi, A., & Yunial, A. H. (2025). Buku Testing dan QA Perangkat Lunak. In CV. Eureka Media Aksara.

[9] Gunawan, I. (2021). Keamanan Data: Teori dan Implementasi. Jawa Barat: CV Jejak.

[10] Handoyo, J., & Subakti, Y. M. (2020). Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (AES). Jurnal SITECH : Sistem Informasi Dan Teknologi, 3(2), 143–152. https://doi.org/10.24176/sitech.v3i2.5865

[11] Hartati, E. (2022). Sistem Informasi Transaksi Gudang Berbasis Website Pada CV. Asyura. Klik - Jurnal Ilmu Komputer, 3(1), 12–18.

[12] Indraka, A. P., & Romli, M. A. (2025). Keamanan Arsip Kelurahan Bumijo Menggunakan Metode Advanced Encryption Standard (AES-128) Berbasis Web. MALCOM: Indonesian Journal of Machine Learning and Computer Science, 05(January), 232–241.

[13] Irfan, M., Siregar, H., & Handoko, J. T. (2023). Pengembangan Dan Integrasi Aplikasi Prediksi Jumlah Gagal Produksi PC Meggunakan Metode Triple Exponential Smoothing Pada Sistem Aplikasi Produksi di PT. Tera Data Indonusa,Tbk. Seminar Nasional Hasil Penelitian Dan Pengabdian Masyarakat, 80–96.

[14] Kurniawan, J., Hartoto, Fahmi, A. Z., Ahyani, H., Hikmah, Ridwan, M., Amane, A. P. O., Afnarius, S., Priyanda, R., Arnita, Yudawisastra, H. G., Rosmawati, A., & Hozairi. (2023). Buku Analisis dan Visualisasi Data. Bandung: Widina Bhakti Persada.

[15] Limbong, T., & Sriadhi. (2021). Pemrograman Web Dasar. Jakarta: Yayasan Kita Menulis.

[16] Marlina, Masnur, & F., M. D. (2021). Aplikasi E-Learning Siswa SMK Berbasis Web. Jurnal Sintaks Logika, 1(1), 8–17. Martin, R. S., & Dewanto, Y. (2023). Prototipe Kunci Pintu Otomatis Menggunakan Sensor Kamera Berbasis Raspberry. Jurnal Teknologi Industri, 12(1), 21–29.

[17] Meianti, A., Rorizki, F., & Suhairi. (2021). Dokumen Bisnis Sosial yang Efektif Dalam Komunikasi Organisasi. Dawatuna: Journal of Communication and Islamic Broadcasting, 1(2), 142–150.

[18] Novianti, H. D., & Hidayat, A. T. (2023). Implementasi Kriptografi Advanced Encryption Standard 128 Bit Dalam Pengamanan Data Keuangan Kas. Jurnal Komputer Dan Teknologi, 01(02), 27–34.

[19] Pitrawati, & Sanjaya, A. (2021). Rekayasa Perangkat Lunak Perhitungan Harga Pokok Produksi Metode Full

Costing Pada UMKM Mitra Cake Di Bandar Lampung. Jurnal Informasi Dan Komputer, 9(2), 154–162.

[20] Suharya, Y., & Widia, H. (2020). Implementasi Digital Signature Menggunakan Algoritma Kriftografi RSA Untuk Pengamanan Data Di SMK Wirakarya 1 Ciparay. Jurnal Informatika (Computing), 07(01), 20–29.

[21] Rangkuti, A. Z. F., & Fahmi, H. (2020). Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5. Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI), 3(2), 170–175. https://doi.org/10.32672/jnkti.v3i2.2384

[22] Tania, M., Alasi, T. S., Yap, R., Informatika, T., Barat, B., Damai, A., Digital, K. D., Web, A. B., Damai, D. A., Damai, A., & Digital, K. D. (2024). Algoritma AES Untuk Kemanan Data Digital Berbasis Web di Kantor Desa Aman Damai. Jurnal Times, 13(02), 142–149.

[23] Wachid Hidayatulloh, N., Tahir, M., Amalia, H., Afdlolul Basyar, N., Prianggara, A. F., & Yasin, M. (2023). Mengenal Advanced Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data. Digital Transformation Technology (Digitech), 3(1), 1–10.

[24] Widyawan, D., & Imelda. (2021). Pengamanan File Menggunakan Kriptografi Dengan Metode AES-128 Berbasis Web Di Komite. SKANIKA, 4(1), 15–22.

[25] Zen, H. R. R., & Nuryasin, I. (2024). Penerapan Whitebox Testing Pada Pengujian Sistem Menggunakan Teknik Basis Path. Journal Of Information Systems And Informatics Engineering, 8(1), 101–111. https://doi.org/10.35145/joisie.v8i1.4229