JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.44

Implementasi Sistem Keamanan Data Menggunakan Algoritma Kriptografi Simetri IDEA

Siti Ikhlisa Azzahwa[1*], Elvira Maulinda [2], Putri Naila Oktavia [3] , Irgi Ahmad Fahrezi [4] , Musyawirdi Mahtuah[5], Khildania[6]
[1,2,3,4,5,6]Universitas Malikussaleh, Indonesia
[1]khil.22018007@mhs.unimal.ac.id, [2]elvira.220180012@mhs.unimal.ac.id, [3]siti.220180014@mhs.unimal.ac.id,
[4]putri.220180032@mhs.unimal.ac.id, [5]irgi.220180038@mhs.unimal.ac.id, [6]musyawirdi.220180153@mhs.unimal.ac.id

ABSTRACT

Banyak algoritma kriptografi modern yang walaupun menyediakan keamanan tinggi,Namun sangat susah dimengerti dan dipelajari masyarakat awam. Tujuan dari penelitian ini adalah untuk membangun suatu perangkat lunak yang tidak hanya bisa menjaga keamanan data dengan kuat dan andal, tapi juga mudah dimengerti banyak orang.Untuk itulah algoritma IDEA dipilih, karena algoritma ini termasuk algoritma yang memuaskan user selain dengan kekuatan dan keandalannya dari berbagai serangan para kriptanalis, juga dengan kemudahannya dipelajari semua orang. Sistem ini dikembangkan menggunakan bahasa pemrograman C++. Analisis kebutuhan perangkat lunak algoritma IDEA dilakukan dengan menentukan nama perangkat lunak yang akan dibangun, mengetahui siapa yang akan menggunakan perangkat lunak tersebut, memahami konsep teknologi yang akan dipakai, membuat tampilan antarmuka yang mendidik, menentukan teknik yang dipergunakan untuk membentuknya, serta menguji hasil perangkat lunak tersebut. Objektif utama sistem ini adalah untuk melihat dan mempelajari berbagai konsep dan prinsip untuk merancang dan mengimplementasikan sistem keamanan data menggunakan algoritma IDEA.

Kata Kunci: *KRIPTOGRAFI,IDEA,KEAMANAN DATA*

PENDAHULUAN

Sistem keamanan pengiriman data (komunikasi data yang aman) dipasang untuk mencegah pencurian, kerusakan, dan penyalahgunaan data yang terkirim melalui jaringan komputer. Dalam praktek, pencurian data berwujud pembacaan oleh pihak yang tidak berwenang biasanya dengan menyadap saluran publik. Teknologi jaringan komputer telah dapat mengurangi bahkan membuang kemungkinan adanya kerusakan data akibat buruknya konektivitas fisik, namun gangguan tetap bisa terjadi karena ada unsur kesengajaan yang mengarah ke penyalahgunaan sistem dari pihak pihak tertentu.

IDEA (International Data Encryption Algorithm) merupakan sebuah algoritma kriptografi simetri yang diciptakan pada awalnya sebagai pengganti Data Encryption Standard (DES). IDEA adalah sebuah revisi kecil dari cipher yang lebih awal, yakni PES (Proposed Encryption Standard). Pada awalnya, IDEA disebut IPES (Improved PES). Algoritma IDEA terbilang sederhana karena hanya melibatkan 3 proses utama dan 9 putaran.

Algoritma ini merupakan algoritma yang menyediakan keamanan cukup tinggi yang tidak didasarkan atas kerahasiaan algoritmanya (algoritma *restricted*), akan tetapi lebih ditekankan pada keamanan/kerahasian kunci yang digunakan (algoritma *kriptografi modern*). Algoritma *restricted* biasanya digunakan oleh sekelompok orang untuk bertukar pesan satu sama lain, mereka membuat suatu algoritma enkripsi yang hanya diketahui oleh anggota kelompok itu saja, sehingga setiap kali ada anggota kelompok yang keluar, maka algoritma *restricted* tersebut harus diganti karena kemungkinan anggota kelompok yang keluar itu dapat membocorkan algoritmanya.

Namun algoritma kriptografi modern, seperti algoritma IDEA ini, dapat mengatasi masalah tersebut dengan menggunakan kunci, yang dalam hal ini algoritmanya tidak lagi dirahasiakan,tetapi kunci harus dijaga kerahasiaannya. Sehingga setiap kali ada anggota kelompok yang keluar, maka algoritma yang dipakai tidak perlu diganti, namun cukup mengganti kuncinya saja.

Dengan perkataan lain, diperlukan algoritma kriptografi modern yang dapat digunakan dan gampang dimengerti oleh semua orang, juga algoritma yang menyediakan keamanan cukup tinggi yang tidak didasarkan atas kerahasiaan algoritmanya. Untuk itulah penulis mengambil judul "Perancangan dan Implementasi Sistem Keamanan Data Menggunakan Algoritma Kriptografi Simetri IDEA".

KAJIAN LITERATUR

Kriptografi berasal dari dua suku kata yaitu kripto dan grafi. Kripto artinya menyembunyikan, sedangkan grafi artinya ilmu. Kriptografi (Cryptography) adalah suatu ilmu yang mempelajari sistem sandi untuk menjamin kerahasiaan dan keamanan data, yang kegiatannya dilakukan oleh seorang kriptographer. Kriptografi secara umum merupakan ilmu dan seni untuk menjaga kerahasian berita (Scheiner. B., 1996). Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes. et al,1996).

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.44

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi (Menezes. et al,1996) (Scheiner. B., 1996), yaitu:

1. Kerahasiaan (Confidentiality), adalah layanan yang digunakan untuk menjaga isi informasi dari siapapun, kecuali yang memiliki kunci rahasia atau otoritas untuk membuka informasi yang telah disandikan.
2. Integritas Data (Message Integrity), berhubungan dengan penjagaan (perlindungan data) dari upaya-upaya pengubahan data secara tidak sah. Untuk dapat menjaga integritas data, suatu sistem harus memiliki kemampuan untuk mendeteksi pemanipulasian data yang dilakukan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pendistribusian data lain ke dalam data yang asli.
3. Autentifikasi (Authentication), berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomuniasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diautentikasi keasliannya, isi datanya, waktu pengirimannya dan lain sebagainya.
4. Nirpenyangkalan (Non-repudiation), merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat, juga sebaliknya.

Sejarah Kriptografi

Kriptografi memiliki sejarah yang panjang dan mengagumkan. Penulisan rahasia ini dapat dilacak kembali ke 3000 tahun SM saat digunakan oleh bangsa Mesir. Mereka menggunakan hieroglyphcs untuk menyembunyikan tulisan dari pihak yang tidak diharapkan. Hieroglyphcs diturunkan dari bahasa Yunani hieroglyphica yang berarti “ukiran rahasia”. Hieroglyphs berevolusi menjadi hieratic, yaitu stylized script yang lebih mudah untuk digunakan (Rahayu. F.S., 2005). Sekitar 400 SM, kriptografi militer digunakan oleh bangsa Spartan dalam bentuk sepotong papyrus atau perkamen dibungkus dengan batang kayu. Sistem ini disebut Scytale. Sekitar 50 SM, Julius Caesar, kaisar Roma, menggunakan cipher substitusi untuk mengirim pesan ke Marcus Tullius Cicero. Pada cipher ini, huruf huruf alfabet disubstitusi dengan huruf-huruf yang lain pada alfabet yang sama. Pada tahun 20-an, Herbert O. Yardley bertugas pada organisasi rahasia US MI 8 yang dikenal sebagai “Black Chamber”. MI-8 menjebol kode-kode sejumlah negara. Selama konferensi Angkatan Laut Washington tahun 1921-1922, US membatasi negosiasi dengan Jepang karena MI-8 telah memberikan rencana negosiasi Jepang yang telah disadap oleh sekretaris negara US. Departemen negara menutup MI-8 pada tahun 1929 sehingga Yardley merasa kecewa. Sebagai wujud kekecewaanya, Yardley menerbitkan buku The American Black Chamber, yang menggambarkan kepada dunia rahasia dari MI-8. Sebagai konsekuensinya, pihak Jepang menginstal kode-kode baru. Karena kepeloporannya dalam bidang ini, Yardley dikenal sebagai “Bapak Kriptografi Amerika.

Enkripsi dan Dekripsi

Enkripsi ialah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan dan atau alat khusus. Sedangkan dekripsi merupakan algoritma atau cara yang dapat digunakan untuk membaca informasi yang telah dienkripsi untuk dapat dibaca kembali (Kurniawan. Y., 2004). Cara yang digunakan untuk melakukan enkripsi ialah dengan cara melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai sebuah kode atau cipher. Sebuah cipher menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari sebuah pesan menjadi cryptogram yang tidak dapat dimengerti (Aryus. D., 2005). Dengan demikian keamanan suatu pesan tergantung pada kunci-kunci yang digunakan, dan tidak tergantung pada algoritma yang digunakan. Sehingga algoritma algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis. (Kristanto. A., 2003).

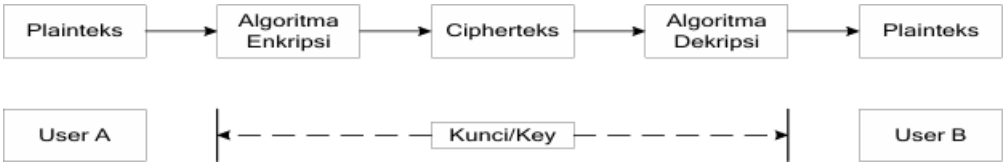
Terdapat tiga kategori enkripsi, yaitu:

1. Kunci enkripsi rahasia. Dalam hal ini, terdapat sebuah kunci yang digunakan untuk mengenkripsi dan juga sekaligus mendekripsikan informasi.
2. Kunci enkripsi publik. Dalam hal ini, terdapat dua kunci yang digunakan, satu kunci untuk proses enkripsi dan kunci yang lain untuk proses dekripsi.
3. Fungsi one-way (fungsi satu-arah) Suatu fungsi dimana informasi dienkripsi untuk menciptakan signature dari informasi asli yang bisa digunakan untuk keperluan autentikasi Terdapat dua macam teknik enkripsi yang biasa digunakan dalam sistem keamanan pada sistem komputer dan jaringan, yaitu teknik enkripsi konvensional dan teknik enkripsi publik.

Enkripsi Konvensional (Kunci Simetri)

Pada enkripsi konvensional, kunci yang digunakan untuk mendekripsikan cipherteks ialah kunci yang sama dengan kunci yang digunakan saat mengenkripsi plainteks.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.44

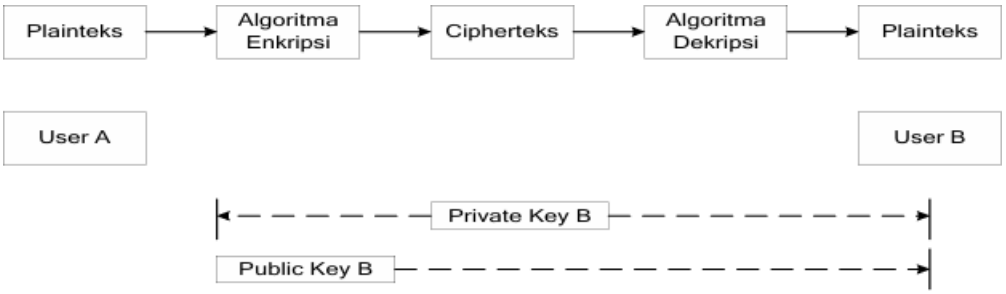


Gambar 1. Proses Enkripsi – Dekripsi pada Enkripsi Konvensional

Keamanan pada enkripsi konvensional terdiri dari beberapa faktor. Pertama, algoritma enkripsi harus cukup kuat sehingga menjadikan kriptanalis sangat kesulitan dalam mendekripsikan cipherteks. Kedua, bergantung pada kerahasiaan kuncinya, yaitu tidak perlu merahasiakan algoritma, tetapi cukup merahasiakan kuncinya.

Enkripsi Kunci Publik

Kelemahan yang terdapat pada enkripsi konvensional yaitu perlunya mendistribusikan kunci yang digunakan dalam keadaan aman. Ada cara agar tidak perlu lagi mendistribusikan kunci, cara tersebut dikenal dengan nama enkripsi kunci publik.



Gambar 2. Proses Enkripsi – Dekripsi pada Enkripsi Kunci Publik

METODE PENELITIAN

Penelitian dalam skripsi ini dilakukan dengan beberapa tahapan, yaitu:

1. **Studi Literatur**

Penulisan ini dimulai dengan studi kepustakaan yaitu mengumpulkan bahanbahan referensi baik dari buku, artikel, jurnal, makalah, maupun situs internet mengenai algoritma kriptografi simetri IDEA, konsep matematis yang mendasarinya, serta bahasa pemrograman untuk pambuatan aplikasinya, dan beberapa referensi lainnya.

2. **Analisis masalah**

Pada tahap ini dilakukan analisis terhadap algoritma kriptografi simetri IDEA,yakni meliputi XOR, penjumlahan modulo dan inversnya, serta perkalian modulo (+1) dan inversnya dari aspek matematis dan proses penyandian kemudian menerapkannya pada algoritma kriptografi simetri IDEA.

3. **Perancangan Sistem**

Pada tahap ini, sistem dirancang sehingga dapat menjamin keamanan data

4. **Pengkodean**

Pada tahap ini, sistem yang telah dirancang kemudian diimplementasikan menggunakan bahasa pemrograman C++.

5. **Pengujian**

Pada tahap ini, menguji program dan mencari kesalahan pada program hingga program itu dapat berjalan sesuai dengan yang dirancang

6. **Penyusunan laporan dan kesimpulan akhir**

Pada tahap ini, menyusun laporan hasil analisis dan perancangan kedalam format penulisan skripsi dengan disertai kesimpulan akhi.

HASIL DAN PEMBAHASAN

Pada tahap ini, hasil dari implementasi sistem keamanan data menggunakan algoritma kriptografi simetri IDEA akan dibahas secara rinci. Hasil yang diperoleh mencakup pengujian fungsionalitas perangkat lunak analisis keamanan, serta kemudahan penggunaan oleh pengguna awam.

Pengujian Fungsionalitas

Setelah sistem diimplementasikan menggunakan bahasa pemrograman C++, pengujian dilakukan untuk memastikan bahwa semua fitur berfungsi dengan baik. Pengujian ini mencakup:

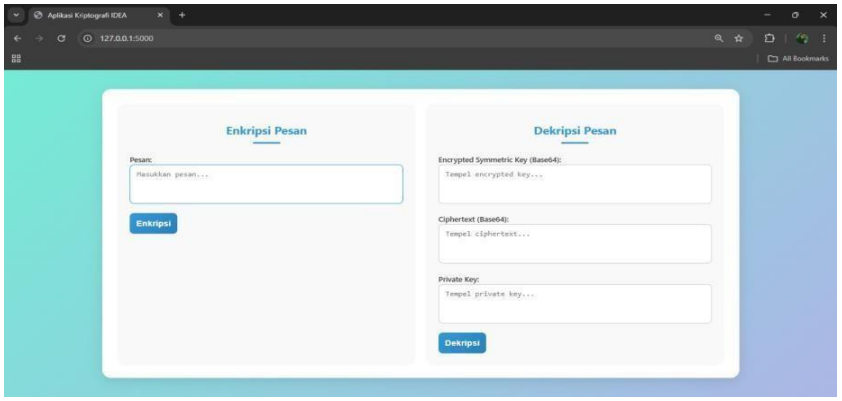
JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.44

- Enkripsi dan Dekripsi: Pengujian dilakukan dengan menggunakan berbagai jenis data input, termasuk teks biasa dan data biner. Hasil enkripsi diuji untuk memastikan bahwa data yang dienkripsi tidak dapat dibaca tanpa kunci yang tepat. Dekripsi juga diuji untuk memastikan bahwa data yang dienkripsi dapat dikembalikan ke bentuk aslinya dengan benar.
- Kecepatan Proses: Waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi diukur. Hasil menunjukkan bahwa algoritma IDEA dapat memproses data dengan cepat, sehingga cocok untuk aplikasi yang memerlukan pengolahan data dalam waktu nyata.
- Ketersediaan Antarmuka Pengguna: Antarmuka pengguna dirancang untuk memudahkan pengguna dalam melakukan enkripsi dan dekripsi. Uji coba dilakukan dengan melibatkan pengguna awam untuk mendapatkan umpan balik mengenai kemudahan penggunaan.

Analisis Keamanan

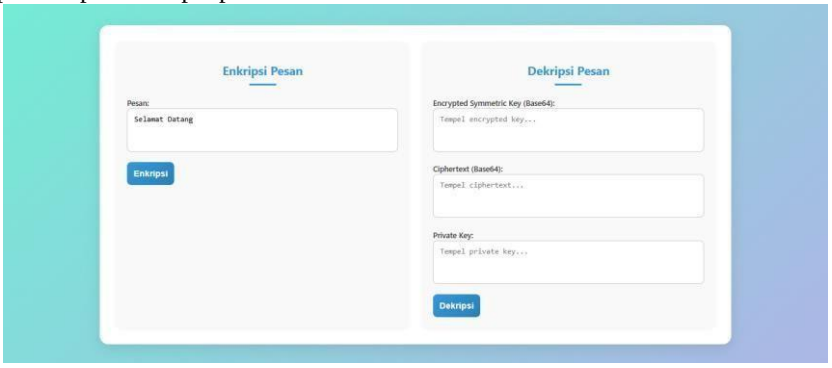
Keamanan sistem diuji dengan melakukan analisis terhadap kekuatan algoritma IDEA dalam menghadapi berbagai serangan kriptanalisis. Beberapa aspek yang dianalisis meliputi:

- Kekuatan Kunci: Algoritma IDEA menggunakan kunci sepanjang 128 bit, yang memberikan tingkat keamanan yang tinggi. Analisis menunjukkan bahwa jumlah kemungkinan kunci yang sangat besar membuat serangan brute force menjadi tidak praktis.
- Resistensi terhadap Serangan: Uji coba dilakukan untuk mengevaluasi ketahanan algoritma terhadap serangan diferensial dan linear. Hasil menunjukkan bahwa IDEA memiliki ketahanan yang baik terhadap kedua jenis serangan tersebut, berkat struktur dan proses enkripsi yang kompleks.
- Keamanan Kunci: Penekanan pada pentingnya menjaga kerahasiaan kunci juga dibahas. Sistem ini dirancang untuk memastikan bahwa kunci tidak disimpan dalam bentuk yang mudah diakses, dan pengguna diingatkan untuk mengganti kunci secara berkala.



Gambar 3. Tampilan antarmuka website

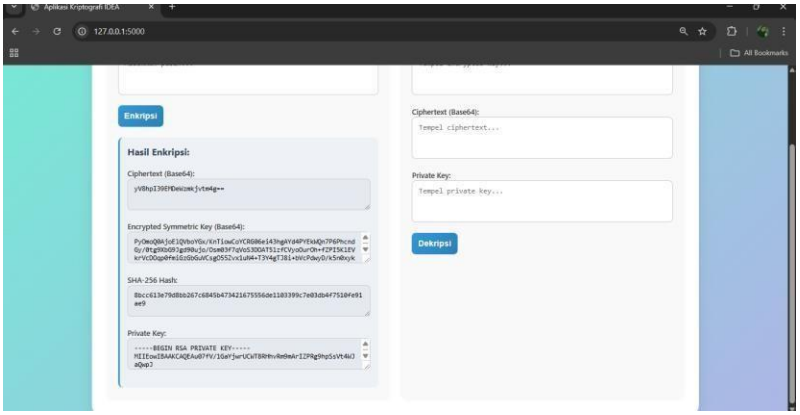
Pada Gambar 3, ditampilkan antarmuka utama website yang menyediakan fitur untuk memasukkan pesan yang akan dienkripsi atau didekripsi. Pada halaman ini, terdapat tiga elemen input utama, yaitu kolom input untuk memasukkan pesan (Enter your message), pilihan mode operasi (Encrypt atau Decrypt), dan kolom input untuk memasukkan kunci (key). Website ini dirancang untuk memudahkan pengguna dalam satu halaman tanpa navigasi tambahan, sehingga interaksi menjadi lebih cepat dan efisien. Antarmuka yang sederhana ini bertujuan untuk meningkatkan pengalaman pengguna dalam melakukan proses enkripsi maupun dekripsi pesan.



Gambar 4. Tampilan pengguna isi pesan

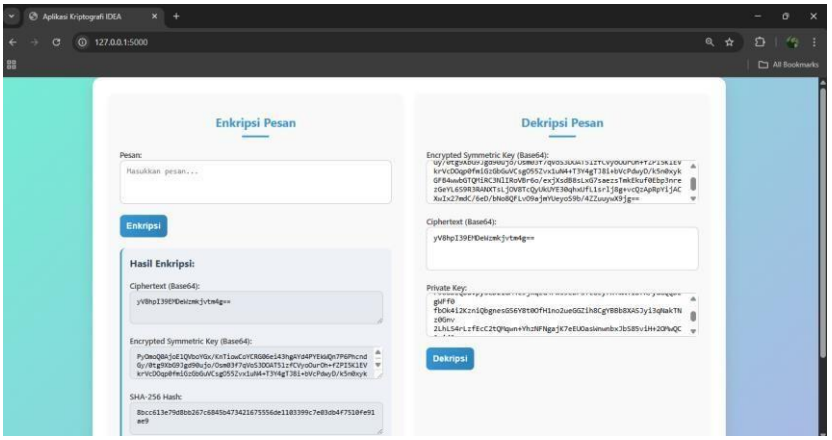
JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.44

Gambar 4 menunjukkan tahap di mana pengguna telah mengisi pesan yang ingin dienkripsi ke dalam kolom input yang tersedia dan memilih opsi Encrypt pada mode operasi. Pemilihan mode Encrypt ini menandakan bahwa pesan yang dimasukkan akan diproses untuk diubah menjadi ciphertext menggunakan kunci yang akan dimasukkan pada tahap berikutnya. Pada tahap ini, ketelitian pengguna dalam memilih mode sangat penting karena menentukan proses algoritma kriptografi yang akan dieksekusi pada data yang diberi.



Gambar 5. Pengguna memasukkan kunci

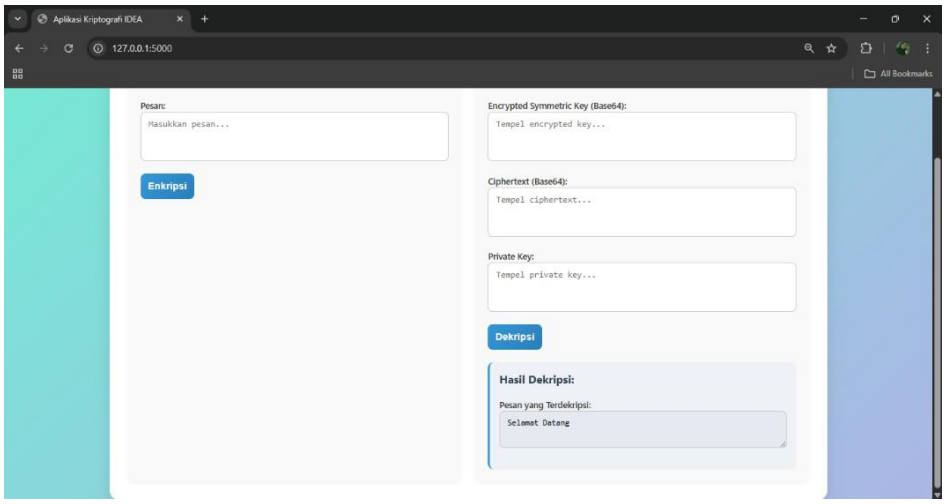
Pada Gambar 5, pengguna melanjutkan dengan memasukkan kunci ke dalam kolom yang telah disediakan. Kunci ini bersifat wajib untuk proses enkripsi, karena algoritma kriptografi yang digunakan mengandalkan kesesuaian kunci untuk mengamankan atau membuka pesan. Kunci yang dimasukkan harus dijaga kerahasiaannya, karena siapa pun yang mengetahui kunci tersebut dapat mendekripsi



Gambar 6. Tombol submit pengguna

Gambar 6 menampilkan tahap saat pengguna menekan tombol **Submit** setelah mengisi pesan, memilih mode Encrypt, dan memasukkan kunci. Tombol ini berfungsi untuk mengeksekusi permintaan enkripsi melalui server atau melalui script client-side. Pada tahap ini, website akan memproses input dan menghasilkan output berupa pesan yang telah dienkripsi.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.44



Gambar 7. pengguna pengiriman pesan aman

Gambar 7 Pengguna dapat menyalin hasil ini untuk digunakan dalam pengiriman pesan yang aman. Website menampilkan pesan dalam bentuk terenkripsi pada bagian output. Jika pengguna memilih mode Decrypt dengan memasukkan pesan terenkripsi dan kunci yang sesuai, maka hasil output yang muncul adalah pesan asli sebelum dienkripsi.

KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem keamanan data menggunakan algoritma kriptografi simetri IDEA (International Data Encryption Algorithm) dengan tujuan menciptakan perangkat lunak yang aman namun tetap mudah digunakan oleh masyarakat umum. Hasil pengujian menunjukkan bahwa:

1. Fungsionalitas sistem bekerja dengan baik dalam melakukan proses enkripsi dan dekripsi terhadap berbagai jenis data, termasuk teks biasa dan data biner.
2. Kecepatan proses enkripsi dan dekripsi tergolong cepat, sehingga sesuai digunakan untuk aplikasi yang membutuhkan pemrosesan data secara real-time.
3. Antarmuka pengguna dirancang dengan mempertimbangkan kemudahan penggunaan oleh pengguna awam, dan uji coba membuktikan bahwa sistem ini cukup mudah dioperasikan. Dari segi keamanan, algoritma IDEA terbukti memiliki:
   - Kekuatan kunci yang tinggi (128-bit) sehingga tahan terhadap serangan brute force
   - Resistensi yang baik terhadap serangan diferensial dan linear
   - Perlindungan terhadap kebocoran kunci dengan tidak menyimpan kunci dalam bentuk yang mudah diakses serta menganjurkan penggantian kunci secara berkala.

UCAPAN TERIMA KASIH

Alhamdulillah, segala puji bagi Allah Subhanahu wa Ta'ala atas rahmat dan hidayah-Nya sehingga saya dapat menyelesaikan jurnal ini yang berjudul "Perancangan dan Implementasi Sistem Keamanan Data Menggunakan Algoritma Kriptografi Simetri IDEA".

Saya mengucapkan terima kasih kepada dosen pembimbing atas bimbingannya, kepada orang tua dan keluarga atas doa dan dukungannya, serta kepada teman-teman yang selalu memberikan semangat.

Semoga jurnal ini bermanfaat dan menjadi amal kebaikan. Aamiin.

REFERENSI

Alasi, T. S., Wanto, R. & Sitanggang, V. H., 2021. Implementasi Kriptografi Algoritma IDEA Pada Keamanan Data Teks Berbasis Android. Jurnal Informasi Komputer Logika, Volume Vol.2 No.1

ISSN:2655-7002.] Schneier, Bruce. (1996). Cryptography 2nd. John Wiley & Sons.. N., Jamaludin & Romindo, 2020. Kriptografi Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere

Cipher dan RSA. Medan: Yayasan Kita Menulis.. Mukhtar, H., 2018. Kriptografi Untuk Keamanan Data. Yogyakarta: Deepublish. Pamungkas, C. A., 2017. Pengantar dan Implementasi Basis Data. Yogyakarta: Penerbit Deepublish.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.44

Rusmala & Prasti, D., 2019. Implementasi Metode Rail Fence Chiper dan Row Transposition Chiper Pada Mata Kuliah Kriptografi. Jurnal Ilmiah d'Computare , Volume Vol.9