Journal of Science and Social Research ISSN 2615 – 4307 (Print)
April 2026, IX (2): 1742 – 1747 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI SIMETRI IDEA (*INTERNATIONAL DATA ENCRYPTION ALGORITHM*)

Ahmad Rasyid Ridho[1], Yusuf Ramadhan Nasution[2], Suhardi[3], Muniruddin[4]
Universitas Islam Negeri Sumatera Utara, Medan
e-mail: arasyidridho25@gmail.com

Abstract: *Data security is a crucial and urgent issue to address, especially with the increasing number of cyber threats such as hacking attacks, data theft, and malware that can cause material and non-material losses to individuals and organizations. This study aims to implement the International Data Encryption Algorithm (IDEA) symmetric cryptography algorithm to secure text data in .xls format files that are often used to store important and confidential documents. More specifically, this study was conducted to secure .xls file data using the IDEA algorithm and to design and develop a web-based data security application that utilizes the International Data Encryption Algorithm (IDEA) algorithm. The IDEA algorithm is implemented in a web application built using the PHP programming language, where the encryption process is carried out by converting text data from .xls files into ciphertext that cannot be read by humans or machines without the right key, while the decryption process is carried out to return the data to its original form. The results of the study show that the IDEA algorithm is able to encrypt and decrypt .xls files effectively and efficiently with a relatively fast processing time and a very high level of security against various attacks, including brute force attacks.*

Keywords: *Data Security, Cryptography, IDEA Algorithm, Symmetric Encryption, Web Application*

Abstrak: Keamanan data menjadi salah satu isu yang sangat krusial dan mendesak untuk diatasi, terutama dengan semakin meningkatnya berbagai jenis ancaman siber seperti serangan *hacking*, pencurian data, dan *malware* yang dapat menyebabkan kerugian material maupun non-material bagi individu maupun organisasi. Penelitian ini bertujuan untuk mengimplementasikan algoritma kriptografi simetri *International Data Encryption Algorithm* (IDEA) guna mengamankan data teks pada file berformat .xls yang sering digunakan untuk menyimpan dokumen penting dan rahasia. Secara lebih spesifik, penelitian ini dilakukan untuk mengamankan data file .xls menggunakan algoritma IDEA dan merancang serta mengembangkan aplikasi pengamanan data berbasis web yang memanfaatkan algoritma *International Data Encryption Algorithm* (IDEA). Algoritma IDEA diimplementasikan pada aplikasi web yang dibangun menggunakan bahasa pemrograman PHP, di mana proses enkripsi dilakukan dengan mengonversi data teks dari file .xls menjadi *ciphertext* yang tidak dapat dibaca oleh manusia maupun mesin tanpa kunci yang tepat, sedangkan proses dekripsi dilakukan untuk mengembalikan data ke bentuk aslinya. Hasil penelitian menunjukkan bahwa algoritma IDEA mampu mengenkripsi dan mendekripsi file .xls secara efektif dan efisien dengan waktu proses yang relatif cepat serta tingkat keamanan yang sangat tinggi terhadap berbagai serangan, termasuk *brute force attack*.

Kata Kunci: Keamanan Data, Kriptografi, Algoritma IDEA, Enkripsi Simetri, Aplikasi Web

PENDAHULUAN

Salah satu teknologi yang sangat

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
April 2026, IX (2): 1742 – 1747 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

berperan dalam melindungi data adalah kriptografi. Kriptografi merupakan ilmu dan seni untuk mengamankan data dengan cara mengubah informasi menjadi format yang tidak dapat dibaca oleh pihak yang tidak berwenang (Aswandi et al., 2025). Melalui teknik-teknik seperti enkripsi dan dekripsi, kriptografi memungkinkan data dapat disimpan dan dikirim dengan aman, sehingga hanya pihak yang memiliki kunci tertentu yang dapat mengakses informasi tersebut (Alfinatul Umam et al., 2025).

Salah satu insiden yang menyoroti pentingnya kriptografi adalah serangan *ransomware* pada Pusat Data Nasional. Dalam serangan ini, penyerang berhasil mengenkripsi data kritis milik pemerintah dan organisasi publik, memaksa mereka untuk membayar tebusan untuk mendapatkan kembali akses ke data mereka. Sebelumnya terdapat penelitian (Devlin, 2021) yang membahas mengenai pengaman *database* sekolah SMK Pembangunan dalam bentuk *file excel*. Ada juga penelitian oleh (TS Alasi, R Wanto, VH Sitanggang, 2020) yang membahas pengamanan data teks berbasis Android.

Berdasarkan latar belakang di atas, penulis mencoba membuat suatu rancangan keamanan data menggunakan algoritma enkripsi IDEA yang berjudul Perancangan dan Implementasi Sistem Keamanan Data menggunakan Algoritma Kriptografi Simetri IDEA (*Internasional Data Encryption Algorithm*).

METODE

Teknik Pengumpulan Data

Teknik pengumpulan data yang dilakukan dalam penelitian ini adalah sebagai berikut:

Studi Literatur

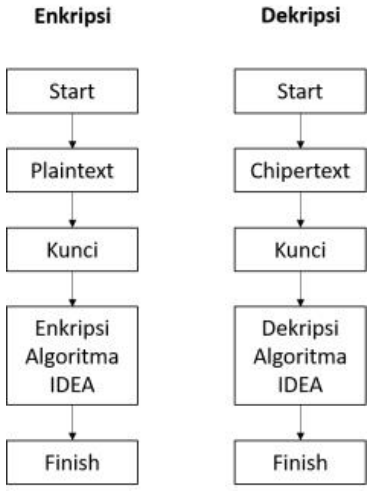
Penelitian ini menggunakan studi literatur di mana teknik pengumpulan data dilakukan dengan mencari informasi pengetahuan serta referensi dari berbagai sumber mulai dari buku, skripsi, jurnal atau artikel ilmiah, *website* resmi serta sumber lainnya yang berkaitan penelitian sebelumnya terutama tentang algoritma IDEA (Firdaus et al., 2023; Syakina & Nurdiati, 2021).

Data Laporan

Penelitian ini menggunakan data laporan untuk mengumpulkan data yang akan diteliti, baik yang berupa file berekstensi xls (Romdona et al., 2025).

Perancangan

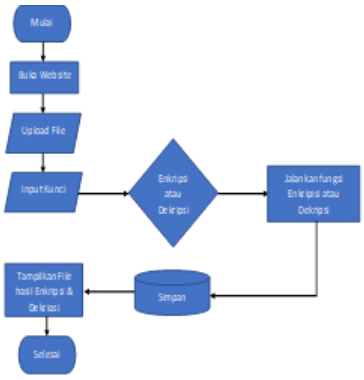
Pada tahapan ini, dari semua data dan analisis yang telah dikumpulkan maka dibentuk konsep desain perancangan sistem pengamanan file dengan menggunakan algoritma IDEA.



Gambar 1 Diagram Algoritma IDEA

Flowchart

Berikut ini adalah *flowchart* dari penelitian ini.



Gambar 2 *Flowchart Website* Enkripsi dan Dekripsi IDEA

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
April 2026, IX (2): 1742 – 1747 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

HASIL DAN PEMBAHASAN

Analisis Proses

Algoritma IDEA berjalan pada plaintext sepanjang 64-bit dan menggunakan kunci sepanjang 128-bit. Proses enkripsi dan dekripsi dengan algoritma ini melibatkan 8 putaran, di mana setiap putaran terdiri dari 14 langkah. Setelah 8 putaran selesai, dilakukan transformasi yang menghasilkan *ciphertext* dalam format ASCII.

Kunci dibentuk dengan membagi kunci menjadi subkey kemudian menggesernya ke kiri sebanyak 25 bit. Dalam proses enkripsi dan dekripsi oleh algoritma IDEA, setiap putaran mengikuti langkah-langkah yang sama, termasuk perkalian, penjumlahan, perpangkatan, XOR, dan modulus, yang diulang 14 kali dalam satu putaran.

Pembentukan Kunci

Transformasi kunci 128-bit menjadi subkunci dalam IDEA menghasilkan total 52 segmen kunci pendek yang masing-masing memiliki panjang 16 bit. Secara operasional, delapan subkunci pertama dihasilkan langsung dari pembagian kunci induk secara sekuensial.

Selanjutnya, putaran perdana enkripsi akan mengonsumsi enam subkunci pertama dari rangkaian tersebut sebagai parameter input prosesnya. Untuk putaran kedua, masih dibutuhkan 4 *subkunci* tambahan, sehingga kunci 128bit awal tersebut digeser ke kiri sebanyak 25bit untuk mendapatkan 8 *subkunci* berikutnya yang akan mengisi kekurangan subkunci. Proses ini diulangi hingga putaran kedelapan sehingga terbentuk total 52 subkunci baru.

Untuk perhitungan manual pembentukan kunci kata ilkompuinsujuara akan digunakan sebagai contoh kunci.

Konversi karakter ke *binary*

Tabel 1 Tabel Konversi Karakter Ke *Binary*

Karakter	Desimal	Biner
i	105	01101001
l	108	01101100
k	107	01101011
…	…	…
a	97	01100001

1. Penggabungan semua kunci
   01101001011011000110101101101111011011010111000001110101011010010110111001111001101110101010100111010101100001011100100110000101
2. Selanjutnya, kunci dibagi menjadi 8 grup, dengan masing-masing grup berukuran 16 bit, dan setiap grup diputar 25bit ke kiri untuk setiap putaran. Dalam satu putaran, terdapat 6 subkunci yang digunakan.

Tabel 2 Tabel Pembentukan Subkunci

	K1	K2	K3
Putaran 1	01101001 01101100	01101011 01101111	01101101 01110000
	K4	K5	K6
	01110101 01101001	01101110 01110011	01110101 01101010
Transformasi Output	K49	K50	K51
	11011011 11011011	01011100 00011101	01011010 01011011
	K52		
	10011100 11011101		

3. Empat subkunci terakhir disimpan untuk digunakan pada proses enkripsi dan dekripsi.

K49 = 1101101111011011
K50 = 0101110000011101
K51 = 0101101001011011
K52 = 1001110011011101

Proses Enkripsi

Proses enkripsi dengan algoritma IDEA dilakukan sebagai berikut: pertama, *plaintext* sepanjang 64bit dibagi menjadi 4 subblok, masing-masing berukuran 16 bit, yaitu X1, X2, X3, dan X4.

Sebagai contoh plaintext yang digunakan dalam proses perhitungan manual peneliti memakai kata ‘sumatera’.

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
April 2026, IX (2): 1742 – 1747 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Tabel 3 Plainteks Diubah Ke Biner

Plainteks	Subblok	Biner
su	X1	0111001101110101
ma	X2	0110110101100001
te	X3	0111010001100101
ra	X4	0111001001100001

Keempat subblok ini menjadi masukan untuk setiap iterasi tahap pertama pada algoritma IDEA, yang nantinya terdiri dari total 8 iterasi. Setiap iterasi terdapat 14 kali proses. Setelah sudah 8 iterasi dan proses transformasi output sudah dilakukan, maka tahap enkripsi sudah selesai dan didapatkan Y1, Y2, Y3 dan Y4 sebagai hasil enkripsi.

Tabel 4 Konversi Bilangan Biner Ke Kode Ascii

	Biner	Chiperteks
Y1	10111101 10110011	½³
Y2	00110100 11101011	4ë
Y3	01010111 00010101	W
Y4	11000101 00101110	Å.

Lalu dikonversikan ke kode ascii yang dipisah menjadi 8bit, sehingga didapatkan *chiperteks* dari *plainteks* ‘sumatera’ adalah ½³4ëWÅ.

Proses Dekripsi

Proses dekripsi adalah kebalikan dari enkripsi, di mana *ciphertext* diubah kembali menjadi plaintext menggunakan algoritma kriptografi IDEA (Nugraha, 2024). Untuk mendapatkan *plaintext*, diperlukan *ciphertext* dan kunci publik yang sama dengan yang digunakan pada enkripsi (Setyawan et al., 2024). Perbedaannya hanya terletak pada invers perkalian dan invers penjumlahan dalam setiap langkah putaran dekripsi, yang terdiri dari 8 putaran. Proses dekripsi dari *ciphertext* ½³4ëWÅ dan kunci ilkompuinsujuara segabai berikut (Widyanto, 2024):

Chiperteks di konversi dulu ke biner:
X1 = ½³ = 1011110110110011
X2 = 4ë = 0011010011101011
X3 = W = 0101011100010101
X4 = Å. = 1100010100101110

Hasil dari konversi inilah yang akan di jadikan X1, X2, X3 dan X4 pada proses dekripsi, sedangkan untuk sub kunci K1, K2, K3, K4, K5 dan K6 sama seperti pada tabel sebelumnya karena kuncinya sama dengan proses enkripsi.
Setelah melewati 8 iterasi dan juga proses transformasi *output* didapatkan hasil Y1, Y2, Y3 dan Y4. Kemudian dikonversikan menggunakan kode ascii dan didapatkan hasil dekripsi dari *chiperteks* ½³4ëWÅ adalah sumatera.

Tabel 5 Konversi Bilangan Biner Ke Teks

	biner	plainteks
Y1	01110011 01110101	su
Y2	01101101 01100001	ma
Y3	01110100 01100101	te
Y4	01110010 01100001	ra

Perancangan Antarmuka

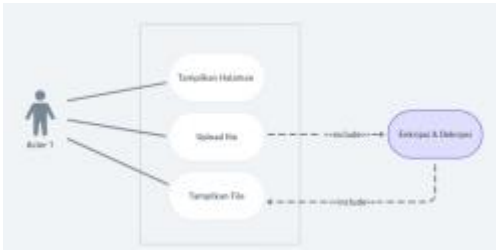
Perancangan antarmuka ini berisikan tentang rancangan tampilan *website* dalam memasukan file, kunci public dan hasil file yang telah dienkripsi atau dekripsi.

Gambar 3 Rancangan antarmuka

Use Case Diagram

Use case diagram dapat digunakan sebagai dasar untuk pengembangan lebih lanjut dan pengujian sistem, memastikan bahwa semua kasus penggunaan yang diidentifikasi telah diimplementasikan dan diuji dengan benar.

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
April 2026, IX (2): 1742 – 1747 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR



Gambar 4 *Use Case Diagram*

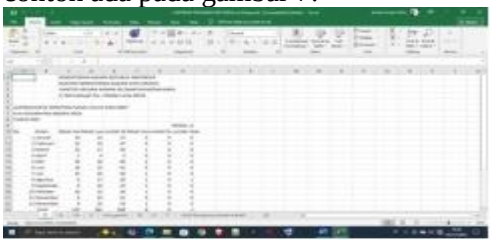
Pengujian

Gambar 5 Tampilan *Website*

Data yang sudah di enkripsi atau dekripsi bisa langsung di unduh dihalaman web dengan menekan tombol unduh, file enkripsi yang sudah di unduh jika dibuka akan menampilkan data teks yang terlihat seperti acak-acakan karena sudah di enkripsi dengan algoritma IDEA seperti pada gambar 6. berikut.

Gambar 6. File Hasil Enkripsi Algoritma IDEA

Dan jika file dekripsi di unduh maka akan menampilkan teks seperti pada awal mula sebelum di enkripsi, sebagai contoh ada pada gambar 7.



Gambar 7 File Hasil Dekripsi Algoritma IDEA

SIMPULAN

Berdasarkan penelitian yang telah dilakukan dapat diperoleh kesimpulan sebagai berikut ini hasil penelitian menunjukkan bahwa penelitian ini berhasil secara baik dalam mengaplikasikan algoritma IDEA untuk melindungi keamanan data teks. Algoritma IDEA dapat melakukan enkripsi dan deskripsi data secara efektif. Dengan kunci enkripsi 128-bit dan struktur algoritma yang kompleks, terbukti memberikan tingkat keamanan yang tinggi terhadap data yang diolah. Sistem ini mempermudah pengguna dalam melakukan proses enkripsi dan dekripsi tanpa memerlukan pemahaman teknis mendalam mengenai algoritma kriptografi yang digunakan.

DAFTAR PUSTAKA

Alfinatul Umam, R., Tahir, M., Maulidia, I., & Zam Zami, Z. (2025). REALISASI KRIPTOGRAFI KLASIK MENGGUNAKAN CAESAR CIPHER DAN VIGENÈRE CIPHER PADA PLATFORM APLIKASI WEB. *Jurnal Mahasiswa Teknik Informatika)*, *9*(4), 7035–7041.

Aswandi, A. S., Nurtanzis Sutoyo, M., & Pradipta, A. (2025). ANALISIS PERFORMA DAN KEAMANAN IMPLEMENTASI KRIPTOGRAFI AES UNTUK PENYANDIAN DOKUMEN BERBASIS WEB. *Jurnal MNEMONIC*, *8*(1), 24–32.

Firdaus, F., Sukmawati, M., Ambiyar, A., & Fadhilah, F. (2023). Studi Literature Penggunaan Media Pembelajaran Berbasis Moodle pada Sekolah Kejuruan. *JAVIT : Jurnal Vokasi Informatika*, 133–139. https://doi.org/10.24036/javit.v3i3.163

Nugraha, S. N. (2024). PENERAPAN ALGORITMA KRIPTOGRAFI ELGAMAL PADA APLIKASI PENGAMANAN PESAN

BERBASIS WEBSITE. *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(3), 2513–2524. https://doi.org/10.23960/jitet.v12i3.4

Romdona, S., Senja Junista, S., & Gunawan, A. (2025). TEKNIK PENGUMPULAN DATA: OBSERVASI, WAWANCARA DAN KUESIONER. *JISOSEPOL: JURNAL ILMU SOSIAL EKONOMI DAN POLITIK*, *3*(1), 39–47. https://samudrapublisher.com/index.php/JISOSEPOL

Setyawan, A. B., Khaerudin, M., & Setiawati, S. (2024). Perancangan Aplikasi Enkripsi Dan Dekripsi Gambar Cetak Biru Pada PT. Patco Elektronik Teknologi Menggunakan Algoritma RSA Berbasis Android. *NUANSA INFORMATIKA*, *18*(2), 19–25.

Syakina, L., & Nurdiati, S. (2021). STUDI LITERATUR: Analisis Distribusi Masalah Lokasi Fasilitas untuk Logistik Bantuan Kemanusiaan. *Jurnal Pijar Mipa*, *16*(2), 207–214. https://doi.org/10.29303/jpm.v16i2.2469

WIDYANTO, A. (2024). IMPLEMENTASI KRIPTOGRAFI TEKS MENGGUNAKAN RSA. *Community Service Article (COMERS) e-ISSN*, *1*, 70–81.