JURNAL DEVICE, VOL. 15 NO 1, Mei 2025, 156-162
ISSN: 0216-9185 | eISSN: 2746-8984

PEMODELAN DAN SIMULASI ALGORITMA *DES (DATA ENCRYPTION STANDARD)* UNTUK ENKRIPSI DAN DEKRIPSI PESAN TEKS MENGGUNAKAN CRYPTOOL2

Fransiska P. Bele Bau [1)], Chrisntsia Kolo [2)], Riza F.B. Akoit [3)], Marcelino M. Correia [4)], Fernandino A. A. F. Manikin[5)]

[1)-5)]Program Studi Teknologi Informasi, Fakultas Pertanian, Sains dan Kesehatan, Universitas Timor
Email : novabelebau@gmail.com [1)], icenkolo91@gmail.com [2)], rizaakoit15@gmail.com [3)], marcelinocorreia08@gmail.com [4)], aldomanikin43@gmail.com [5)]

ABSTRAK

Keamanan data sangat penting dalam pertukaran informasi digital, terutama saat pesan teks dikirim melalui jaringan yang tidak aman dan rentan terhadap ancaman penyadapan. Untuk mengatasi hal ini, salah satu solusi yang diterapkan adalah enkripsi data menggunakan algoritma kriptografi. Penelitian ini berfokus pada pemodelan dan simulasi algoritma *DES* (*Data Encryption Standard)* untuk proses enkripsi dan dekripsi pesan teks dengan menggunakan perangkat lunak CrypTool2. Berbeda dengan studi sebelumnya yang menggunakan algoritma *TEA (Tiny Encryption Algorithm),* penelitian ini mengkhususkan pemodelan pada DES dengan pendekatan visual interaktif. Metode yang digunakan mencakup kajian pustaka dan pendekatan kuantitatif eksperimental. Pada tahap simulasi enkripsi, pesan teks dan kunci dimasukkan melalui *Text Input,* kemudian dikodekan dalam format ASCII dan UTF-8 sebelum diproses oleh algoritma DES dengan mode *ECB (Electronic Codebook*) dan *Padding Zeroes*. Hasil enkripsi ditampilkan dalam bentuk heksadesimal dan dapat divisualisasikan sebagai QR Code yang dapat disimpan dalam bentuk file. Proses dekripsi dilakukan dengan cara yang berlawanan untuk mengembalikan *chipertext* ke bentuk pesan asli. Hasil penelitian menunjukkan bahwa CrypTool2 dapat memvisualisasikan setiap tahap DES dengan rinci, sehingga memudahkan pemahaman tentang mekanisme enkripsi dan dekripsi. Pengujian terhadap 10 sampel file teks menunjukkan bahwa enkripsi dengan algoritma DES menyebabkan peningkatan ukuran file karena data dikodekan dalam format heksadesimal atau biner. Namun, setelah dekripsi, ukuran file kembali seperti semula, membuktikan bahwa DES mampu menjaga integritas data meskipun menambah ukuran file saat enkripsi.

Kata Kunci : *DES (Data Encryption Standard),* Enkripsi, Dekripsi, CrypTool2.

ABSTRACT

Data security is critical in the exchange of digital information, especially when text messages are sent over networks that are insecure and vulnerable to eavesdropping threats. To overcome this, one of the solutions implemented is data encryption using cryptographic algorithms. This research focuses on modeling and simulation of Data Encryption Standard (DES) algorithm for encryption and decryption of text messages using CrypTool2 software. Unlike the previous study that used the TEA algorithm(Tiny Encryption Algorithm), this study specializes in the analysis of DES with an interactive visual approach. The methods used include literature review and experimental quantitative approach. In the encryption simulation phase, text messages and keys are entered through Text Input, then encoded in ASCII and UTF-8 formats before being processed by DES algorithm with ECB (Electronic Codebook) mode and Padding Zeroes. The encryption result is displayed in hexadecimal form and can be visualized as a QR Code that can be stored in the form of a file. The desccription process is carried out in the opposite way to return the chipertext to the original banana shape. The results show that CrypTool2 can visualize each stage of DES in detail, making it easier to understand the encryption and decryption mechanisms. Testing of 10 sample text files showed that encryption with the DES algorithm led to an increase in file size because the data was encoded in hexadecimal or binary format. However, after the decryption, the file size returns to what it was, proving that DES is able to maintain data integrity despite increasing the size during encryption.

Keywords : DES (Data Encryption Standard), Encryption, Decryption, CrypTool2.

1. PENDAHULUAN

Keamanan data menjadi aspek penting yang harus diperhatikan oleh individu, perusahaan, dan pemerintahan. Informasi digital yang tersimpan dalam komputer atau jaringan rentan terhadap berbagai ancaman, seperti peretasan, pencurian data, dan serangan siber yang dapat merugikan banyak pihak. Keamanan siber sebagai upaya menjaga keamanan data merupakan serangkaian tindakan yang bertujuan untuk melindungi sistem dari berbagai ancaman, gangguan, dan serangan yang menargetkan jaringan komputer, baik dari sisi perangkat keras maupun perangkat lunak. Selain itu, keamanan siber juga mencakup perlindungan terhadap informasi yang tersimpan di dalamnya serta elemen-elemen lain yang terdapat dalam ruang siber (Aji, 2023). Serangan ini tidak hanya mengancam privasi pengguna, tetapi juga dapat menyebabkan kerugian finansial dan reputasi bagi organisasi. Sebagai upaya untuk melindungi data dari akses tidak sah, enkripsi digunakan sebagai metode keamanan yang efektif.

Enkripsi merupakan teknik yang dipakai untuk mengubah data menjadi bentuk yang tidak dapat dikenali, sehingga informasi tetap aman dan hanya bisa diakses setelah melalui proses dekripsi terlebih dahulu. Istilah *encryption* berasal dari bahasa Yunani *kryptos*, yang berarti tersembunyi atau rahasia (Putra Rahmadi & Hilda Dwi Yunita, 2020). Salah satu algoritma yang sering digunakan dalam proses enkripsi adalah *Data Encryption Standard (DES).*

Algoritma DES merupakan algoritma kriptografi simetris yang digunakan untuk mengenkripsi data elektronik. Meskipun ukuran kuncinya relatif pendek, algoritma ini memiliki peran penting dalam perkembangan kriptografi modern (Ariska & Wahyuddin, 2022). DES tergolong dalam jenis sandi *Feistel*, sehingga memiliki arsitektur yang mirip dengan struktur pada umumnya yang digunakan dalam algoritma *Feistel*. Ciri khas DES meliputi panjang blok sebesar 64 bit, dengan ukuran teks asli dan teks tersandi yang sama, yaitu 64 bit. Walaupun telah banyak digantikan oleh algoritma yang lebih mutakhir seperti *Advanced Encryption Standard (AES)*, DES masih kerap dimanfaatkan dalam studi dan riset di bidang kriptografi. Algoritma DES masih memiliki keunggulan karena dinilai lebih unggul dibandingkan algoritma XOR lainnya (Thahara & Siregar, 2021). Untuk memahami algoritma DES lebih mendalam, perangkat lunak CrypTool2 dapat digunakan untuk memodelkan, menyimulasikan, serta menganalisis keamanannya secara interaktif.

CrypTool adalah program yang dapat membantu menganalisis dan menjalankan prosedur kriptografi dalam antarmuka pengguna yang terintegrasi(Nurdin & Djuniadi, 2022). Salah satu versi lainnya adalah CrypTool2, yang dikembangkan sebagai program e-learning modern untuk Windows, yang memvisualisasikan kriptografi dan kriptanalisis. Aplikasi ini tidak hanya mencakup enkripsi dan kriptanalisis sandi, tetapi juga dasar-dasarnya dan seluruh spektrum kriptografi modern (CrypTool Contributors, 2021). Kemampuannya memvisualisasikan setiap tahap proses enkripsi dan dekripsi menjadikan CrypTool2 sebagai alat yang efektif dalam mempermudah pemahaman konsep kriptografi yang kompleks.

Pemodelan dan simulasi algoritma DES menjadi suatu kebutuhan penting untuk memahami secara mendalam cara kerja enkripsi dan dekripsi dalam algoritma tersebut. CrypTool2 adalah aplikasi open-source yang dibuat untuk mempelajari dan mensimulasikan berbagai jenis algoritma kriptografi, salah satunya adalah algoritma DES. Perangkat lunak ini memungkinkan pengguna untuk memahami proses enkripsi dan dekripsi secara lebih interaktif dan mendalam melalui visualisasi yang intuitif. CrypTool2 tidak hanya mendukung enkripsi dan dekripsi, tetapi juga menyediakan berbagai template serta fitur visual programming, yang memungkinkan pengguna untuk menggabungkan dan menjalankan fungsi kriptografi secara fleksibel (CrypTool Contributors, 2025). Dengan pendekatan ini, proses yang kompleks seperti

algoritma DES dapat divisualisasikan dengan lebih jelas, sehingga membantu dalam analisis dan pemahaman berbagai teknik kriptografi, termasuk kriptoanalisis dan keamanan data.

Penelitian sebelumnya yang dilakukan oleh "Muhammad Femy Mulya dan Nofia Rismawati" dengan judul "Analisis dan Simulasi Algoritma *TEA (Tiny Encryption Algorithm)* untuk Enkripsi dan Dekripsi Pesan Text Menggunakan CrypTool2" telah membahas simulasi enkripsi dan dekripsi pesan teks menggunakan algoritma *Tiny Encryption Algorithm (TEA)*. Tujuan dari penelitian ini adalah untuk menganalisis, merancang dan mengimplementasikan algoritma TEA dalam bentuk simulasi enkripsi dan dekripsi pesan teks, baik dalam bentuk teks biasa maupun file teks (Femy Mulya & Rismawati, 2019). Penelitian lainnya yang dilakukan oleh "M.Z. Yakubova, T.G. Serikov, D.A. Naubetov, dan S.A. Mirzakulova" dengan judul "*Modeling and Research of Cryptographic Algorithms DES, 3DES, AES, and RSA in the Cryptool Program*". Penelitian ini berfokus pada pemodelan dan analisis berbagai algoritma kriptografi menggunakan CrypTool, yaitu DES, 3DES, AES, dan RSA. Hasil penelitian menunjukkan bahwa ketika panjang kunci diubah (8, 16, dan 24 *byte*), nilai teks terenkripsi tetap tidak berubah, tetap isi pesannya berubah (Yakubova et al., 2022).

Berbeda dengan kedua penelitian tersebut, penelitian ini berfokus pada pemodelan dan simulasi algoritma DES untuk enkripsi dan dekripsi pesan teks menggunakan CrypTool2. Dengan fitur visualisasi yang interaktif, CrypTool2 memungkinkan pengguna untuk memahami setiap tahapan algoritma DES secara lebih jelas dan mendalam, sehingga dapat memberikan wawasan lebih dalam (Aji, 2023).

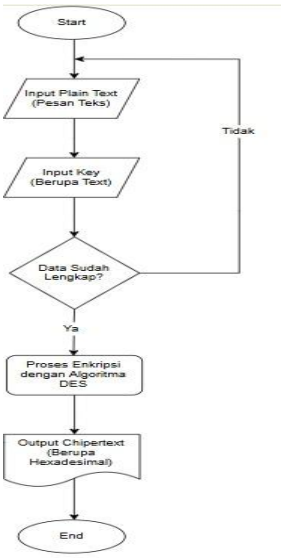
2. METODE

Untuk memahami cara kerja dan alur algoritma DES, diperlukan simulasi proses enkripsi dan dekripsi yang didukung oleh metode kuantitatif serta studi literatur. Studi literatur meliputi tinjauan pustaka yang membahas mengenai enkripsi dan dekripsi menggunakan algoritma DES. Metode kuantitatif dalam penelitian ini diterapkan melalui penelitian eksperimental, dengan cara menguji variabel-variabel input untuk mengevaluasi hasil atau output yang diperoleh (Femy Mulya & Rismawati, 2019). Penelitian ini juga bertujuan untuk mengetahui perbedaan antara dua perlakuan yang diberikan pada sampel tertentu. Agar data yang dihasilkan valid, reliabel, dan dapat diterapkan, maka diperlukan prinsip-prinsip eksperimen yang tepat. Selain itu, analisis data statistik digunakan untuk mendukung proses pengolahan dan interpretasi data secara objektif (Dianti, 2017).

3. HASIL DAN PEMBAHASAN

3.1. Tinjauan Alur Proses Simulasi Enkripsi dan Dekripsi Menggunakan Algoritma DES (Data Encryption Standard)

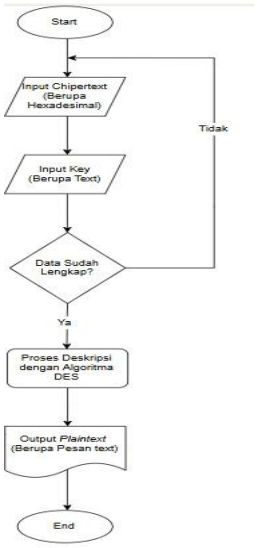
Analisis ini bertujuan untuk memahami mekanisme kerja algoritma DES melalui simulasi enkripsi dan dekripsi pesan teks.



Gambar 1. Flowchart Simulasi Enkripsi Algoritma *DES (Data Encryption Standard)*

Gambar 1 menampilkan sebuah diagram alur (flowchart) yang menggambarkan proses simulasi enkripsi dengan menggunakan algoritma DES. Langkah pertama yang dilakukan adalah

memasukkan input berupa *plaintext* (pesan teks) serta kunci (*key*) yang juga akan digunakan pada saat proses dekripsi. Setelah input dimasukkan, proses enkripsi dilakukan menggunakan algoritma DES, sehingga menghasilkan *chipertext* dalam format heksadesimal.

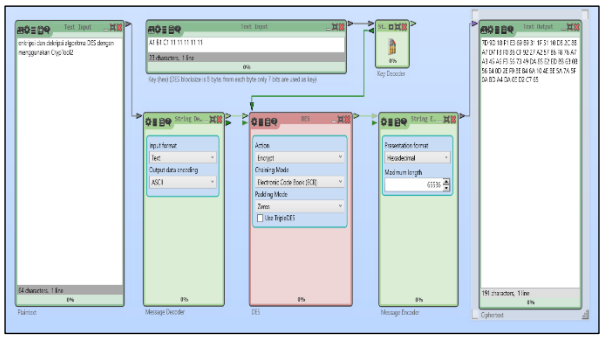


Gambar 2. Flowchart Simulasi Dekripsi Algoritma *DES (Data Encryption Standard)*

Pada flowchart simulasi dekripsi algoritma DES yang ditampilkan pada Gambar 2, diperlihatkan proses dekripsi untuk mengubah input berupa *chipertext* (dalam format heksadesimal) kembali ke bentuk pesan teks (*chipertext*). Langkah awal dimulai dengan memasukkan *ciphertext* yang merupakan hasil dari proses enkripsi, kemudian dilanjutkan dengan memasukkan kunci (*key*) yang identik dengan yang digunakan saat enkripsi. Setelah itu, algoritma DES digunakan untuk melakukan proses dekripsi hingga menghasilkan output berupa *plaintext* (teks pesan).

3.2. Simulasi Proses Enkripsi Algoritma *DES (Data Encryption Standard)* dengan CrypTool2

1. *Text Input* sebanyak 2 (dua) buah, yang satu digunakan untuk memasukkan *plaintext* (pesan teks) yang akan diubah menjadi *chipertext*, dan yang kedua untuk memasukkan *key* (kunci pada algoritma DES)
2. Sebuah *Message Decoder* digunakan untuk mengubah teks masukan menjadi format ASCII.
3. Sebuah *Key Decoder* digunakan untuk mengonversi input teks ke dalam format UTF-8.
4. Satu buah algoritma DES digunakan, dengan action yang dipilih adalah *Encrypt*, *Chaining Mode* diatur ke *Electronic Code Book (ECB)*, dan *Padding Mode* diatur ke *Zeroes*.
5. Hasil algoritma DES dapat diubah ke format hexadecimal dengan menggunakan *Message Encoder*.
6. Satu buah *Text Output* digunakan untuk menampilkan *chipertext* (dalam format hex)

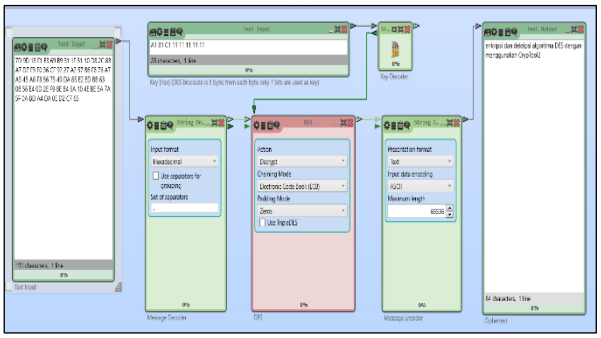


Gambar 3. Simulasi Enkripsi pada Algoritma DES dengan CrypTool

3.3. Simulasi Dekripsi Algoritma *DES (Data Encryption Standard)* dengan CrypTool2

1. *Input Text* sebanyak dua buah, satu untuk chipertext yang akan diubah menjadi pesan teks biasa, dan yang lain untuk memasukkan kunci pada algoritma DES.
2. Satu buah *Message Decoder* digunakan untuk mengonversi input berupa heksadesimal ke dalam format ASCII.
3. Input teks diubah ke dalam format UTF-8 dengan menggunakan *Key Decoder*.
4. Satu buah algoritma DES digunakan, dengan action yang dipilih adalah *Decrypt*, *Chaining Mode* diatur ke *Electronic Code Book (ECB)*, dan *Padding Mode* diatur ke Zeroes
5. Satu buah *Message Encoder* digunakan untuk mengonversi hasil perhitungan algoritma DES ke dalam format text.

6. Sebuah *Text Output* digunakan untuk menampilkan plaintext dalam format teks.



Gambar 4. Simulasi Dekripsi pada Algoritma DES dengan CrypTool

3.4. Pengujian Enkripsi dan Dekripsi Pesan Text Menggunakan Algoritma *DES (Data Encryption Standard)* dengan CrypTool2

Pengujian dilakukan untuk mempelajari cara kerja algoritma *DES (Data Encryption Standard)* menggunakan Cryptool2 dalam proses enkripsi dan dekripsi data berupa pesan teks. Pengujian ini menggunakan metode sampling dengan 10 sampel, masing-masing terdiri dari 10 file *plaintext* (dengan format .txt)

Tabel 1. Hasil Uji Coba Enkripsi dan Dekripsi Pesan Text Menggunakan algoritma DES (Data Encryption Standard) dengan CrypTool2

No	Pesan Text Asli		Enkripsi	Dekripsi
	Nama File (*.txt)	Ukuran Pesan Text Original (*byte*)	Ukuran (*byte*)	Ukuran (*byte*)
1	Sampel 1	137	431	137
2	Sampel 2	170	572	170
3	Sampel 3	191	575	191
4	Sampel 4	217	671	217
5	Sampel 5	273	839	273
6	Sampel 6	377	1151	377
7	Sampel 7	396	1199	396
8	Sampel 8	503	1511	503
9	Sampel 9	566	1703	566
10	Sampel 10	873	2639	873

4. PENUTUP

4.1. Kesimpulan

Berdasarkan hasil penelitian dan pengujian simulasi enkripsi dan dekripsi pesan teks menggunakan algoritma *DES (Data Encryption Standard)*, dapat disimpulkan bahwa ukuran file teks (dalam *byte*) setelah melalui proses enkripsi cenderung mengalami peningkatan dibandingkan dengan ukuran file asli. Hal ini disebabkan oleh proses pengkodean data hasil enkripsi yang biasanya dalam format heksadesimal atau biner. Di sisi lain, ukuran file teks (dalam *byte*) setelah proses dekripsi akan sama dengan ukuran file teks asli, karena data telah dikembalikan ke bentuk semula (*plaintext*) tanpa adanya tambahan *encoding*.

4.2. Saran

Berdasarkan hasil analisis dan temuan yang diperoleh dalam penelitian ini, terdapat beberapa poin yang dapat dijadikan arahan untuk pengembangan studi ke depan. Pertama, disarankan agar cakupan penelitian tidak hanya terbatas pada data teks, tetapi juga mencakup format data lain seperti gambar maupun audio guna mengevaluasi kinerja algoritma DES secara lebih menyeluruh. Kedua, penelitian selanjutnya dapat mempertimbangkan studi komparatif dengan algoritma kriptografi lain seperti AES dan RSA untuk mendapatkan pemahaman yang lebih utuh terkait efisiensi, kecepatan proses, dan tingkat keamanannya.

5. DAFTAR PUSTAKA

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in

Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Ariska, A., & Wahyuddin, W. (2022). Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard). *Jurnal Sintaks Logika*, *2*(2), 9–19. https://doi.org/10.31850/jsilog.v2i2.1734

CrypTool Contributors. (2021). *About CrypTool 2*. https://www.cryptool.org/en/ct2/

CrypTool Contributors. (2025). *About CrypTool 2*. Www.Cryptool.Org. https://www.cryptool.org/en/ct2/

Dianti, Y. (2017). Metode Penelitian Kuantitatif. In *Angewandte Chemie International Edition, 6(11), 951–952.* http://repo.iain-tulungagung.ac.id/5510/5/BAB 2.pdf

Femy Mulya, M., & Rismawati, N. (2019). Analisis Dan Simulasi Algoritma Tea (Tiny Encryption Algorithm) Untuk Enkripsi Dan Dekripsi Pesan Text Menggunakan Cryptool2. *Jurnal Sistem Komputer Dan Kecerdasan Buatan*, *3*(1).

Nurdin, A. A., & Djuniadi, D. (2022). Securing Audio Chat With Cryptool-Based Twofish Algorithm. *Journal of Soft Computing Exploration*, *3*(1), 37–43. https://doi.org/10.52465/joscex.v3i1.65

Putra Rahmadi, & Hilda Dwi Yunita. (2020). Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi. *Jurnal Cendikia*, *19*(1), 413–418.

Thahara, A., & Siregar, I. T. (2021). Implementasi Kriptografi untuk keamanan Data dan Jaringan menggunakan Algoritma DES. *Jurnal Rekayasa Teknologi Informasi (JURTI)*, *5*(1), 31. https://doi.org/10.30872/jurti.v5i1.5657

Yakubova, M. Z., Serikov, T. G., Naubetov, D. A., & Mirzakulova, S. A. (2022). Modeling and Research of Cryptographic Algorithms Des, 3Des, Aes and Rsa in the Cryptool Program. *Вестник Алматинского Университета Энергетики И Связи*, *4*, 114–126. https://doi.org/10.51775/2790-0886_2022_59_4_114