

APPLICATION OF CRYPTOGRAPHY WITH DATA ENCRYPTION STANDARD (DES) ALGORITHM IN PICTURE

Angga Aditya Permana¹, Desi Nurnaningsih²

^{1,2} Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Tangerang
Jalan Perintis Kemerdekaan 1/33 Cikokol Kota Tangerang
email : anggaamt@gmail.com¹, desi.nurnaningsih1986@gmail.com²

Abstract

Cryptography is the science of maintaining data confidentiality, where the original text (plaintext) is encrypted using an encryption key to be ciphertext (text that has been encrypted). In this case cryptography secures data from a third party so that the third party cannot know the original contents of the data because the one who holds the key for encryption and decryption is only the sender and receiver. There are several cryptographic methods that are commonly used, one of which is DES or Data Encryption Standard. DES is included in the key-symmetric cryptography and is classified as a block cipher type.

Article history

Received May 18, 2020
Revised May 19, 2019
Accepted May 27, 2019
Available online May 31, 2020

Keywords

Cryptograph
Algorithm
Date Encryption Standard

Abstrak

Kriptografi adalah ilmu untuk menjaga kerahasiaan data, dimana teks asli (plaintext) diacak menggunakan suatu kunci enkripsi menjadi ciphertext (teks yang sudah terenkripsi). Dalam hal ini kriptografi mengamankan data dari pihak ketiga agar pihak ketiga tersebut tidak dapat mengetahui isi asli dari data tersebut karena yang memegang kunci untuk enkripsi dan dekripsi hanya pengirim dan penerima. Terdapat beberapa metode kriptografi yang umum digunakan, salah satunya adalah DES atau Data Encryption Standard. DES termasuk ke dalam kriptografi kunci-simetris dan tergolong jenis block cipher.

Riwayat

Diterima 18 Mei 2020
Revisi 19 Mei 2020
Disetujui 27 Mei 2020
Terbit 31 Mei 2020

Kata Kunci

Kriptografi
Algoritma
Data Enkripsi Standar

PENDAHULUAN

Teknologi pada masa kini sudah mengalami perkembangan yang sangat pesat. Teknologi khususnya dalam bidang komunikasi telah memudahkan kita dalam berkomunikasi hanya lewat telepon genggam atau hp kita. Di sosial media kita dapat mengirimkan tidak hanya teks kita juga berbagai macam hal lain contohnya seperti audio, gambar, dan video.

Seiring dengan perkembangan teknologi komunikasi, keamanan dan kerahasiaan data dalam berkomunikasi menjadi hal yang krusial dan patut diperhatikan. Karena data yang akan dikirimkan adalah hal yang sangat berharga, keamaan dibutuhkan agar segala data yang dikirimkan tidak dapat dilihat, diubah, maupun dihapus oleh orang ketiga yang tidak mempunyai hak untuk melakukannya. Teknik dalam mengamankan data dapat

dilakukan dengan berbagai macam hal, salah satunya adalah dengan menggunakan teknik kriptografi.

Permana (2018) telah melaporkan metode kriptografi yang diaplikasikan untuk pengamanan teks dengan algoritma *vigenere chiper* menggunakan perangkat android. Permana dan Nurnaningsih (2018) juga melaporkan metode kriptografi yang digunakan untuk merancang aplikasi pengamanan teks menggunakan algoritma *Advanced Encryption Standard* (AES). Kedua jurnal tersebut melaporkan pengamanan data dalam bentuk teks, sehingga pengamanan data dalam bentuk gambar perlu dianalisis lebih lanjut. Pada penelitian ini data yang diamankan berupa gambar, dengan teknik kriptografi menggunakan algoritma *Data Encryption Standard* (DES). Algoritma DES adalah salah satu metode

penyandian dengan sistem block cipher. Yaitu sistem penyandian yang pengacakannya dilakukan secara blok demi blok dengan blok input (teks asli) 64 bit dan menghasilkan output (teks sandi) yang juga per blok 64 bit, algoritma yang digunakan adalah kunci simetris dengan panjang kunci 56 bit.

KAJIAN LITERATUR

Kriptografi

Kriptografi adalah ilmu dan teknik dalam pengamanan data dari pihak ketiga. Pada kriptografi terdapat istilah enkripsi dan dekripsi. Enkripsi adalah mengubah text awal (plain text) menjadi text ter-enkripsi (cipher text) menggunakan sebuah kunci. Sedangkan Dekripsi adalah mengubah text ter-enkripsi (cipher text) kembali menjadi text awal (plain text) dengan menggunakan kunci yang sama, dalam hal ini jika menggunakan *symmetric-key cryptography*. Permana (2017)

Tipe Kriptografi

Terdapat tiga macam kriptografi:

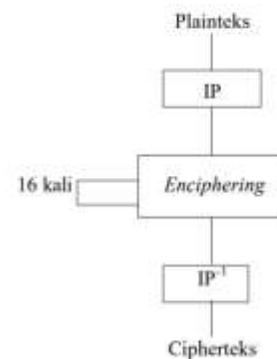
- Kriptografi Kunci Simetris (*Symmetric Key Cryptography*):
Kriptografi ini menggunakan kunci yang sama untuk enkripsi dan dekripsi pesan. di mana pengirim dan penerima pesan menggunakan kunci yang sama untuk enkripsi dan dekripsi pesan. Ada beberapa macam algoritma yang termasuk ke dalam *symmetric-key cryptography*, salah satu algoritma yang paling terkenal dari Kriptografi kunci simetris ini adalah DES (Data Encryption Standard).
- Kriptografi Kunci Asimetris (*Asymmetric Key Cryptography*):
Kriptografi ini menggunakan sepasang kunci yang berbeda untuk enkripsi dan dekripsinya. Sebuah kunci publik (*public key*) digunakan untuk enkripsi dan kunci rahasia (*private key*) digunakan untuk dekripsi. *Public key* dan *Private Key* adalah hal yang berbeda. Walaupun jika kunci publik diketahui oleh semua orang, hanya penerima lah yang dapat men-*decrypt* informasi tersebut karena hanya dia yang tahu kunci rahasia (*private key*) nya.

- Kriptografi Hybrid
Kriptografi ini memadukan *symmetric* dan *asymmetric* cipher
Dalam penggunaannya. Pengirim mengenkripsi pesan dengan session key, lalu session key tersebut di-encrypt kembali dengan menggunakan public key. Lalu, penerima men-decrypt session key tersebut dengan priate key yang dimilikinya.

METODE

Data Encryption Standard (DES)

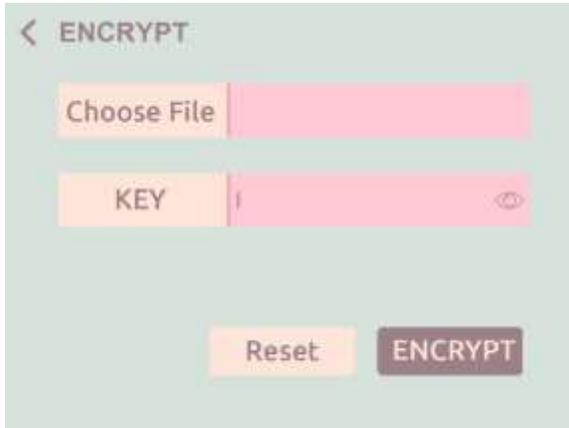
Data Encryption Standard (DES) termasuk ke dalam algoritma kunci-simetris, dimana kunci yang sama digunakan untuk enkripsi dan dekripsi. DES termasuk ke dalam blok cipher, dimana data tergabung dalam blok berukuran masing-masing 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau sub-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit. Skema global dari algoritma DES adalah sebagai berikut:



Gambar 1. Skema Global Algoritma DES (Munir, 2004)

Skema Global Dari Algoritma DES adalah sebagai berikut:

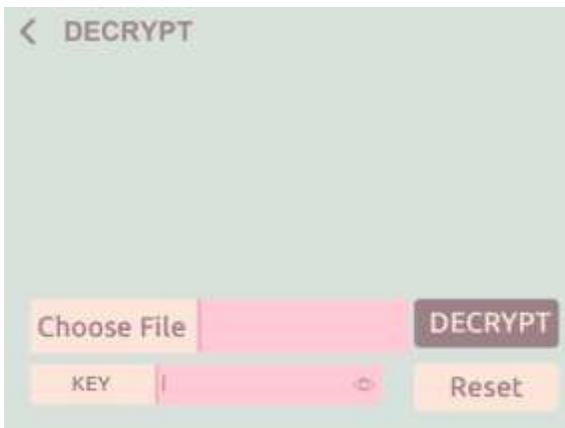
- Blok *plaintext* dipermutasi dengan matriks permutasi awal (*Initial Permutation* atau IP).
- Hasil permutasi awal kemudian di-*enchipering* sebanyak 16 kali putaran. Setiap putaran menggunakan kunci internal yang berbeda.



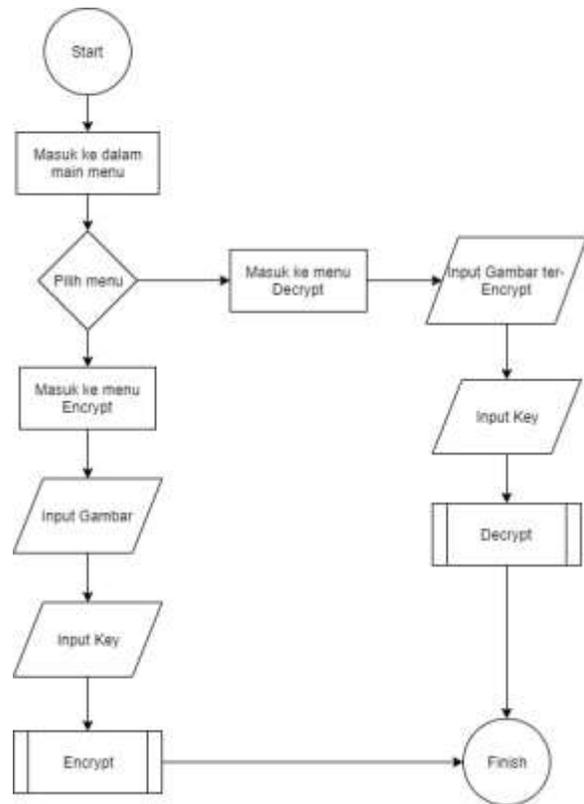
Gambar 6. Menu Encrypt



Gambar 7. Choose File / File Destination



Gambar 8. Menu Decrypt

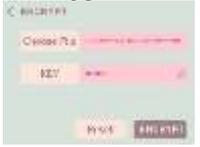
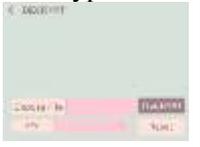
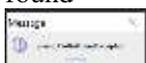


Gambar 9. Alur Aplikasi

PENGUJIAN

Tabel 1. BlackBox Testing Aplikasi

No	Pengujian Skenario	Hasil yang diharapkan	Kesimpulan
1	Mengosongkan field pilihan gambar dan key, lalu klik tombol "Encrypt"	Sistem akan menolak proses Encrypt dan mengeluarkan pop up dialogue file not found	Valid
2	Mengosongkan key setelah	Sistem menolak	Valid

	<p>memilih gambar yang akan di-encrypt, lalu klik button "Encrypt"</p> 	<p>proses encrypt dan muncul pop up dialogue EmptyKey</p> 	
3	<p>Field gambar terisi dan panjang key tidak sama dengan 8 byte, lalu klik button "Encrypt"</p> 	<p>Sistem menolak proses encrypt dan muncul pop up dialogue Wrong Key Size</p> 	Valid
4	<p>Field gambar terisi dan panjang key sama dengan 8, lalu klik button "Encrypt"</p> 	<p>Sistem berhasil mengenkripsi gambar dan muncul pop up dialogue The file encrypted successfully</p> 	Valid
5	<p>Mengosongkan field pilihan gambar dan key, lalu klik tombol "Decrypt"</p> 	<p>Sistem menolak proses Decrypt dan muncul pop up dialogue File not found</p> 	Valid
6	<p>Field gambar terisi, namun key salah</p>	<p>Sistem menolak proses</p>	Valid

		<p>Decrypt dan tidak akan memunculkan gambar hasil Decrypt</p> 	
7	<p>Field gambar terisi dan key benar</p> 	<p>Sistem berhasil Decrypt gambar dan memunculkan pop up dialogue The Image Was Encrypted Successfully</p>  <p>Dan memunculkan gambar yang awal</p> 	Valid

KESIMPULAN

Berdasarkan aplikasi yang telah dirancang menggunakan Algoritma DES dengan input berupa gambar, dapat berhasil mengenkripsi gambar tersebut. Panjang kunci untuk Algoritma DES harus sepanjang 8 byte atau 8 karakter, karena DES adalah algoritma kriptografi blok-chiper 64 bit. Sedangkan kunci yang digunakan untuk *decrypt* adalah kunci yang sama dengan kunci saat *encrypt*.

Kelemahan dari algoritma DES sendiri adalah, ketika gambar yang terencrypt dan dibuka maka akan bertuliskan Image not supported, yang akan menimbulkan kecurigaan pada pihak ketiga. Selain itu karena kunci yang digunakan sama, kunci dapat mengalami kebocoran.

DAFTAR PUSTAKA

- Data Encryption Standard (DES), diakses pada 5 Januari 2020 Website : [http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Data%20Encryption%20Standard%20\(DES\).pdf](http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Data%20Encryption%20Standard%20(DES).pdf)
- Firmansyah, R dan Permana, A, A., 2019, Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma RSA dengan Metode Waterfall berbasis JAVA, *Joutica* Vol 4 No 1, ISSN : 2621-511X.
- Munir, R. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.
- Permana, A, A., 2017, Aplikasi Penyisipan Teks Pada Gambar dengan Algoritma Blowfish dan Least Significant Bit, *JIKA (Jurnal Informatika)* Vol 1 No 1, ISSN : 2549-0710.
- Permana, A, A. 2018. Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. *Jurnal Al-Azhar Indonesia Seri Sains dan Teknologi*, Vol 4 No 3, ISSN : 2355-8059.
- Permana, A, A. Nurnaningsih, D. 2018. Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encryption Standard (AES). *Jurnal Teknik Informatika* Vol 11 No. 2, ISSN : 2549-7901.
- Primartha, R., 2011, Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES), *Jurnal Sistem Informasi Unsri*, ISSN : 2355-4614.