JIKSTRA *Vol. 01, No. 02, September 2019*
p-ISSN:2715-887X
e-ISSN:2747-2485 12-17

Sistem Pengamanan Data Customer dengan Metode Data Encryption Standart (DES)

Azanuddin

Program Studi Sistem Komputer, STMIK Triguna Dharma
e-mail : azdin.bpc@gmail.com

ABSTRAK

Pengamanan data menjadi salah prioritas penelitian pada era digital. Keamanan, kerahaisaan dan integritas data sangat dibutuhkan oleh setiap pengguna sebuah sistem informasi berbasis teknologi. Kerahasiaan data customer pada sebuah perusahaan memang sangat fundamental dalam mengelola data customr akan tetapi tidak didukung dengan sebuah sistem yang memadai dalam menjaga kerahasian data customer. Sehingga banyak data customer yang disalah gunakan oleh orang yang tidak berkepentingan yang mengakibatkan ketidaknyamanan para customer apabila data diri customer dapat diketahui banyak orang, apalagi jika informasi tersebut mencakup data keuangan dan kartu kredit. Oleh karena hal tersebut perlu adanya pengamanan khusus yang digunakan untuk mengamankan data customer dengan menggunakan metode DES sehingga kerahasiaan data customer dengan tujuan data customer terjaga selain itu juga dapat meningkatkan kepercayaan customer

Kata kunci: Kriptografi, Keamanan Data Customer, DES

ABSTRACT

Data security is a priority of research in the digital age. Security, confidentiality and data integrity are needed by every user of a technology-based information system. The confidentiality of customer data in a company is indeed very fundamental in managing custom data, but it is not supported by an adequate system in maintaining customer data confidentiality. So that a lot of customer data is misused by unauthorized people which results in the inconvenience of customers if the customer's personal data can be known to many people, especially if the information includes financial and credit card data. Because of that, there needs to be special security that is used to secure customer data using the DES method so that the confidentiality of customer data with the aim of maintaining customer data can also increase customer confidence.

Keywords: Cryptography, Customer Data Security, DES

1. PENDAHULUAN

Sistem informasi yang aman menjadi kepercayaan untuk seseorang dalam menggunakan sebuah sistem informasi berbasis teknologi, keamanan dan kerahasiaan informasi hal yang terpenting dalam pengelolaan sebuah informasi. Didalam sebuah perusahaan atau organisasi, data customer merupakan informasi yang harus dijaga dengan maksimal. Jika data tersebut dapat diakses secara online dengan suatu jaringan komputer, tentu data yang sangat penting dapat dengan mudah diakses oleh orang yang tidak berwenang sehingga dapat dilihat dan dimanfaatkan untuk kepentingan lainnya.

Kemungkinan informasi dapat didapatkan oleh orang yang tidak berkepentingan dengan cara apapun dipastikan sangat merugikan pengguna siste, apalagi jika informasi tersebut merupakan informasi yang harus rahasia terkait data diri pribadi yang

mencakup data kartu kredit dan lainnya, yang jika dapat diketahui oleh orang yang tidak bertanggung jawab maka dapat membahayakan bagi orang yang memiliki informasi tersebut.

Sebuah informasi yang dikirim melalui media apapun haruslah dapat dijaga kerahasiaan, Untuk mengamankan informasi atau *message* didalam komuter diperlukan cara keamanan penyandian yang biasa disebut dengan kriptografi. Penggunaan teknik kriptografi ini perlu dilakukan untuk menjaga keamanan informasi customer agar orang yang tidak berkepentingan yang melihat dan memiliki data terebut tidak dapat memahami isi dari informasi tersebut dengan penggunaan enkripsi. Salah satu metode enkripsi data yang akan dibahas dalam penelitian ini adalah Metode Data Encryption Standart (DES).

Enkripsi merupakan salah satu cara yang dilakukan untuk mengamankan sistem atau informasi dari hal yang akan menyebabkan aspek-aspek diatas tidak terpenuhi, seperti untuk menjaga integritas data atau informasi. Ketika pengguna yang berhak dapat mengakses informasi maka dapat dilakukan deskripsi agar informasi dapat dipahami kembali. Keamanan dengan penggunaan metode DES ini dipilih karena mengadopsi teknik keamanan penyandian kunci simetri.

2. METODE PENELITIAN

Data Encryption Standard (DES) adalah algoritma cipher blok yang populer digunakan karena tingginya tingkat keamanan informasi karena dijadikan standard algoritma enkripsi kunci-simetri. DES adalah nama standard enkripsi simetri, yang dahaulu memiliki nama algoritma enkripsinya DEA (Data Encryption Algorithm), namun nama DES lebih populer daripada DEA.

Proses kinerja pada penggunaan DES dengan melakukan blok plainteks yang berikutnya dilakukan permutasi dengan matriks permutasi awal . Hasil dari permutasi awal tersebut kemudian di enkripsikan sebanyak 16 kali putaran. Setiap putarannya akan menggunakan kunci internal yang berbeda. Hasil dari proses enchiper kembali dipermutasi dengan matriks permutasi balikan (invers initial permutation) menjadi blok cipherteks. Secara matematis, satu putaran DES dinyatakan sebagai berikut :

$$Li = Ri - 1$$
$$Ri = Li - 1 + f(Ri - 1, Ki)$$

Contoh penerapan metode DES Misalkan suatu plaintext M = 0123456789ABCDEF, M dalam format heksadesimal (basis 16).

3. HASIL DAN PEMBAHASAN

Algoritma DES merupakan metode enkripsi yang menggunakan metode simetrik dan pengolahan dalam bentuk blok chiper, jadi kata kunci yang sama digunakan untuk proses enkripsi dan deskripsi. Parameter yang digunakan dalam Algoritma DES memiliki beberapa tahapan dalam menggunakan algoritma DES (Data Encryption System).

Ubahlah Planintext kedalam bentuk biner berdasarkan tabel ASCII

I : 01001001; C : 01000011; A : 01000001; R : 01010010; A : 01000001 ;M : 01001101; O : 01001111l N : 01001110 Atau bilangan hexanya : 49 43 41 52 41 4D 4F 4E

Lakukan Initial Permutation (IP) pada bit Planintext menggunakan tabel IP berikut:

Tabel 1 Initial Permutation(IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Tabel 2 Plainteks

$0^{(1)}$	$1^{(2)}$	$0^{(3)}$	$0^{(4)}$	$1^{(5)}$	$0^{(6)}$	$0^{(7)}$	$1^{(8)}$
$0^{(9)}$	$1^{(10)}$	$0^{(11)}$	$0^{(12)}$	$0^{(13)}$	$0^{(14)}$	$1^{(15)}$	$1^{(16)}$
$0^{(17)}$	$1^{(18)}$	$0^{(19)}$	$0^{(20)}$	$0^{(21)}$	$0^{(22)}$	$0^{(23)}$	$1^{(24)}$
$0^{(25)}$	$1^{(26)}$	$0^{(27)}$	$1^{(28)}$	$0^{(29)}$	$0^{(30)}$	$1^{(31)}$	$0^{(32)}$
$0^{(33)}$	$1^{(34)}$	$0^{(35)}$	$0^{(36)}$	$0^{(37)}$	$0^{(38)}$	$0^{(39)}$	$1^{(40)}$
$0^{(41)}$	$1^{(42)}$	$0^{(43)}$	$0^{(44)}$	$1^{(45)}$	$1^{(46)}$	$0^{(47)}$	$1^{(48)}$
$0^{(49)}$	$1^{(50)}$	$0^{(51)}$	$0^{(52)}$	$1^{(53)}$	$1^{(54)}$	$1^{(55)}$	$1^{(56)}$
$0^{(57)}$	$1^{(58)}$	$0^{(59)}$	$0^{(60)}$	$1^{(61)}$	$1^{(62)}$	$1^{(63)}$	$0^{(64)}$

Tabel 3 Ekspansi (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Hasil $E(R_{i-1})$ kemudian di XOR dengan K_i dan menghasilkan Vektor Matriks A_i. Berikut hasil outputnya:

00011010 00000100 00001000 00001100

Iterasi 1

E(R(1)-1) = 011010 000100 001000 001100 100001 010100 011000011100

K1 = 000101 001001 001101 000010 111101 100001 011000 001100
---------- XOR
A1 = 101111 001101 001101 001110 011101 110101 011000 011100

Tabel 4 Box 1 S1

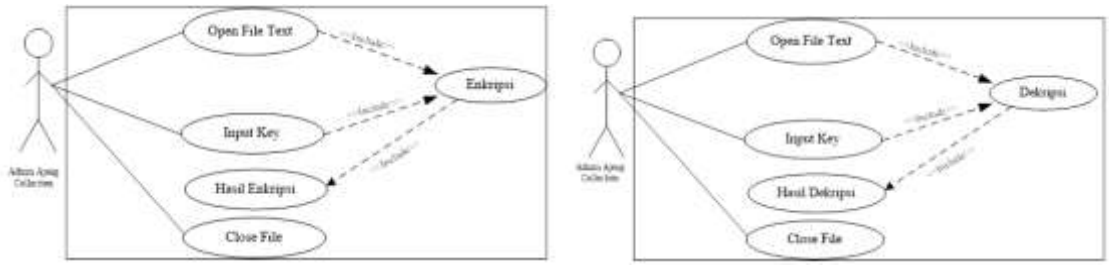
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

Tabel 5 IP-1

Langkah terakhir dalam proses enskripsi adalah menggabungkan R16 dengan L16 yang kemudian akan dipermutasikan untuk terakhir Invers Initial Permutasi (IP-1).

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26

33	1	41	9	49	17	57	25



Gambar 1 Use Case Enkripsi dan Deskripsi

Gambar 2 Proses Enkripsi

Gambar 3 Proses Deskripsi

4. KESIMPULAN

Dari hasil penelitia ini dapat disimpulkan data customer maka diperoleh hasil kesimpulan sebagai berikut:

1. Dengan melakukan pengujian terhadap algoritma Data Encryption Standart (DES) untuk melihat sejauh mana sistem keamanan dari data yang diterapkan.
2. Sistem ini dirancang dengan menggunakan perancangan sistem, perancangan database dan perancangan interface.
3. Dengan mengimplementasikan sistem yang telah dirancang sistem ini mampu memberikan keamanan data customer di dalam komputer.

UCAPAN TERIMA KASIH

Penulis mengucapakn terima kasih kepada rekan peneliti pada bidang keamanan informasi dilingkungan penulis.

DAFTAR PUSTAKA

Islam, E., & Azad, S. (2014). Data encryption standard. In Practical Cryptography: Algorithms and Implementations Using C++. https://doi.org/10.1201/b17707

Rob, D. E. (1982). Cryptography and Data Security. Security.

ENISA. (2015). Privacy and Data Protection by Design - from policy to engineering. Cryptography and Security. https://doi.org/10.2824/38623

Kumar, P., & Rana, S. B. (2016). Development of modified AES algorithm for data security. Optik. https://doi.org/10.1016/j.ijleo.2015.11.188

Anggraini, Y., & Sakti, D. V. S. Y. (2014). Penerapan Steganografi Metode End of File (Eof) Dan Enkripsi Metode Data Encryption Standard (Des) Pada Aplikasi Pengamanan Data Gambar Berbasis Java. Konferensi Nasional Sistem Informasi 2014, STMIK Dipanegara Makassar.

Primartha, R. (2011). Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Data Encryption Standard (DES). Jurnal Sistem Informasi (JSI).

Sulaiman, O. K., Ihwani, M., & Rizki, S. F. (2016). Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encryption Standard (Des) Algorithm. InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan). https://doi.org/10.30743/infotekjar.v1i1.82