**Sains dan Komputer (SAINTIKOM)**
Vol.17B, No.1, Februari 2018, pp. 121-124
ISSN: 1978-6603


# Sistem Pengamanan Data Customer di Toko Ajeng Collection dengan Metode Data Encryption Standart (DES)

**Badrul Anwar[#1], Hendryan Winata[#2]**
[#1,] Program Studi Sistem Komputer, STMIK Triguna Dharma
[#2] Program Studi Manajemen Informatika, STMIK Triguna Dharma

**Article Info**

***Article history:***
Received Jan 13th, 2018
Revised Feb 03th, 2018
Accepted Feb 07th, 2018

***Keyword:***

Keamanan Data Customer
Kriptografi
Data Encryption Standart

**ABSTRACT**

Pengamanan data menjadi salah satu tantangan terbesar dari dunia digital saat ini. Keamanan, kerahaisaan dan integritas data diperlukan dalam setiap operasi yang ada. Kerahasiaan data customer pada Toko Ajeng Collection memang sangat diprioritaskan akan tetapi tidak didukung dengan sistem yang memadai. Sehingga banyak data customer Toko Ajeng Collection yang disalah gunakan oleh orang yang tidak bertanggungjawab yang mengakibatkan ketidaknyamanan para customer.

Oleh karena itu Toko Ajeng Collection memerlukan program khusus yang digunakan untuk mengamankan data customer dengan menggunakan metode DES sehingga kerahasiaan data customer Toko Ajeng Collecction akan tetap terjaga selain itu juga dapat meningkatkan kepercayaan customer pada Toko Ajeng Collection.

Hasil dari penelitian ini diharapkan dapat membantu Toko Ajeng Collection dalam mengamankan data para customernya agar data-data yang ada tidak dapat diketahui oleh orang kecuali admin Toko Ajeng Collection. Tujuannya adalah agar data-data customer tidak disalahgunakan oleh orang yang tidak bertanggungjawab.



First Author
Nama : Badrul Anwar, SE., S.Kom., M.Kom.
Kantor : STMIK Triguna Dharma
Program Studi : Sistem Komputer
E-Mail :

## 1. PENDAHULUAN

Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apalagi jika data tersebut berada dalam suatu jaringan komputer yang terhubung / terkoneksi dengan jaringan lain yang publik misalnya internet. Tentu saja data yang sangat penting tersebut jangan sampai jatuh ke tangan yang tidak berwenang sehingga bisa dilihat atau dibajak oleh orang yang tidak bertanggung jawab.

Sebab kalau hal ini sampai terjadi kemungkinan informasi yang terkandung di dalamnya bisa diketahui oleh orang lain yang tidak berhak sehingga mungkin saja membahayakan bagi orang yang mengirim pesan atau dikirimi pesan bahkan banyak orang. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan sehingga bisa membahayakan kedua pihak atau bahkan banyak orang. Selain itu data yang dibajak tersebut akan memiliki kemungkinan rusak bahkan bisa hilang yang akan menimbulkan kerugian bagi pengirim pesan.

Toko Ajeng Collection adalah toko yang menjual berbagai barang branded seperti tas, sepatu, jam dan lainnya. Toko yang berada di kota medan ini lebih mengarahkan ke sistem pesanan barang secara online. Rata-rata 500 lebih pesanan barang customer perhari siap dikirim ke berbagai daerah. Toko ajeng collection memiliki 25 admin online yang melayani customer setiap harinya dimana setiap admin memiliki customer masing-masing dan untuk mengamankan data customer atau pelanggan mereka, maka setiap admin memiliki Id password sendiri sehingga data konsumen dapat diamankan dan yang dapat melihat data tersebut hanya admin tertentu. Sehingga data konsumen tidak dapat di acak-acak atau diketahui oleh orang lain karena disebabkan persaingan bisnis.

Untuk mengamankan data atau message didalam komuter diperlukan kriptografi dengan metode 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. Ada beberapa algoritma enkripsi yang sudah terbuka untuk dipelajari, seperti Data Encryption Standard (DES), RC-4, TwoFish, RC-5 dan lain-lain.

## 2. METODE PENELITIAN

### 2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani. Menurut dari bahasa tersebut kata kriptografi dibagi dua yaitu cripto dan graphia. Cripto berarti secret (rahasia) dangraphia berarti writing (tulisan). Menurut teminologinya kriptografi adalah ilmu dan seni menjaga keamana pesan ketika pesan dikirim dari suatu tempat ketempat yang lain. Dalam perkembangannya kriptografi juga digunakan untuk mengindentifikasi pengiriman pesan dengan tanda tagan digital dan keaslian pesan dengan sidik jari digital (fingerprint).(Dony, 2012:77)

Cryptographic system atau Cryptosystem adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapakunci kriptografi. Secara umum, kunci-kunci yang digunakan untuk proses pengenkripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan. Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut :

EK (M) = C (Proses Enkripsi)
DK (C) = M (Proses Dekripsi)

Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya. Dengan demikian keamanan suatu pesan tergantung pada kunci ataupun kunci-kunci yang digunakan, dan tidak tergantung pada algoritma yang digunakan. Sehingga algoritma-algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis, serta produk-produk yang menggunakan algoritma tersebut dapat diproduksi massal. Tidaklah menjadi masalah apabila seseorang mengetahui algoritma yang kita gunakan. Selama ia tidak mengetahui kunci yang dipakai, ia tetap tidak dapat membaca pesan.

### 2.2 Algoritma DES

Menurut Salim (2014:36) DES (Data Encryption Standard) adalah algoritma cipher blok yang populer karena dijadikan standard algoritma enkripsi kunci-simetri, meskipun saat ini standard tersebut telah digantikan dengan algoritma yang baru, AES, karena DES sudah dianggap tidak aman lagi. Sebenarnya DES adalah nama standard enkripsi simetri, nama algoritma enkripsinya sendiri adalah DEA (Data Encryption Algorithm), namun nama DES lebih populer daripada DEA.

Dalam proses enchiper, blok plainteks terbagi menjadi dua bagian yaitu bagian kiri (L) dan bagian kanan (R), yang masing masing memiliki panjang 32 bit. Pada setiap putaran i, blokR merupakan masukan untuk fungsi transformasi fungsi f. Pada fungsi f, blok R dikombinasikan dengan kunci internal Ki. Keluaran dari fungsi ini di XOR kan dengan blok L yang langsung diambil dari blok R sebelumnya. Ini merupakan 1 putaran DES.

## 3. ANALISIS DAN HASIL

Tabel 3.1 *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 3.2 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 3.3 Hasil IP (x)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |

Tabel 3.5 PC -1

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

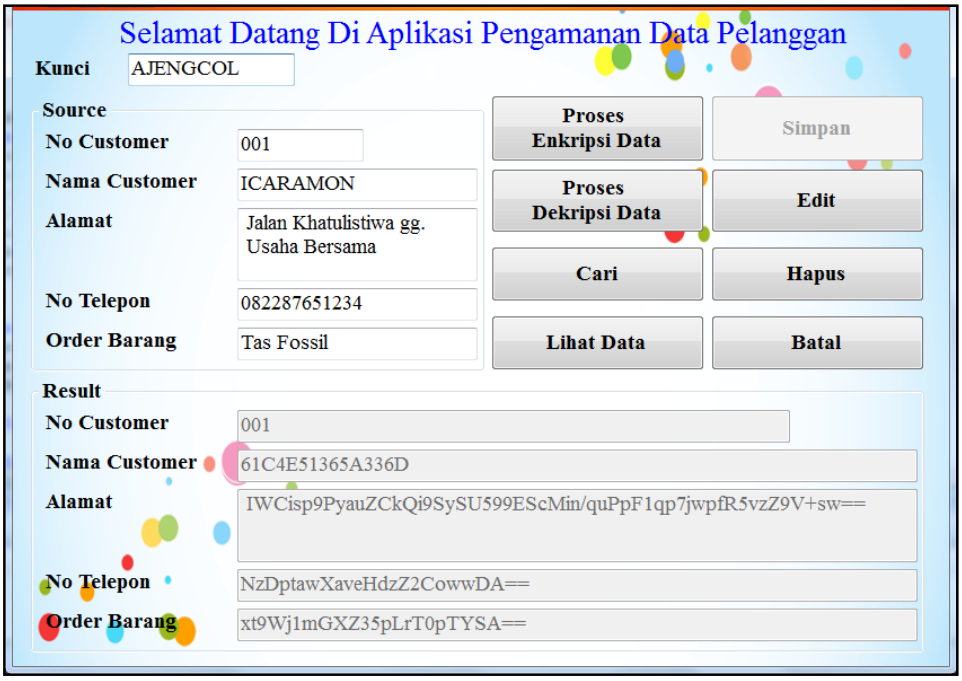
Iterasi 1
E(R(1)-1) = 011010 000100 001000 001100 100001 010100 011000011100
K1 = 000101 001001 001101 000010 111101 100001 011000 001100
---------- XOR
A1 = 101111 001101 001101 001110 011101 110101 011000 011100

$R_{15} = L_{16} \oplus F(R_{16}, K_{16})$

$$R_{15} = \frac{1011\ 0110\ 0101\ 1111\ 0111\ 1000\ 1001\ 1111}{0010\ 0101\ 0100\ 1101\ 1110\ 0101\ 0110\ 0001}$$

$R_{15} = 1001\ 0011\ 0001\ 0010\ 0001\ 1101\ 1111\ 1110$

Cipher(dalam hexa) = ICARAMON




## 4. KESIMPULAN

1. Untuk membantu perawat memberikan informasi kepada pasien berkenaan dengan diagnose penyakit kerongkongan.
2. Penerapan metode *Dempster Shafer* dalam sistem yang dibangun agar mampu memberikan hasil diagnosa pasien.
3. Apikasi sistem pakar yang dibangun dapat memberikan manfaat kepada pasien.
4. Implementasi Aplikasi berbasis desktop *programming* diterapakan untuk mempermudah pasien dan perawat untuk berhubungan langsung dengan sistem yang dibuat.