ISSN : 2548-6985

Implementasi Algoritma Rot Dan Subtitusional Block Cipher Dalam Mengamankan Data

Ayu Pratiwi
STMIK Budi Darma Medan, Sumatera Utara, Indonesia
Jl. Sisingamangaraja No. 338 Simpang Limun Medan
http://stmik-budidarma.ac.id // Email : ayupratiwi455@gmail.com

ABSTRACT
The security and confidentiality of data is one of the most important aspects in the information system at this time. Caused by the rapid development of science and technology that allows the emergence of new techniques, which are misused by certain parties that threaten the security of information systems. In general, the data are categorized into two, namely confidential data and data that is not confidential. Data that is not confidential is usually not too much attention. What really needs to be considered is confidential data, where every information contained in it will be very valuable for those who need it because the data can be easily duplicated.
The ROT-n algorithm is one simple encryption algorithm that uses alphabetical shifts as much as n to convert plain text into cipher text, whereas Block ciphers work by processing data in blocks, where several characters / data are combined into one block. Each one block process produces one block output as well.

Keywords: Implementation, ROT-Algorithm and Block Cipher Substitutional.

PENDAHULUAN

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Disebabkan pesatnya perkembangan ilmu pengetahuan dan teknologi yang memungkinkan munculnya teknik-teknik baru, yang disalah gunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia.

Enkripsi merupakan suatu proses pengubahan pesan asli menjadi karakter yang tidak dapat dibaca. Ada beberapa algoritma enkripsi yang biasa digunakan seperti *Block Cipher*, *Stream Cipher*, *Data Encryption Standard* (DES), *Triple* DES, *Advanced Encryption Standard* (AES), dan sebagainya. Dimana setiap algoritma memiliki karakteristik tersendiri. Sedangkan proses pengubahan kembali hasil enkripsi menjadi pesan asli dinamakan dekripsi. Untuk merahasiakan data yang sangat penting maka digunakanlah metode kriptografi yang akan mengenkripsi dan deskripsikan data [2].

Dari beberapa metode yang ada dalam mengamankan data digunakanlah Algoritma ROT dan Subtitusional *Block Chiper*. Algoritma ROT-**n** merupakan salah satu algoritma enskripsi sederhana yang menggunakan pergeseran abjad-abjad sebanyak **n** untuk mengubah plain text menjadi cipher text. Sedangkan Block cipher bekerja dengan memproses data secara blok, dimana beberapa karakter / data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga. metode ini diimplementasikan pada level *binary digit* (*bit*), sehingga pola proses enkripsi tidak dapat terbaca, serta proses enkripsi dan dekripsi memerlukan waktu yang singkat

Berdasarkan latar belakang pemilihan judul, maka yang menjadi permasalahan dalam penelitian ini, yaitu :

1. Bagaimana penerapan algoritma ROTn dan diteruskan dengan teknik blok pada proses penyandian data ?
2. Bagaimana merancang aplikasi pengamanan data dengan Algoritma ROT dan Subtitusional Block Cipher dalam mengamankan data ?

Manfaat dari penulisan penelitian ini adalah :

1. Mengetahui proses penyandian data dengan teknik subtitusi menggunakan Algoritma ROTn dan diteruskan dengan teknik blok .
2. Dapat digunakan untuk mengaman data.
3. Sebagai bahan perbandingan bagi penulis lain mengenai metode kriptografi yang telah ada pada saat ini.
4. Dapat memperkaya literature mengenai kriptografi khususnya algoritma ROT dan Cipher Block, sehingga nantinya dapat bermanfaat untuk menjaga keamanan data dan dapat diimplementasikan.

LANDASAN TEORI

ISSN : 2548-6985

2.1 Implementasi

Implementasi adalah tahapan penerapan atau tindakan yang diperlukan agar mencapai sukses dalam suatu penelitian. Oleh karenanya, tahapan ini bukan lagi sebagai wacana pemikiran atau ide lagi, tetapi sudah berada pada tahapan perilaku dan tindakan yang diperlukan dalam penelitian[5].

Menurut Van Horn dan Van Meter dalam buku terjemahan Wahab, Implementasi dapat diartikan sebagai tindakan-tindakan oleh individu publik dan swasta atau kelompok yang diarahkan pada prestasi tujuan yang ditetapkan dalam keputusan kebijakan sebelumnya. Jadi Implementasi dimaksudkan sebagai tindakan individu publik yang diarahkan pada tujuan serta ditetapkan dalam keputusan dan memastikan terlaksananya dan tercapainya suatu kebijakan serat memberikan hasil yang bersifat praktis terhadap sesama[8].

2.2 Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani, terdiri dari dua suku kata yaitu "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan), Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan, keadsahan data, integritas data, serta autentikasi data. Secara umum kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita (bruce Schneier – *Applied Criptography*).

Selain definisi tersebut diatas, terdapat pula definisi yang dikemukakan didalam Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan, integritas data, serta otentikasi. [7].

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu[7]:

1. Kerahasiaan, adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak
2. Integritas data, adalah layanan yang menjamin pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman
3. Otentikasi, adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikassi kebenaran pihak-pihak yang berkomunikassi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*origin authentication*)

   Nirpenyangkalan (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.3 Algoritma

Algoritma adalah urutan langkah-langkah untuk memecahkan suatu masalah. Terdapat macam-macam definisi algoritma, berikut ini merupakan beberapa definisi lain dari algoritma, antara lain:

1. Algoritma adalah deretan langkah-langkah komputasi yang *mentransformasikan* data masukan menjadi data keluaran.
2. Algoritma adalah deretan intruksi yang jelas untuk memecahkan masalah, yaitu untuk memperileh keluaran yang diinginkan dari suatu masukan dalam jumlah waktu yang terbatas.
3. Prosedur komputasi yang terdefinisi dengan baik yang menggunakan beberapa nilai sebagai masukan dan menghasilkan beberapa nilai yang disebut keluaran. Jadi Algoritma adalah deretan langkah komputasi yang masukan menjadi keluaran (Rinaldi Munir, 2007: 4).

2.4 Algoritma ROT

ROT-**n** (rotate by **n**) merupakan salah satu algoritma enskripsi sederhana yang menggunakan pergeseran abjad-abjad sebanyak **n** untuk mengubah plain text menjadi cipher text**.** Artinya jika pada ROT-13**,** abjad A diganti dengan N sedangkan abjad B diganti dengan O demikian seterusnya.Secara sederhana berikut penggunaan algoritma ROT-13**:**

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm

Dari uraian diatas jelas terlihat bahwa pada ROT-13 setiap abjad A akan diganti dengan abjad N, setiap abjad a akan diganti dengan abjad n. Demikian seterusnya.

Contoh:

KOMPUTER (plaintext)
XBZCHGRE (ciphertext, hasil enskripsi ROT-13)
BfDGLKvI (cipher text, hasil enskripsi ROT-17)

Algoritma ini pertama kali dikemukakan oleh Julius Caesar untuk melakukan

komunikasi dengan para panglimanya. (http://elib.unikom.ac.id diakses tanggal,06-April-2015,Jam-21.54-WIB).

2.5 Algoritma *Block Cipher*

Block Cipher adalah algoritma enkripsi yang akan membagi-bagi *plaintext* yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama. Pada umumnya, *block cipher* memproses *plaintext* dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit penggunaan pola-pola serangan yang ada untuk membongkar kunci.

Pada cipher blok, rangkaian bit-bit plainteks dibagi menjadi blok- blok bit dengan panjang sama, biasanya 64 bit (tapi adakalanya lebih). Algoritma enkripsi menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks. Dengan blok cipher, blok plainteks yang sama akan dienkripsi menjadi blok cipherteks yang sama bila digunakan kunci yang sama pula. Ini berbeda dengan cipher aliran dimana bit-bit plainteks yang sama akan dienkripsi menjadi bit-bit cipherteks yang berbeda setiap kali dienkripsi.

Misalkan blok plainteks (P) yang berukuran *m* bit dinyatakan sebagai vector:

$P = (P_1,P_2,P_3,\ldots,P_m)$

Yang dalam hal ini P_i adalah 0 atau 1 untuk i = 1,2,…,n, dan blok chiperteks (C) adalah:

$C = (c_1,c_2,\ldots c_n)$

Yang dalam hal ini c_1 adalah 0 atau 1 untuk i = 1,2,…,n. Bila plainteks dibagi menjadi m buah blok, barisan blok – blok plainteks dinyatakan sebagai:

$(P_1,P_2,\ldots,P_m)$

Untuk setiap blok plainteks P_i bit- bit penyusunannya dapat dinyatakan sebagai vektor:

$P_i = (P_{i1},P_{i2},\ldots,P_{in})$

Enskripsi dan dekripsi dengan kunci K dinyatakan berturut-turut dengan persamaan:

$E_k(P) = C$ (enkripsi)....(1)

Dan

$D_k(C) = P$ (dekripsi)..(2)

Fungsi E haruslah fungsi yang bekoresponden satu ke satu, sehingga:

$E^{-1} = D$.....(3)

Algoritma blok chipper menggabungkan beberapa teknik kriptografi klasik dalam proses enkripsi.Dengan kata lain, *chipper* blok dapa diacu sebagai super enkripsi. Teknik kriptografi klasik yang digunakan adalah :

1. Subtitusi
   Teknik ini menggani satu atau sekumpulan bit pada blok plainteks tanpa mengubah urutannya. Secara matemais, teknik subtitusi ini ditulis sebagai $C_i = E(p_i)$, i= 1,2,…. (urutan bit), Yang dalam hal ini c_i adalah bit cipherteks, p_i adalah bit plainteks, dan f adalah fungsi subtitusi. Dalam praktek, EE dinyatakan sebagai fungsi matematis atau dapat merupakan tabel substitusi (S-box).
2. Transposisi atau permutasi
   Teknik ini memindahkan posisi bit pada blok plainteks berdasarkan aturan tertentu. Secara matematis, teknik transposisi ini ditulis sebagai C = PM, Yang dalam hal ini C adalah blok chiperteks, P adalah blok plainteks, dan M adalah fungsi transposisi. Dalam praktek, M dinyatakan sebagai tabel matriks atau matriks permutasi.
3. Ekspansi
   Teknik ini memperbanyak jumlah bit pada blok plainteks berdasarkan aturan tertentu. Misalnya dari 32 bit menjadi 48 bit. Dalam praktek, aturan ekspansi dinyatakan dengan tabel.
4. Kompresi
   Teknik ini kebalikan dar ekspansi, di mana jumlah bit pada blok plainteks diciutkan berdasarkan aturan tertentu. Dalam prakteknya, aturan kompresi dinyatakan dengan tabel.

Contoh *block chipper*: DES, 3DES, GOST, RC5, AES, Blowfish, IDEA, LOKI, RC2, FEAL, Lucifer, CAST, CRAB, SAFER, Twofish, Serpent, RC6, MARS, Camellia, 3-WAY, MMB, SkipJack, dll. (Rinaldi Munir, 2006: 118).

2.6 Data

Data adalah catatan atas kumpulan fakta. Data merupakan bentuk jamak dari **datum**, berasal dari bahasa Latin yang berarti "sesuatu yang diberikan". Dalam penggunaan sehari-hari data berarti suatu pernyataan yang diterima secara apa adanya. Pernyataan ini adalah hasil pengukuran atau pengamatan suatu variabel yang bentuknya dapat berupa angka, kata-kata, atau citra. Dalam keilmuan (ilmiah), fakta dikumpulkan untuk menjadi data. Data kemudian diolah sehingga dapat diutarakan secara jelas dan tepat sehingga dapat dimengerti oleh orang lain yang tidak langsung mengalaminya sendiri, hal ini dinamakan deskripsi. Pemilahan banyak data sesuai dengan persamaan atau perbedaan yang dikandungnya dinamakan klasifikasi.

Menurut berbagai sumber lain, data dapat juga didefinisikan sebagai berikut [3]:

1. Menurut kamus bahasa inggris-indonesia, data berasal dari kata *datum* yang berarti fakta.

2. Dari sudut pandang bisnis, data bisnis adalah deskripsi organisasi tentang sesuatu (resources) dan kejadian (transactions) yang terjadi.

PEMBAHASAN

3.1 Analisa

Adapun analisa yang akan dibahas adalah: Analisa Enkripsi Algoritma ROT, Analisa Enkripsi Algoritma Block Cipher (CBC), Analisa Dekripsi Algoritma Block Cipher (CBC), Analisa Dekripsi Algoritma ROT

3.1.1 Analisa Enkripsi Algoritma ROT

ROT-**n** (rotate by **n**) merupakan salah satu algoritma enskripsi sederhana yang menggunakan pergeseran abjad-abjad sebanyak **n** untuk mengubah plain text menjadi cipher text**.** Artinya jika pada ROT-13**,** abjad A diganti dengan N sedangkan abjad B diganti dengan O demikian seterusnya.

ABCDEFGHIJKLMNOPQRSTUVWXYZabcd efghijklmnopqrstuvwxyz
NOPQRSTUVWXYZABCDEFGHIJKLMnopq rstuvwxyzabcdefghijklm

Proses Enkripsi :

Plainteks = BUDIDARMA
Cipherteks = OHRVRNEZN (Hasil Enkripsi)

3.1.2 Analisa Algoritma Enkripsi Block Cipher

Block Cipher adalah algoritma enkripsi yang akan membagi-bagi *plaintext* yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama. Pada umumnya, *block cipher* memproses *plaintext* dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit penggunaan pola-pola serangan yang ada untuk membongkar kunci. Pada cipher blok, rangkaian bit-bit plainteks dibagi menjadi blok- blok bit dengan panjang sama, biasanya 64 bit (tapi adakalanya lebih). Algoritma enkripsi menghasilkan blok cipherteks yang – pada kebanyakan sistem kriptografi simetri – berukuran sama dengan blok plainteks. Dengan blok cipher, blok plainteks yang sama akan dienkripsi menjadi blok cipherteks yang sama bila digunakan kunci yang sama pula. Ini berbeda dengan cipher aliran dimana bit-bit plainteks yang sama akan dienkripsi menjadi bit-bit cipherteks yang berbeda setiap kali dienkripsi. Dalam mode operasinya menggunakan *Cipher Block Chaining (CBC).*
Cara Kerja Algoritma Cipher Block Chaining :

1. Setiap block Ciphertext bergantung tidak hanya pada block plaintextnya tapi pada seluruh block sebelumnya.
2. Hasil enkripsi block sebelumnya diumpan balik kedalam enkripsi block yang current
3. Enkripsi block pertama memerlukan block semu (Co) yang disebut IV (Intialization Vektor)
4. IV dapat diberikan oleh pengguna atau dibangkitkan secara acak oleh program.

Proses Enkripsi :

Tabel 1 Proses Enkripsi

Char	Desimal	Hexa	Biner
O	79	4F	01001111
H	72	48	01001000
R	82	52	01010010
V	86	56	01010110
R	82	52	01010010
N	78	4E	01001110
E	69	45	01000101
Z	90	5A	01011010
N	78	4E	01001110

Plainteks = 01001111, 01001000, 01010010, 01010110, 01010010, 01001110, 01011010, 01001110
KUNCI (K) = 01010000
Intialization vektor :
W (C_0) = 010000011
01001111, 01001000, 01010010, 01010110, 01010010, 01011110, 01000101,
P1 P2 P3 P4 P5 P6 P7
01011010, 01001110
P8 P9

C1 = P1 ⊕ C0 → O
= 01001111 ⊕ 01000011
= 00001100
= 00001100 ⊕ K
= 00011000 ⊕ 01010000
= 01011100 => 10111000
C2 = P2 ⊕ C1 H
= 01001000 ⊕ 10111001 →
= 11110001
= 11110001 ⊕ K
= 11100011 ⊕ 01010000
= 10100001 => 01000011
C3 = P3 ⊕ C2 → R
= 01010010 ⊕ 01000011
= 00010001
= 00010001 ⊕ K
= 00010001 ⊕ 01010000
= 01000001 => 10000011
C4 = P4 ⊕ C3 → V
= 01010110 ⊕ 10000011
= 11010101
= 11010101 ⊕ K
= 11010101 ⊕ 01010000

= 10000101 => 00001011
C5 = P5 ⊕ C4 → R
= 01010010 ⊕ 00001011
= 01010101
= 01010101 ⊕ K
= 01010101 ⊕ 01010000
= 00000101 => 00001010
C6 = P6 ⊕ C5 → N
= 01001110 ⊕ 00001010
= 01000101
= 01000101 ⊕ K
= 01000101 ⊕ 01010000
= 00010101
C7 = P7 ⊕ C6 → E
= 01011010 ⊕ 00010101
= 01001111
= 01001111 ⊕ K
= 01001111 ⊕ 01010000
= 00011111 => 00111110
C8 = P8 ⊕ C7 → Z
= 00111110 ⊕ 00001100
= 01110010
= 01110010 ⊕ K
= 01110010 ⊕ 01010000
= 00100010 => 01001000
C9 = P9 ⊕ C8 → N
= 01000101 ⊕ 00001100
= 01001001
= 01001001 ⊕ K
= 01001001 ⊕ 01010000
= 00011001 => 01001000
Jadi Hasil Enkripsinya adalah :
10111000, 01000011, 10000011, 00001011, 00001010, 00010101, 00111110, 01001000, 01001000

3.1.3 Analisa Dekripsi Algoritma Block Cipher

Dekripsi Algoritma Block Cipher merupakan salah satu algoritma dekripsi sederhana yang menggunakan mode operasi *Cipher Block Chaining (CBC)* untuk mengembalikan cipher text menjadi plain text semula**.** Pada dekripsi block plainteks diperoleh dengan cara meng Xor kan IV dengan hasil dekripsi terhadap block Cipherteks pertama.

Proses Dekripsi

C = 10111000, 01000011, 10000011, 00001011, 00001010, 00001010, 00001100,
C1 C2 C3 C4 C5 C6 C7

11001110, 11001110,
C8 C9

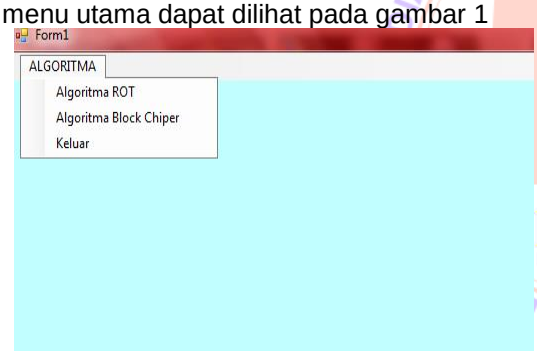
P1 = C1 ⊕ C0 → B
= 10111000 ⊕ 01000011
= 11111011
= 11111011 ⊕ K
= 11111011 ⊕ 01010000
= 10101011 => 01001111
P2 = C2 ⊕ C1 → U
= 01000011
= 10100000 ⊕ 10111000
= 00011000
= 00011000 ⊕ K
= 00011000 ⊕ 01010000
= 01001000
P3 = C3 ⊕ C2 → D
= 10000011
= 00000111 ⊕ 01000011
= 01000010
= 01000010 ⊕ 01010000
= 01010010
P4 = C4 ⊕ C3 → I
= 00001011
= 10001010 ⊕ 10001100
= 00000110
= 00000110 ⊕ 01010000
= 01010110
P5 = C5 ⊕ C4 → D
= 00001010
= 00000101 ⊕ 00001011
= 00000010
= 00000010 ⊕ 01010000
= 01010010
P6 = C6 ⊕ C5 → A
= 00010101
= 00101010 ⊕ 00001010
= 00011110
= 00011110 ⊕ 01010000
= 01001110
P7 = C7 ⊕ C6 → R
= 00111110
= 00011111 ⊕ 00010101
= 00001010
= 00001010 ⊕ 01010000
= 01011010
P8 = C8 ⊕ C7 → M
= 01001000
= 00100100 ⊕ 00111110
= 00011110
= 00011110 ⊕ 01010000
= 01001110
P9 = C9 ⊕ C8 → A
= 00010101
= 00101010 ⊕ 00001010
= 00011110
= 00011110 ⊕ 01010000

= 01001110
Jadi, hasil dekripsinya adalah :
01000010, 01010101, 01000100, 01001001, 01000100, 01000001, 01010010, 01001101, 01000001 = BUDIDARMA

3.1.4 Analisa Dekripsi Algoritma ROT

Dekripsi Algoritma ROT merupakan salah satu algoritma dekripsi sederhana yang menggunakan pergeseran abjad-abjad sebanyak **n** untuk mengembalikan ciphertext menjadi plaintext semula**.** Artinya jika pada ROT-13**,** abjad N diganti dengan A sedangkan abjad O diganti dengan B demikian seterusnya.
NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
Proses Dekripsi :
NOPQRSTUVWXYZABCDEFGHIJKLM
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipherteks = OHRVRNEZN
Plainteks = BUDIDARMA (Hasil Dekripsi)

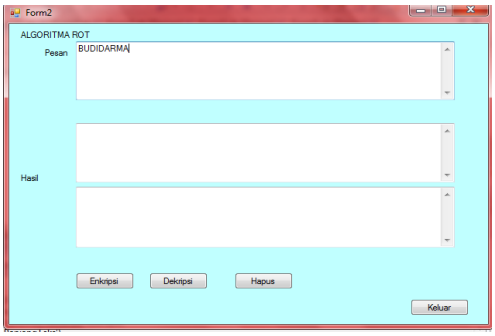
Tampilan menu utama merupakan tampilan yang muncul setelah menjalankan program untuk pengamanan teks. Tampilan menu utama dapat dilihat pada gambar 1



Gambar 1 Form Menu Utama

Pada gambar 1 diatas merupakan *form menu utama* yang berfungsi untuk menuju ke menu berikutnya sehingga pengguna bisa memilih menu untuk Algoritma ROT dan Algoritma Block Cipher.

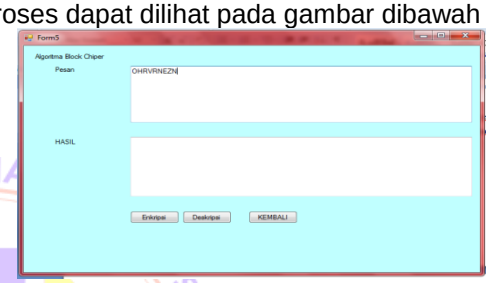
Tampilan berikutnya dari menu adalah menu Algoritma ROT. Tampilan awal proses dapat dilihat pada gambar dibawah ini :



Gambar 2 Form Algoritma ROT

Pada gambar 2 diatas merupakan form Algoritma ROT yang berfungsi untuk proses enkripsi dan deskripsi dalam Algoritma ROT.

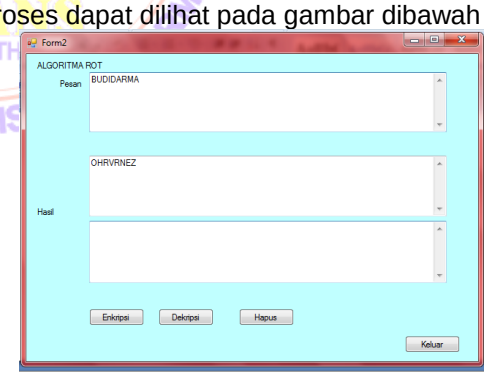
Tampilan berikutnya dari menu adalah menu Algoritma Block Cipher. Tampilan awal proses dapat dilihat pada gambar dibawah ini:



Gambar 3 Form Algoritma Block Cipher

Pada gambar 3 diatas merupakan form Algoritma Block Cipher yang berfungsi untuk proses enkripsi dan deskripsi.

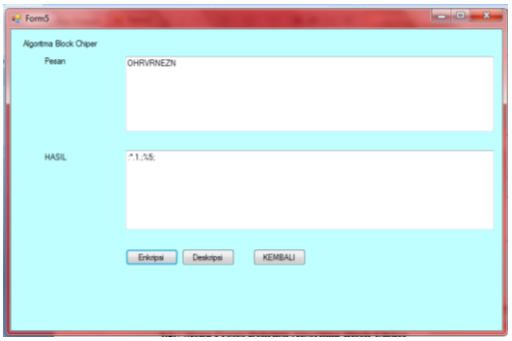
Tampilan berikutnya dari menu adalah menu enkripsi algoritma ROT. Tampilan awal proses dapat dilihat pada gambar dibawah ini:



Gambar 4. Tampilan menu enkripsi Algoritma ROT

Tampilan berikutnya dari menu adalah menu Enkripsi algoritma Block Cipher. Tampilan awal proses dapat dilihat pada gambar dibawah ini :

ISSN : 2548-6985

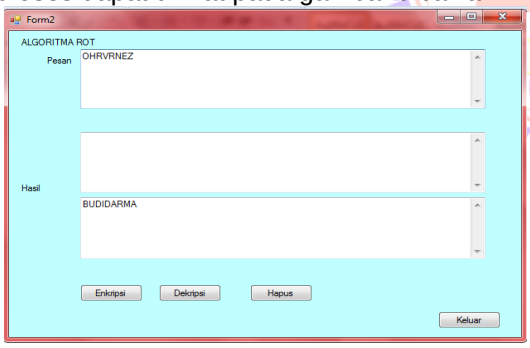


Gambar 5. Tampilan Menu Enkripsi Algoritma Block Cipher

Tampilan berikutnya dari menu adalah menu Dekripsi algoritma Block Cipher. Tampilan awal proses dapat dilihat pada gambar dibawah ini :

Gambar 6 Tampilan Menu Dekripsi Algoritma Block Cipher

Tampilan berikutnya dari menu adalah menu Dekripsi algoritma ROT. Tampilan awal proses dapat dilihat pada gambar dibawah ini:



Gambar 7 Tampilan Menu Dekripsi Algoritma ROT

KESIMPULAN

Berdasarkan dari pembahasan skripsi tersebut maka penulis menarik kesimpulan sebagai berikut :

1. Algoritma ROT melakukan proses enskripsi sederhana yang menggunakan pergeseran abjad-abjad sebanyak **n** untuk mengubah plain text menjadi cipher text dan Algoritma Block Cipher melakukan proses enkripsi yang akan membagi-bagi *plaintext* yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama.
2. Program dapat dibuat dengan menggunakan bahasa pemograman visual basic 2008 dengan form enkripsi dan dekripsi.

DAFTAR PUSTAKA

1. Adi Nugroho, “Rekayasa Perangkat Lunak Berorientasi Objek Dengan Metode USDP”, Penerbit Andi, Bandung, 2010
2. Dafid, “Kriptografi Kunci Simetri Dengan Menggunakan Algoritma Cryton”, Vol. 2, No. 3, 2006
3. http://id.wikipedia.org/wiki/Data/.diakses ,21-04-2015
4. Kaidir, Abdul, “Pengenalan Algoritma Pendekatan Secara Visual Dan Interaktif Menggunakan Raptor”, Penerbit Andi, Yogyakarta, 2013
5. Nurli Hairiah, “Analisa Dan Implementasi Algoritma Cipher Block Chaining Dalam Penyandian Teks ”, Vol. 5, No. 1, 2015
6. Rifki Sadikin, “Kriptografi Untuk Keamanan Jaringan ”, Penerbit Andi, Yogyakarta, 2012
7. Rinaldi Munir, “Kriptografi”, Penerbit Informatika Bandung, Bandung, Edisi 1, 2006
8. Tata Sutabri, “Sistem Informasi Manajemen ”, Penerbit Andi, Yogyakarta, 2005