PENERAPAN ALGORITMA CAESAR CIPHER DAN ALGORITMA VIGENERE CIPHER DALAM PENGAMANAN PESAN TEKS

Priyono

Mahasiswa Program Studi Teknik Informatika STMIK Budi Darma Medan
Jl.Sisingamangaraja No.338 Simpang Limun Medan
http://www.stmik.budidarma.ac.id // Email : upry_obay@yahoo.co.id

ABSTRAK

Kriptografi merupakan ilmu yang mempelajari cara pengamanan data atau pesan dengan tujuan mencegah dari orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya. Salah satu yang harus benar-benar dijaga adalah pesan yang bersifat rahasia.Pesan adalah setiap pemberitahuan, kata, atau komunikasi baik lisan maupun tertulis, yang dikirimkan dari satu orang ke orang lain.Algoritma caesar merupakan sistem persandian klasik berbasis subtitusi yang sederhana pada enkripsi dan dekripsi sebuah sistem persandian caesar menggunakan operasi shift.Algoritma Vigenere Cipher merupakan salah satu algoritma kriptografi klasik yang memanfaatkan prinsip bujursangkar vigenere untuk melakukan enkripsi.

Kata kunci : ***Kriptografi, Pesan,Caesar Cipher, Vigenere Cipher***

1. Pendahuluan

1.1 Latar Belakang

Kerahasiaan pesan atau data yang dimiliki oleh seseorang merupakan hal penting dalam pengiriman pesan agar pesan tersebut hanya dapat diberikan oleh orang tertentu saja yang dapat mengakses informasi tersebut. Di jaman yang serba canggih seperti ini alat untuk mengirim pesan sudah banyak termasuk medianya seperti: facebook dan twitter sehingga kita bisa mengirim pesan dengan cepat begitu pun sebaliknya kita bisa menerima pesan dengan cepat pula. Dari semua kemudahan tutentu akan sangat berpengaruh ketika kita akan mengirim pesan yang isinya hanya orang-orang tertentu saja yang boleh mengetahui isinya. Salah satu yang harus benar-benar dijaga adalah pesan yang bersifat rahasia karena jika pesan itu tersebar maka akan berdampak buruk pada kita. Salah satu cara yang biasa digunakan adalah dengan enkripsi. Enkripsi adalah proses untuk menyamarkan atau menyandikan pesan sehingga orang yang tidak berkepentingan tidak bisa mengetahui makna dari pesan tersebut. Untuk memperkuat keamanan pesan yaitu dengan menggunakan kriptografi sehingga orang tidak akan curiga jika pesan tersebut sudah terenkripsi dan orang akan tetap mengira jika pesan itu tidak mengandung pesan rahasia.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain (DonyAriyus 2006, 9). Seperti contoh algoritma kriptografi yaitu : algoritma *caesar cipher* dan *vigenere cipher*, algoritma caesar cipher dan vigener cipher termasuk kriptografi klasik yang menggunakan plainteks, cipherteks dan kunci untuk melakukan proses enkripsi dan dekripsi dalam pengamanan data. Algoritma *caesar chiper* adalah teknik kriptografi yang dilakukan dengan mensubtitusi setiap abjad dari pesan yang akan dienkripsi melalui pergeseran susunan sebagai kuncinya.

1.2 Rumusan Masalah

Beberapa rumusan masalah yang diambil dari latar belakang diatas adalah:

1. Bagaimana proses Enkripsi dan Depenelitian dalam pengamanan pesan teks?
2. Bagaimana cara menerapkan Algoritma *Caesar Cipher* dan Algoritma *Vigenere Cipher* dalam pengamanan pesan teks?
3. Bagaimana merancang sebuah aplikasi pengamanan pesan teks menggunakan Algoritma *Caesar Cipher* dan Algoritma *Vigenere Chiper*?

1.3 Batasan Masalah

Berikut adalah beberapa batasan masalah:

1. Karakter yang akan dienkripsi dan dekripsi adalah karakteryang ada pada tabel ASCII 256.
2. Panjang maksimal pesan yang akan di amankan adalah 14 karakter.
3. Metode yang digunakanadalahAlgoritma *Caesar Cipher* dan *Vigenere Cipher.*
4. Tidak membandingkan atau menggabungkan Algoritma yang dipakai
5. Bahasapemrograman menggunakan*Microsoft Visual Basic. Net* 2008

1.4 Tujuan dan Manfaat

Adapun Tujuan Penelitian ialah:

1. Menjelaskan bagaimana proses Enkripsi dan Depenelitian dalam pengamanan pesan teks.
2. Menjelaskan bagaimana cara kerja Algoritma *Caesar Cipher* dan *Vigenere Cipher* dalam pengamanan pesan teks.
3. Membangun sebuah aplikasi pengamananpesanteksmenggunakanAlgoritma*CaesarCipher*dan Algoritma *Vigenere Chiper*.

Dan sebagai manfaat penelitian yang dapat penulis uraikan adalah:

1. Melindungi dan merahasiakan pesan teks yang akan dikirim dengan menggunakan Algoritma *Caesar Cipher* dan *Vigenere Cipher*
2. Seseorang dapat mengirim suatu informasi rahasia tanpa takut diketahui isi informasi tersebut terhadap orang lain.
3. Memberi kemudahan bagi pengguna untukmengirimkan informasi rahasia lewat pesan yang dikirim

2 Landasan Teori

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia. Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yangmempelajari teknik-teknik matematika yang berhubungan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta *autentikasi* data (Menezes, Oorschot and Vanstone, 1996). Secara umum kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita (bruce Schneire-*Applied Cryptography*). Selain defenisi tersebut ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi (sumber: Rinaldi Munir,2006,2).Ada empat tujuanmendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

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.berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerimaan pesan menyangkal telah menerimanya (sumber: Rinaldi Munir,2006,9).
3. Otentikasi, adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-phak yang berkomunikasi (*user authentication* atau *entry authentication*) maupun mengidentifikasi kebenaran sumber pesan (*origin authentication*).
4. Nirpenyangkalan (*non-repudiation*), adalah layanan untuk mencegah entitas yang

2.2 *Caesar Cipher*

Caesar Cipher merupakan salah satu algoritma *cipher* tertua dan paling diketahui dalam perkembangan ilmu kriptografi. *Caesar cipher* merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks. Teknik seperti ini disebut juga sebagai chiper abjad tunggal.Algoritma kriptografi *Caesar Cipher* sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Adapun langkah-langkah yang dilakukan untuk membentuk chiperteks dengan *Caesar Cipher*adalah :Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks, Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.

Algoritma dari *Caesar Cipher* adalah C = E (P) = (P + K) mod 26 untuk fungsi enkripsi. Sedangkan untuk fungsi depenelitian adalah P = D (C) = (C - 7) mod 26 .

2.3 *Vigenere Cipher*

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifra del. Sig. Giovan Battista Bellaso pada tahun 1553. Nama vigenere sendiri diambil dari seorang yang bernama Blaise de Vigenere. Nama vigenere diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma ini dengan metode autokey cipher meskipun algoritma dasarnya telah ditemukan lebih dahulu oleh Giovan Battista Bellaso.

Algoritmanya adalah Enkripsi : Ci = (Pi + Ki) mod 25Dekripsi: Pi = (Ci – Ki) mod 25 ; untuk Ci > = Ki atau Pi = (Ci + 25 – Ki) mod 25 ; untuk Ci < = Ki

3. Analisa dan Perancangan

3.1 Analisa *Caesar Cipher*

Caesar Cipher merupakan salah satu algoritma *cipher* tertua dan paling diketahui dalam perkembangan ilmu kriptografi. *Caesar cipher* merupakan salah satu jenis *cipher* substitusi yang membentuk *cipher* dengan cara melakukan penukaran karakter pada *plainteks* menjadi tepat satu karakter pada *chiperteks*.

Teknik seperti ini disebut juga sebagai *chiper* abjad tunggal. Algoritma kriptografi *Caesar Cipher* sangat mudah untuk digunakan.

1. Enkripsi *Caesar Cipher*
   Cara kerja enkripsi dari algoritma *caesar cipher* dalam kriptografi adalah sebagai berikut :
   1. Tentukan nilai kunci (bilangan bulat positif)
   2. Konversikan setiap karakter plainteks ke desimal

3. Lakukan proses enkripsidengan formula (rumus) Ci = (Pi+K) Mod 256
4. Konversikan setiap nilai Ci ke karakter

Contoh :

Plainteks : PRIYONO_BUDIDA

Key : 2

Tabel 1 EnkripsiAlgoritma*Caesar Cipher*

P	R	I	Y	O	N	O	_	B	U	D	I	D	A
80	82	73	89	79	78	79	95	66	85	68	73	68	65

RumusCi = (Pi + K) mod 256

C_1 = (P_1 + K) mod 256

C_4 = (P4 +K) mod 256

= (P + 2) mod 256

= (Y + 2) mod 256

= (8O + 2) mod 256

= (89 + 2) mod 256

= 82 ⟶ R

= 91

C_2 = (P2 + K) mod 256 = 80

C_5 = (P5 +K) mod 256 = 95 _

=(R + 2) mod 256

= (82 + 2) mod 256

= (79 + 2) mod 256

= 84⟶ T

= 81⟶ Q

C_3 = (P3 +K3) mod 256

C_6 = (P6 +K) mod 256

= (I + 2) mod 256

= (N + 2) mod 256

= (73 + 2) mod 256

= 75 ⟶ K

C_7 = (P7 +K) mod 256

C_{11} = (P11 +K) mod 256

= (O + 2) mod 256

= (79 + 2) mod 256

= 81⟶ Q

= 70⟶F

C_8 = (P8 +K) mod 256

C_{12} = (P12 +K) mod 256

=(_ + Y) mod 256

= (I + 2) mod 256

= (95 + 2) mod 256

= (73 + 2) mod 256

= 97⟶ a

= 75⟶K

C_9 = (P9 + K9) mod 256 C_{13}

= (P13 +K) mod 256

= (B + 2) mod 256

= (66 + 2) mod 256 =

(68 + 2) mod 256

= 68 D ⟶ = 70

C_{10} = (P10 +K) mod 256 C_{14} = (P14 +K) mod 256

= (U + 2) mod 256 =

(A + 2) mod 256

= (85 + 2) mod 256 =

(65 + 2) mod 256

= 87 ⟶W

HasilEnkripsi (Ci) : R T K [Q P Q a D W F K F C

2. DekripsiAlgoritma*Caesar Cipher*

Cara kerjadekripsidarialgoritma*caesar cipher*dalamkriptografiadalahsebagaiberikut :

1. Konversikansetiapkarakter*ciphertek*skedesimal
2. Dekripsidengan formula (rumus) Pi= (Ci-K) Mod 256
3. Konversikan Pi kekarakter

Tabel 2 DekripsiAlgoritma*Caesar Cipher*

R	T	K	[	Q	P	Q	a	D	W	F	K	F	C
82	84	75	91	81	80	81	97	68	87	70	75	70	67

Rumus : Pi = (Ci – K) mod 256

P_1 = (C_1 - K) mod 256

P_8 = (C8 – K) mod 256

= (R - 2) mod 256

= (a - 2) mod 256

= (82 - 2) mod 256

= (97 - 2) mod 256

P ⟶

P_2 = (C2 –K) mod 256

P_9 = (C9 –K) mod 256

=(T - 2) mod 256

= (D - 2) mod 256

= (84 - 2) mod 256

= (68 - 2) mod 256

= 82 R ⟶

= 66 B

P_3 = (C3 - K) mod 256

P_{10} = (P10 - K) mod 256

= (K - 2) mod 256

= (78 + 2) mod256

= (W - 2) mod 256

= 80 P

= (75 - 2) mod 256

= (87 - 2) mod 256

= 73 ⟶ I

= (D + 2) mod 256

= 85 U

= (68 + 2) mod 256

P_4 = (C4 - K) mod 256

P_{11} = (C11 - K) mod 256

= ([- 2) mod 256

= (F - A) mod 256

= (91 - 2) mod 256

= (70 - 2) mod 256

= 89 ⟶ Y

= 68 D

P_5 = (C5 - K) mod 256 ⟶

P_{12} = (C12 – K) mod 256

= (Q - 2) mod 256

= (K - 2) mod 256

= (81 - 2) mod 256 \

= (75 - 2) mod 256 = (D + 2) mod 256

= 79⟶ O

= 73 ⟶ I

P_6 = (C6 -K) mod 256 F

P_{13} = (C13 -K) mod 256

= (P - 2) mod 256

= (F - 2) mod 256

= (80 - 2) mod256

= (70 - 2) mod 256

= 78⟶ N = 67 C = 68 D

P_7 = (C7 – K) mod 256
P_{14} = (C14 -K) mod 256
= (Q - 2) mod 256
= (C - 2) mod 256
= (81 - 2) mod 256
= (67 - 2) mod 256
= 79 → O
= 65 A
Hasil Dekripsi (Pi) : P R I Y O N O _ B U D I D A

3.2 Analisa *Vigenere Cipher*

Untuk mempermudah perhitungan *plainteks* dan key terlebih dahulu dibuat dalam tabel, seperti tabel 3 berikut :

Tabel 3 EnkripsiAlgoritma*Vegenere Cipher*

P	R	I	Y	O	N	O	_	B	U	D	I	D	A
80	82	73	89	79	78	79	95	66	85	68	73	68	65
O	B	A	Y	O	B	A	Y	O	B	A	Y	O	B
79	66	65	89	79	66	65	89	79	66	65	89	79	66

RumusCi = (Pi + Ki) mod 256
C_1 = (P_1 + K1) mod 256
C_4 = (P4+K4) mod 256
= (P + 0) mod 256
= (Y+ Y) mod 256
= (8O + 79) mod 256
= (89 + 89) mod 256
= 159 → Ÿ
= 178 2
C_2 = (P2+K2) mod 256
C_5 = (P5+K5) mod 256
=(R+ B) mod 256
= (82 + 66) mod 256
= (79 + 79) mod 256
= 148 → ”
= 158 Ž
C_3 = (P3+K3) mod 256
C_6 = (P6+K6) mod 256
= (I + A) mod 256
= (N + B) mod 256
= (73 + 65) mod 256
= 135 → ╪
C_7 = (P7+K7) mod 256 C_{11} = (P11+K11) mod 256
= (O + A) mod 256
= (79 + 65) mod 256
= 144 → 144 = 133 ...
C_8 = (P8+K8) mod 256 C_{12} = (P12+K12) mod 256
=(_ + Y) mod 256 = (I + Y) mod 256
= (95 + 89) mod 256 = (73 + 89) mod 256
= 184 → = 162 ç
C_9 = (P9+K9) mod 256 C_{13} = (P13 + K13) mod 256
= (B + O) mod 256 = (D + O) mod 256
= (66 + 79) mod 256 = (68 + 79) mod 256
= 145 → ‘
= 147 “
C_{10} = (P10 + K10) mod 256
C_{14} = (P14 + K14) mod 256
= (U + B) mod 256
= (A + B) mod 256
= (85 + 65) mod 256
= (65 + 66) mod 256
= 140 → Œ = 131 *ƒ*
HasilEnkripsi (Ci) : Ÿ ” ╪ 2 Ž 144 144 , ‘ Œ ... ç “*ƒ*

1. Dekripsi*Vegenere cipher*

Cara kerjadarialgoritma*vigenere cipher*dalamkriptografiadalahsebagaiberikut :

a. Konversikansetiapkarakter*cipherteks*dankuncik edesimal
b. Lakukan proses dekripsidengan formula (rumus) Pi = (Ci-Ki) Mod 256
c. Konversikansetiapnilai Pi kekarakter

Tabel 4 DekripsiAlgoritma*Vegenere Cipher*

Ÿ	”	╪	2	Ž	144	144	,	‘	Œ	...	ç	“	*ƒ*
159	148	135	178	158	144	144	184	145	140	133	162	147	131
O	B	A	Y	O	B	A	Y	O	B	A	Y	O	B
79	66	65	89	79	66	65	89	79	66	65	89	79	66

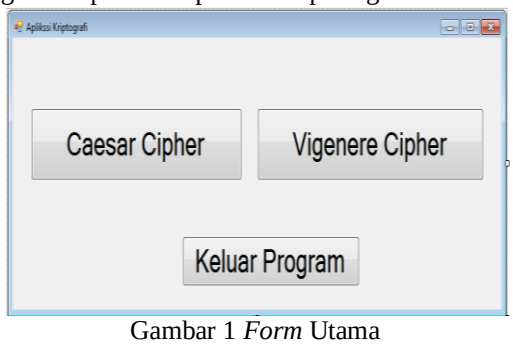
Rumus : Pi = (Ci – Ki) mod 256
P_1 = (C_1 - K1) mod 256
P_8 = (C8 – K8) mod 256
= (Ÿ - O) mod 256
= (Y) mod 256
= (O) mod 256
= (159 - 79) mod 256
= (184 - 89) mod 256
= 80 → P
P_2 = (C2 -K2) mod 256
P_9 = (C9 - K9) mod 256
=(” - B) mod 256
= (‘ - O) mod 256
= (148 - 66) mod 256
= (145 - 79) mod 256
= (78 + 66) mod256
= 82 R
= 144 → 144
= 66 → B
P_3 = (C3 - K3) mod 256 P_{10} = (P10 - K10) mod 256
= (╪ - A) mod 256
= (Œ - B) mod 256
= (68 + 65) mod 256
= (135 - 65) mod 256
= (140 - 65) mod 256
= 73 → I
= 85 → U
P_4 = (C4 - K4) mod 256
P_{11} = (C11 - K11) mod 256
= (2 - Y) mod 256
= (... - A) mod 256
= (178 - 89) mod 256
= (133 - 65) mod 256
= 89 → Y
= 68 → D

P_5 = (C5 - K5) mod 256
P_{12} = (C12 – K12) mod 256
= (Ž - O) mod 256
= (ç - Y) mod 256
= (158 - 79) mod 256
= (162 - 89) mod 256
= 79 → O
= 73 → I
P_6 = (C6 -K6) mod 256
P_{13} = (C13 -K13) mod 256
= (N - B) mod 256
= (“ - O) mod 256
= (144 - 66) mod256
= 144 → N
P_7 = (C7 – K7) mod 256
P_{14} = (C14 -K14) mod 256
= (144 - A) mod 256
= (144 - 65) mod 256
= (147 - 79) mod 256
= 79 → O
= 68 → A
HasilDekripsi (Pi) : P R I Y O N O _ B U D I D A

Implementasi

a. *Form* Utama

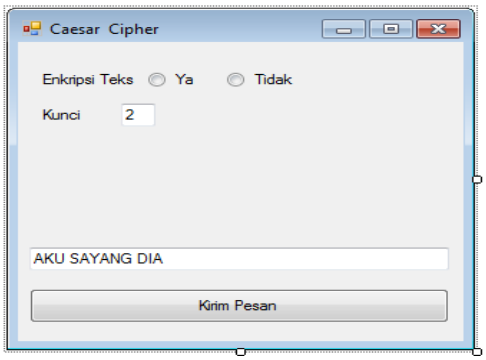
Form utama adalah form untuk pengguna dalam menampilkan algoritma guna melakukan pengiriman pesan. Dapat dilihat pada gambar 1



Gambar 1 *Form* Utama

b. *Form Caesar Cipher*

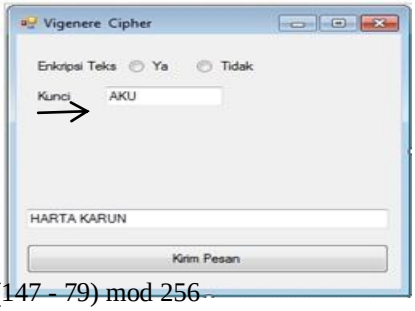
Form Caesar Cipher adalah *form* untuk pengguna dalam melakukan pengiriman pesan melalui algoritma *caesar cipher*.



Gambar 2 *Form* Enkripsi *Caesar Cipher*

c. *Form Vigenere Chiper*

Form Vigenere Cipher adalah *form* untuk pengguna dalam melakukan pengiriman pesan melalui algoritma *caesar cipher*.



= (147 - 79) mod 256
= 168 D

= (“ - O) mod 256

Gambar 3 *Form* Enkripsi *Vigenere Cipher*

Gambar 4 *Form* Depenelitian *Vigenere Cipher*

5 Kesimpulan

1. Keamanan pesan teks dapat diimplementasikan dengan metode enkripsi, salah satunya adalah enkripsi caesar cipher dan vigenere cipher. Dimana proses pesan yang dikirim atau diterima dapat diubah dengan metode caesar dan viginere untuk keamanan isi dari pesan.
2. Metode penyandian Caesar Cipher dan Vigenere Cipher termasuk dalam kriptografi klasik dimana kedua algoritma tersebut merupakan teknik enkripsi yang paling sederhana dan banyak digunakan.
3. Pada proses pengenkripsian digunakan rumus mod 256 dalam mode ASCII. Supaya tidak hanya 26 karakter saja yang dapat diproses melainkan semua karakter yang ada pada tabel ASCII dapat digunakan.

Saran

1. Perbaikan dan pengembangan aplikasi pengamanan pesan teks yang dirancang sangat diperlukan untuk memenuhi kebutuhan pengguna dalam berkomunikasi.
2. Pada penelitian selanjutnya aplikasi ini diharapkan dapat berkembang agar bisa lebih berguna lagi, dengan mengembangkan fitur lain agar penerapan algoritma kriptografi ini lebih efisien seperti mengkombinasikan kedua

algoritma tersebut, atau juga menambahkan kriptogrtafi yang lebih modern seperti, DES, AES, dan lain sebagainya.

Daftar Pustaka

1. Abdul Kadirdan Terra Ch. Triwahyuni, "PengantarTeknologiInformasiEdisiRevisi", Penerbit ANDI, Yogyakarta, 2013
2. C. WidyoHermawan (ed), "Visual Basic 2008", Penerbit ANDI, Yogyakarta, 2009
3. DepartemenPendidikan Dan Kebudayaan, 2008, *KamusBesarBahasa Indonesia*, BalaiPustaka,Jakarta.
4. DonyAriyusdan Rum Andri K.R, "Komunikasi Data", Penerbit ANDI, Yogyakarta, 2008
5. Dody Indra Harahap, "ImplementasiVigenere Cipher Dengan Random Key Metode Linear Feddback Shift Register (LFSR) Pada Teks", PelitaInformatika Budi Darma : V, Nomor :2 Desember 2013
6. Faterdhi Rizky Andhika, "Midifikasi Cipher Block Chaining (CBC) MAC dengan Penggunaan Vigenere Cipher, Pengubahan Mode Block, dan Pembangkitan Kunci Berbeda untuk tiapBlok" Makalah IF3058 Kriptografi-Sem. II Tahun 2011
7. Prastuti, "AnalisisdanPerancangan Unified ModellingLaguage (UML) Generate VB.6", GrahaIlmu, Yogyakarta, 2013
8. RifkiSadikin,"Kriptografi untuk Keamanan Jaringan", Penerbit ANDI, Yogyakarta, 2012.
9. Rinaldi Munir, "Kriptografi", Penerbit Informatika, Bandung, 2006.
10. Rosa A.S "Database Design", PT. Elex Media Komputindo, Jakarta, 2015.
11. Suyanto M, "Pengantar Teknologi Informasi" ,Penerbit ANDI, Yogyakarta, 2015
12. http://kursuswebsite.org/webdesign/simbol-sequence-diagram, diaksestanggal 10 Mei 2015)