KOMBINASI VIGENERE CIPHER DAN POLYALPHABETIC CIPHER PADA PENGAMANAN FILE TEXT

Elvin Tarigan[1], Denny H.S. Maha[2], Eliasta Ketaren[3]

[1,2,3]STMIK Kristen Neumann Indonesia
Jl. Letjen Jamin Ginting KM. 10,5 Medan
elvintarigan18@gmail.com

Program Studi Teknik Informatika

ABSTRAK

Kriptografi merupakan seni untuk merahasiakan keamanan pesan. Tujuan penelitian ini adalah menghasilkan sebuah aplikasi enkripsi dan dekripsi untuk mengamankan pesan yang berbentuk teks dengan mengkombinasikan dua metode Kriptografi Vigenere Cipher dan Polyalphabetic Cipher. Saat terjadinya proses enkripsi dan dekripsi sebaiknya harus menginputkan plaintext dan kunci dahulu untuk menjalankan program. Dalam merancang aplikasi ini menggunakan bahasa pemograman Visual Studio 2010. Melalui aplikasi ini pengguna dapat melakukan Pengkombinasian Vigenere Cipher dengan Polyalphabetic Cipher dan menghasilkan enkripsi dan dekripsi terhadap sebuah teks ataupun kalimat. Dalam proses penyandian memiliki batas karakter yang ditentukan yaitu 200 karakter. Plaintext dibagi menjadi 1 blok terdiri dari 3 karakter. Pada aplikasi Kombinasi ini menggunakan 3 kunci. Pada kunci tidak diperkenankan ada huruf yang berulang. Hasil enkripsi dan dekripsi yang dilakukan akan menghasikan spasi pada kalimat.

Kata kunci : Kriptografi, Keamanan Pesan, Enkripsi-dekripsi, Vigenere Cipher dan Polyalphabetic Cipher.

PENDAHULUAN

Perkembangan teknologi yang sangat pesat saat ini yang memungkinkan dapat berkomunikasi dan saling bertukar informasi secara jarak jauh. Begitu banyak pengguna seperti suatu perusahaan dan lembaga yang ingin menjaga keamanan kerahasiaan informasi atau datanya tidak ingin diketahui oleh sembarang pihak. Sebab itu dikembangkanlah ilmu-ilmu yang mempelajari bagaimana teknik pengamanan data yang disebut kriptografi.

Untuk melindungi keamanan kerahasiaan data, kriptografi dapat mengubah data asli (plaintext) ke bentuk sandi (ciphertext) agar tidak dimengerti lagi maknanya. Ciphertext ini yang akan dikirim oleh pengirim kepada penerima dan ciphertext akan di transformasikan berubah seperti semula agar dapat dimengerti lagi maknanya.

Kriptografi merupakan suatu cara ataupun seni untuk mengamankan suatu pesan yang diamankan melalui proses pengenkripsian /penyandian. Pengamanan data atau pesan bisa dilakukan dengan berbagai algoritma kriptografi, salah satunya dengan menggabungkan algoritma Vigenere dan Polyalphabetic Cipher agar data/infomasi tidak mudah diketahui orang lain. Pada proses pembuatan tugas akhir ini data yang akan diamankan berupa teks.

Vigenere cipher kode abjad majemuk(*polyalphabetic substitution cipher*). Vigenere cipher termasuk dalam kriptografi klasik yang pada dasarnya cukup sulit dipecahakan, vigenere cipher merupakan metode substitusi Polyalfabetic dengan huruf campuran. Polyalphabetic ataupun cipher abjad majemuk menggunakan sejumlah monoalphabetic cipher, metode polyalphabetic menghasilkan pola enkripsi yang lebih acak karena, setiap huruf yang sama menghasilkan penyandian yang berbeda.

Berdasarkan latar belakang masalah diatas penulis merasa tertarik untuk mengangkat judul skripsi **"Kombinasi Vigenere Cipher Dan Polyalphabetic Cipher Pada Pengamanan File Text"**

Berdasarkan penjelasan latar belakang diatas, maka dapat dirumuskan beberapa hal dalam penjelasan skripsi ini adalah bagaimana menghasilkan aplikasi yang dapat mengenkripsi dan dekripsi sebuah teks dengan menggabungkan dua algoritma Vigenere cipher dan Polyalphabetic cipher.

Tujuan yang ingin dicapai untuk menghasilkan aplikasi yang dapat mengenkripsi dan mendekripsikan vigenere cipher dan polyalphabetic cipher.

Adapun manfaat yang diperoleh ialah:

a. Memahami cara mengubah enkripsi ke deksripsi dan juga mengubah dekripsi ke enkripsi dengan kombinasi pada metode vigenere dan polyalphabetic.
b. Memberikan tingkat keamanan atau kerahasiaan yang akurat dalam komunikasi ataupun informasi.
c. Menerapkan ilmu dan pengetahuan yang sudah di dapat untuk merancang aplikasi sistem selama kuliah.

Definisi Kriptografi

Bahasa kriptografi berasal dari kata *crypto* yang berarti rahasia dan *graphy* yang berarti tulisan. Jadi kriptografi dapat diartikan sebagai tulisan rahasia.

Kriptografi secara umum merupakan ilmu dan seni untuk menjaga keamanan kerahasiaan data. Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi. Namun pada kriptografi tidak semua aspek keamanan informasi akan ditangani.

Vigenere Cipher

Kode Vigenere termasuk kode abjad-majemuk (*polyalphabetic substitution cipher*). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) perancis, Blaise de Vigenere pada abad 16, tahun 1586.

Vigenere cipher merupakan jenis *cipher* abjad majemuk sederhana. Vigenere Cipher menerapkan metode substitusi polialfabetik dan termasuk ke dalam katagori kunci simetris dimana kunci yang digunakan untuk proses enkrispi adalah sama dengan kunci yang digunakan untuk proses dekripsi.

Enkripsi dengan metode algoritma Vigenere Cipher pada dasarnya adalah menggunakan prinsip Caesar cipher dengan melakukan pengenkripsi karakter pada plaintext yang diubah menjadi karakter lain pada cipherteks. Perbedaaan antara Caesar Cipher dan Vigenere Cipher adalah huruf yang sama pada plainteks tidak selalu di enkripsi menjadi huruf yang sama pada cipherteks. Hal ini disebabkan karena pada Vigenere Cipher, pergeseran karakternya ditentukan pada karakter kunci dan kata ini selalu di ulang.

Teknik dari substitusi Vigenere Cipher bisa dilakukan dengan 2 cara yaitu dengan angka dan huruf :

1. Angka

   Teknik substitusi vigenere dilakukan dengan menggunakan angka dengan menukarkan huruf dengan angka. Hal tersebut mirip dengan Shift Cipher.

Tabel 1. Teknik Substitusi Vigenere

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Memiliki kunci dengan 6 huruf CIPHER, jika kita tukar dengan angka, maka akan menjadi K= (2, 8, 15, 7, 4, 17). Dengan demikian, plaintextnya adalah "This cryptosystem is not secure."

Tabel 2. Hasil Dekripsi Substitusi Vigenere

T	H	I	S	C	R	Y	P	T	O	S	Y	S	T
19	7	8	18	2	17	24	15	19	14	18	24	18	19
I	S	[illegible]					S	[illegible]		T	[illegible]		

E	M	I	S	N	O	T	S	E	C	U	R	E
1	12	8	18	13	14	19	18	4	2	20	17	4
B	[illegible]											

Plaintext : This cryptosystem is not secure

Kunci : (2,8,15,7,4,17)

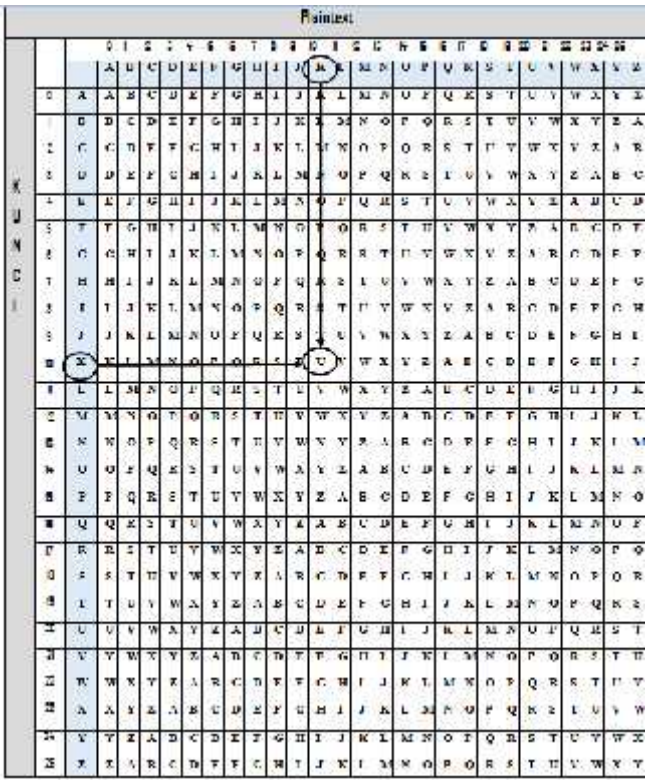
Ciphertext : VPXZGIAXIVWPUBTT MJPWIZITWZT

Untuk melakukan dekripsi, kita juga bisa menggunakan kunci yang sama dengan modulo 26.

2. Huruf

   Cara menentukan ciphertext pada sistem ini bisa dilihat pada tabel pada posisi horizontal yang merupkan plaintext dan pada posisi vertical kunci. Jika plaintext huruf K, maka lihat posisi letak huruf K pada plaintext tabel dan posisi huruf K pada posisi kunci. Jika sudah menemukan, tarik garis lurus ke bawah dari plaintext dan garis lurus ke samping dari posisi kunci hingga kita menemukan huruf U. Dengan demikian, huruf U yang akan menjadi ciphertext, dan begitu seterusnya. Dibawah ini contoh gambar substitusi dengan huruf.

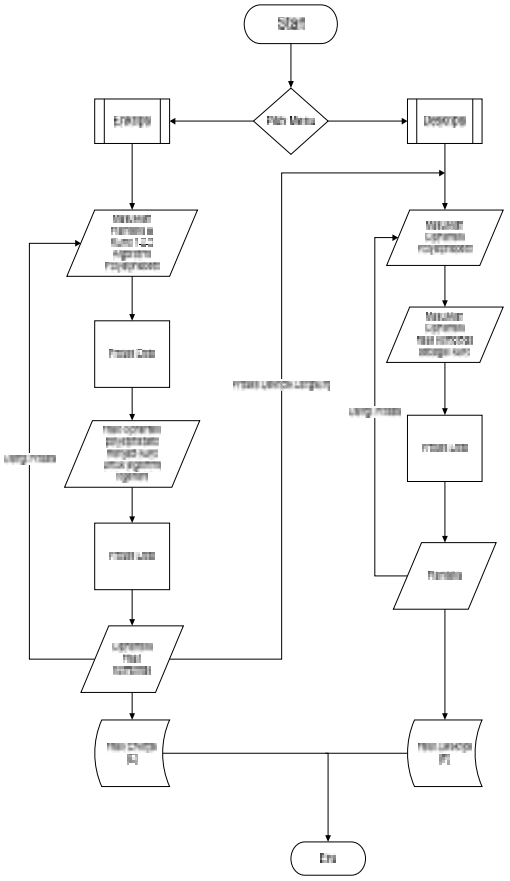
Tabel 3. Substitusi Vigenere Dengan Huruf



Polyalphabetic Cipher

Polyalphabetic merupakan penyandian yang dilakukan dengan mengelompokkan beberapa huruf menjadi sebuah kesatuan dan kemudian dienkripsi. Pada cipher ini, menggunakan beberapa alfabet kemudian ditulis disebuah tabel. Polyalphabetic cipher menggunakan cipher abjad-tunggal yang masing-masing dengan kunci berbeda.

METODE PENELITIAN



Pada gambar diatas *Flowchart* proses analisis perancangan sistem menunjukkan bagaimana cara kerja sistem untuk mengamankan suatu data. Pertama untuk melakukan proses enkripsi yaitu, dengan memilih menu setelah itu memasukkan plainteks dan kunci maka data akan diproses dan akan dilakukan penyandian atau enkripsi dan mendapatkan hasil pengenkripsian berupa ciphertext. Ciphertext yang dihasilkan tersebut akan didekripsi untuk mengembalikan data ke seperti semula yaitu menjadi plaintext.

HASIL DAN PEMBAHASAN

Hasil Perangkat Lunak

Sesuai dengan perancangan aplikasi BAB III, maka diperoleh hasil yang sebenarnya. Adapun aplikasi yang dimaksud terdiri dari beberapa Form, yaitu :

Form Menu Utama

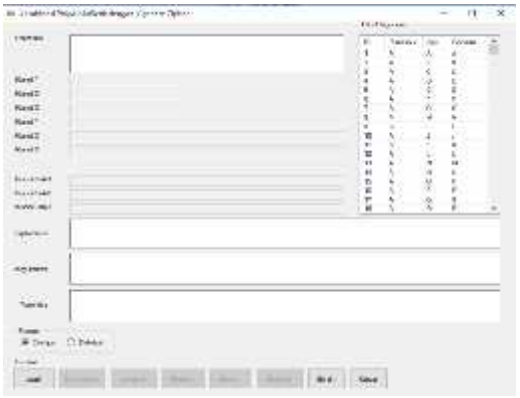
Form menu utama ini merupakan tampilan yang pertama kali meuncul pada saat kita jalankan aplikasi.

Gambar 1. Tampilan Menu Aplikasi

Tampilan form Menu utama ini terdapat dua menu yaitu Kombinasi kriptografi dan Exit dimana pada menu kriptografi kita akan melakukan teknik enkripsi dan juga dekripsi dan combo Exit yang kegunaanya untuk keluar aplikasi.

Tampilan Form Kombinasi Kriptografi

Pada Form ini *user*/pengguna diminta untuk mengetikkan teks yang akan di enkripsi ataupun didekripsi dan juga user/pengguna diminta untuk memasukkan kunci agar dapat melakukan jalan ataupun taknik enkripsi dan juga dekripsi.



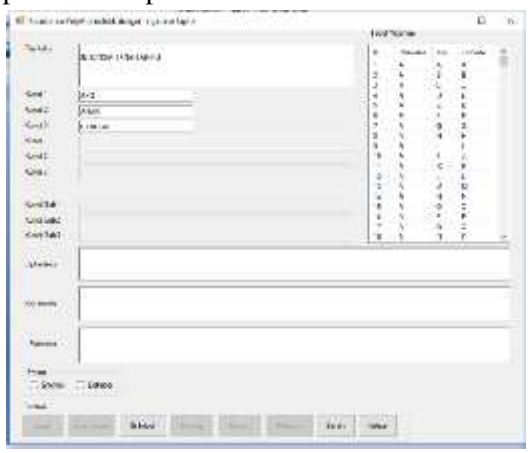
Gambar 2. Form Kombinasi Polyalphabetic dengan Vigenere Cipher

Pada Form Kombinasi kriptografi proses pilihan enkripsi dan dekripsi berfungsi untuk menentukan plaintext yang akan dienkripsi dan didekripsi, tombol Enkripsi yang berfungsi untuk melakukan teknik penyandian, tombol dekripsi yang

berfungsi untuk melakukan teknik pengembalian kalimat yang sebenarnya, tombol kombinasi berfungsi untuk melakukan pengkombinasian algoritma Vigenere dan Polyalphabetic Cipher, tombol load yang berfungsi untuk melakukan penggilan file atau membuka file yang ingin dienkripsi maupun didekripsi, tombol load kunci yang berfungsi untuk memaanggil kunci yang sudah tersimpan ke dalam bentuk file, tombol simpan berfungsi untuk menyimpan hasil enkripsi plaintext dan kunci yang disebut *ciphertext*, tombol bersih berfungsi untuk mengahapus semua teks disemua kolom ketika kita mau mengulangi proses dari awal dan tombol keluar berfungsi ketika kita mau mengakhiri atau keluar dari program.

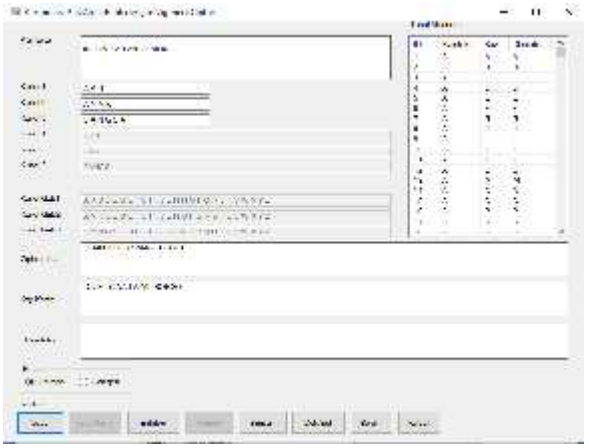
Tampilan Form Enkripsi

Setelah membuka Form Kombinasi Kriptografi *user*/pengguna diminta untuk mengetikan kalimat yang akan dienkripsi dan *user*/pengguna juga diminta untuk mengetikkan kunci agar dapat melakukan proses enkripsi.



Gambar 3. Tampilan form kombinasi kriptografi sebelum dienkripsi

Setelah *user*/pengguna melakukan enkripsi dengan teks yaitu INDONESIATANAHAIRKU dan kuncinya AKU, ANAK, BANGSA, maka :

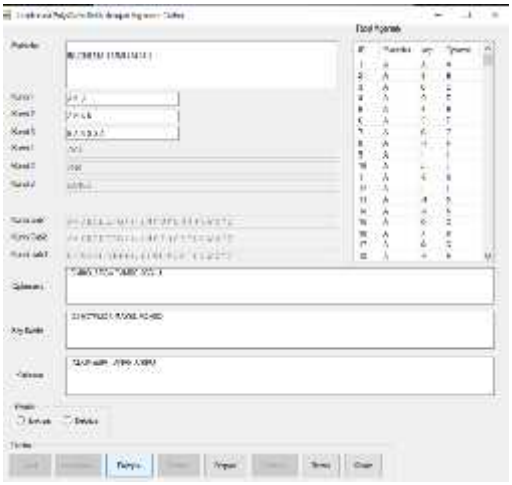


Gambar 4. Tampilan form setelah dienkripsi dan dikombinasikan.

Pada saat *user*/pengguna melakukan proses enkripsi, setiap karakter atau huruf yang sama pada setiap kunci akan dihilangkan, karna setiap huruf dalam kuncinya hanya diperkenankan muncul sekali maka setelah proses enkripsi teks diubah menjadi kalimat yang sudah tidak dimengerti lagi maknanya (*Ciphertext*).

Proses Dekripsi

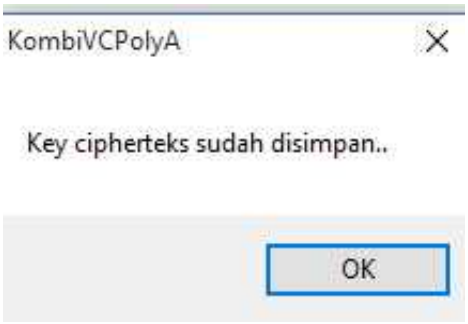
Proses Dekripsi tidak jauh berbeda dengan proses enkripsi, yaitu Setelah membuka form kombinasi kriptografi *user*/pengguna bisa langsung mendekripsikan teks kembali menjadi pesan yang sebenarnya yang disebut (*Plaintext*).



Gambar 5. Tampilan form kombinasi kriptografi setelah dekripsi langsung.

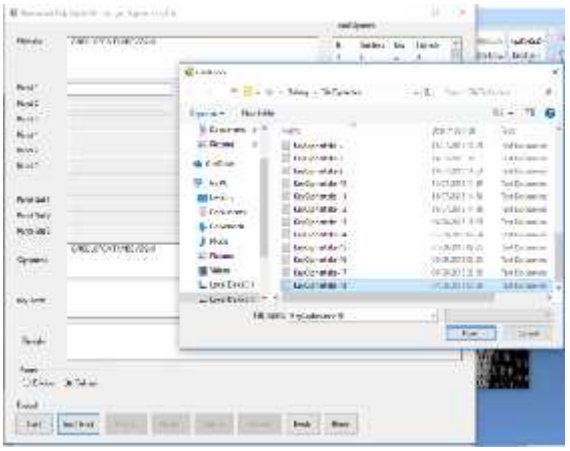
Pada saat *user*/pengguna melakukan proses dekripsi langsung maka

ciphertext akan berubah menjadi data atau pesan yang asli (*Plaintext*). Dan *user*/pengguna dapat menyimpan *ciphertext* dan kunci kedalam sebuah file yang nantinya bisa didekripsi kembali.



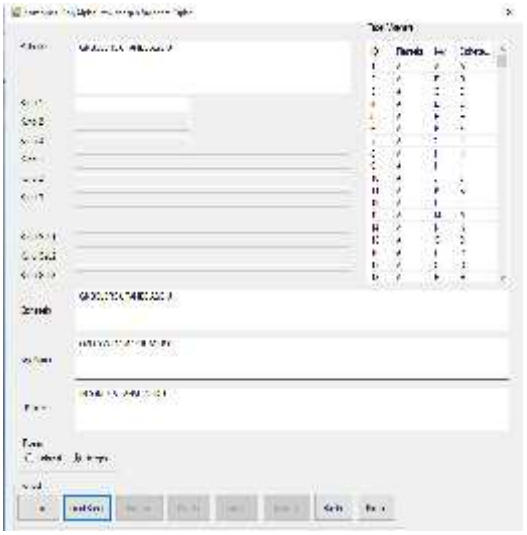
Gambar 6. Ciphertext yang sudah disimpan Setelah *user*/pengguna menyimpan

hasil dekripsi dan kunci, otomatis ciphertext dan kunci akan disimpan kedalam sebuah file, maka setelah itu untuk mengembalikan *ciphertext* kedalam bentuk *plaintext* adalah dengan menggunakan tombol proses Load dan Load Kunci.



Gambar 7. Dekripsi menggunakan Load dan Load Kunci

Pada saat *user*/pengguna melakukan proses dekripsi pada tombol Load dan Load Kunci maka ciphertext yang sudah tersimpan dan kita pilih akan muncul sebagai *ciphertext* dan *key* pada form untuk melakukan cara pengembalian kalimat atau pesan asli.



Gambar 8. Hasil Dekripsi Menggunakan Load dan Load Kunci

Pada saat user/pengguna melakukan proses dekripsi maka *ciphertext* akan kembali menjadi pesan yang asli (*Plaintext*).

KESIMPULAN

Dari hasil penelitian yang dilakukan penulis terhadap aplikasi kriptografi enkripsi dan dekripsi teks dengan menggabungkan kombinasi algoritma *Vigenere Cipher* Dan *Polyalphabetic Cipher*, penulis menarik beberapa kesimpulan, yaitu :

1. Proses pengenkripsian dan dekripsi dapat dilakukan secara langsung dan disimpan terlebih dahulu kedalam sebuah file.
2. Proses Enkripsi kunci pada algoritma *Polyalphabetic Cipher* diperkenankan hanya muncul sekali atau menghapus karakter/abjad yang berulang.
3. Kombinasi ini memliki 3 kunci dan plaintext pada proses algoritma Polyalphabetic memiliki 1 blok terdiri dari 3 karakter
4. Dengan adanya aplikasi yang dirancang oleh penulis maka algoritma *Vigenere Cipher* dapat menerapkan metode substitusi polialfabetic.

DAFTAR PUSTAKA

[1] Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi. Yogyakarta : Andi Offset.

[2] Ariyus, Dony. 2005. *Computer Security*. Yogyakarta. Andi Offset

[3] Chandra, Rina dan Noer Santi. 2014. *Implementasi Algoritma Enkripsi Playfair pada File Text*. Jurnal Teknologi Informasi Volume : VII, Nomor : 2

[4] Munir, Rinaldi. 2006. ***Kriptografi***. Bandung : informatika

[5] Munir, Rinaldi. 2004. Algoritma Kriptografi Klasik. Bandung. Informatika

[6] Suarga, 2005. *Algoritma dan Pemograman*. Yogyakarta, ANDI.

[7] Sugiyono, 2013. *Metode Penelitian Kombinasi (Mixed Methods)*. Bandung : Alfabeta

[8] Sitepu, N. B. 2014. PerbandinganAlgoritma*Elias Gamma Code* dengan Shannon-Fano untukKompresi File Teks. Skripsi. Universitas Sumatera Utara.

[9] Yesputra, Rolly. 2017. ***Belajar Visual Basic.Net denganVisual Studio 2010***, Penerbit Royal Asahan Press Kisaran