Perancangan Aplikasi Penyandian Pesan Teks dengan Menggunakan Algoritma Digraph Cipher

Yhopi Suhelna
STMIK Budidarma Medan, Jl. Sisingamangaraja No.388 Simpang Limun Medan
E-mail: yovie_suhelna@yahoo.com

Abstrak- Manusia berinteraksi dengan sesama manusia menggunakan komunikasi. Tidak semua hal yang dikomunikasikan tersebut berisi pesan sehingga dapat diketahui oleh banyak orang, adakalanya komunikasi tersebut bersifat rahasia sehingga hanya orang-orang tertentu yang dapat mengetahuinya. Terjadinya penyadapan data yang disampaikan tentunya menjadi masalah apabila data tersebut bersifat rahasia, oleh sebab itu dibutuhkan sistem pengamanan data sehingga data tersebut tidak dapat dicuri atau diubah oleh penyadap atau cracker. Salah satu solusi untuk mengamankan data adalah dengan menggunakan kriptografi. Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari satu media ke media lainnya tanpa mengalami gangguan dari pihak ketiga. Melalui teknik kriptografi, data dapat diubah menjadi sandi-sandi yang tidak dimengerti serta mengembalikannya kembali ke semula, proses ini disebut enkripsi dan dekripsi data. Proses pengaman data ini menggunakan metode Digraph Cipher. Beberapa kemudahan dalam metode Digraph Cipher yaitu kunci yang digunakan dalam proses enkripsi dan dekripsi adalah sama (simetris) dan proses dekripsi merupakan kebalikan dari proses enkripsi.

Kata Kunci : kriptografi, Digraph Cipher, enkripsi, dekripsi.

Abstract-Humans interact with fellow humans using communication. Not everything that is communicated contains a message so that it can be known by many people, sometimes the communication is confidential so that only certain people can know it. The occurrence of data tapping submitted is certainly a problem if the data is confidential, therefore a data security system is needed so that the data cannot be stolen or changed by tappers or crackers. One solution to secure data is to use cryptography. Cryptography is the science and art of maintaining message security when messages are sent from one media to another without experiencing interference from third parties. Through cryptographic techniques, data can be changed into passwords that are not understood and return them back to the original, this process is called data encryption and decryption. This data security process uses the Digraph Cipher method. Some facilities in the Digraph Cipher method are the keys used in the encryption and decryption process are the same (symmetrical) and the decryption process is the opposite of the encryption process.

Keywords: cryptography, Digraph Cipher, encryption, decryption.

PENDAHULUAN

Manusia berinteraksi dengan sesama manusia menggunakan komunikasi, baik secara lisan maupun tulisan. Tidak semua hal yang dikomunikasikan tersebut berisi pesan sehingga dapat diketahui oleh banyak orang. Ada kalanya hal yang dikomunikasikan tersebut bersifat rahasia sehingga hanya orang-orang tertentu yang dapat mengetahuinya. Kerahasiaan dan keamanan data adalah hal yang sangat penting dalam komunikasi data, baik dengan tujuan keamanan bersama, maupun untuk privasi individu. Para pengguna komputer yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikan atau yang akan disimpan[1].

Terjadinya penyadapan data yang disampaikan tentunya menjadi masalah apabila data tersebut bersifat rahasia. Oleh karena itu dibutuhkan sistem pengamanan data, ketika data tersebut disampaikan kepihak yang bersangkutan. Data yang dikirim melalui media tersebut belum tentu terjamin keamanannya, karena media yang menghubungkan antara pengirim dan penerima informasi tersebut terlebih dahulu mengubah informasi menjadi kode/isyarat. Kode inilah yang akan dimanipulasi dengan berbagai macam cara untuk diubah kembali menjadi data kepada penerima, sehingga dimungkinkan dapat terjadi pencurian dan pengubahan data yang dilakukan oleh penyadap atau *cracker*. Hal ini tentunya menjadi masalah besar apabila data yang disadap merupakan data yang sangat penting dan rahasia yang tidak seharusnya diketahui secara umum[2], [3].

Salah satu solusi untuk mengamankan data adalah dengan menggunakan kriptografi. Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu media ke media lain tanpa mengalami gangguan dari pihak ketiga. Seiring dengan semakin berkembangnya teknologi jaringan komputer dari internet, semakin banyak aplikasi yang memanfaatkan teknologi jaringan. Melalui teknik kriptografi, data dapat diubah menjadi sandi-sandi yang tidak dimengerti serta mengembalikannya kembali ke semula, proses ini disebut enkripsi dan dekripsi data. Enkripsi merupakan proses

mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus[4].

Berdasarkan uraian latar belakang di atas, maka dapat diambil beberapa perumusan masalah yang berhubungan dengan masalah keamanan data antara lain:

1. Bagaimana prosedur enkripsi dan dekripsi pesan teks dengan algoritma *digraph cipher*?
2. Bagaimana menerapkan algoritma *digraph cipher* dalam proses penyandian pesan teks?
3. Bagaimana merancang aplikasi penyandian pesan teks berdasarkan algoritma *digraph cipher*?

Adapun yang menjadi batasan masalah dalam penulisan skripsi ini adalah sebagai berikut:

1. Hanya membahas tentang prosedur enkripsi dan dekripsi pesan teks dengan algoritma *digraph cipher*, tidak membahas tentang prosedur distribusi pesan.
2. Pengujian program ini hanya pada satu komputer *stand alone* saja, tidak pada jaringan.
3. Pesan yang akan dienkripsi adalah pesan teks.
4. Bahasa pemrograman yang digunakan adalah *Visual Basic.Net 2008*

LANDASAN TEORI

2.1 Kriptografi

Kriptografi merupakan suatu ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting ke dalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula dengan menggunakan berbagai macam teknik yang telah ada sehingga informasi tersebut tidak dapat diketahui oleh pihak manapun yang bukan pemilik atau yang tidak berkepentingan. Kriptografi juga mempunyai sejarah panjang yang sangat menarika[1]. Kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang-orang Mesir dengan menggunakan *hieroglyph* yang tidak standar untuk menulis pesan.

Aspek-aspek keamanan yang merupakan tujuan utama dari suatu sistem kriptografi [3] adalah sebagai berikut :

1. Kerahasiaan (*confidentiality*)
   Kerahasiaan adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak kecuali pihak yang memiliki otoritas terhadap informasi. Ada beberapa pendekatan untuk menjaga kerahasiaan dari pengamanan secara fisik hingga penggunaan algoritma matematika yang membuat data tidak dapat dipahami.
2. Integritas Data (*data integrity*)
   Integritas data berhubungan dengan penjagaan dari perubahan data secara tidak sah. Agar integritas data terjaga, maka sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain menyangkut penyisipan, penghapusan, dan pensubstitusian data lain ke dalam data yang sebenarnya. Layanan di dalam kriptografi dapat direalisasikan dengan menggunakan tanda tangan (*signature scheme*). Pesan yang di tandatangani menyiratkan bahwa pesan yang dikirim adalah asli.
3. Otentikasi (*authentication*)
   Otentikasi merupakan identitas yang dilakukan oleh masing-masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapat oleh suatu pihak dari pihak lain harus di identifikasi untuk memastikan keaslian dari informasi yang diterima. Identifikasi terhadap suatu informasi dapat berupa tanggal pembuatan informasi, isi informasi, waktu kirim dan hal-hal lainnya yang berhubungan dengan informasi tersebut.
4. Ketiadaan penyangkalan (*non-repudiation*)
   *Non-rupudiation*yaitu layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu mengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. Sebagai contoh, pengirim pesan anggota otoritas kepada penerima pesan untuk melakukan pembelian, namun kemudian ia menyangkal telah memberikan otoritas tersebut.

Sistem kriptografi secara umum terdiri dari lima bagian [5],yaitu sebagai berikut :

1. *Plaintext*
   Plaintext yaitu pesan atau data dalam bentuk aslinya yang dapat terbaca. *Plaintext* adalah masukan bagi algoritma enkripsi. Selanjutnya digunakan istilah teks asli sebagai padanan kata *plaintext*
2. *Secret Key*
   Secret Key yang juga merupakan masukan bagi algoritma enkripsi merupakan nilai yang bebas terhadap teks asli dan menentukan hasil keluaran algoritma enkripsi. Selanjutnya digunakan istilah kunci rahasia sebagai padanan kata *secret key*.
3. *Ciphertext*
   Ciphertext adalah keluaran algoritma enkripsi. *Ciphertext* dapat dianggap sebagai pesan dalam bentuk tersembunyi. Algoritma enkripsi yang baik akan menghasilkan *ciphertext* yang terlihat acak [6]. Selanjutnya digunakan istilah teks sandi sebagai padanan kata *ciphertext.*
4. Algoritma enkripsi
   Algoritma enkripsi memiliki 2 (dua) masukan teks asli dan kunci rahasia. Algoritma enkripsi melakukan transformasi terhadap teks asli sehingga menghasilkan teks sandi.
5. Algoritma dekripsi
   Algoritma dekripsi memiliki 2 (dua) masukan teks sandi dan kunci rahasia. Algoritma dekripsi memulihkan kembali teks sandi menjadi teks asli bila kunci rahasia yang dipakai algoritma dekripsi sama dengan kunci rahasia yang dipakai algoritma enkripsi.

Algoritma adalah urutan langkah-langkah logis untuk penyelesaian masalah yang disusun secara sistematis. Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut [7]. Secara umum algoritma kriptografi terbagi atas 2 (dua), yaitu algoritma kriptografi berdasarkan perkembangannya dan algoritma kriptografi berdasarkan kunci yang digunakan.

Berdasarkan perkembangannya algoritma kriptografi dibagi menjadi dua bagian [3], yaitu :

1. Algoritma Kriptografi Klasik
   Kriptografi Klasik) merupakan suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Teknik ini sudah digunakan beberapa abad yang lalu. Contoh algoritma kriptografi klasik adalah *caesar cipher, vigenere cipher, hill cipher, transposisi columnar* dan lain-lain.
   Kriptografi klasik memiliki beberapa kategori :
   a. Algoritma kriptografi klasik berbasis karakter.
   b. Menggunakan pena dan kertas saja, belum ada komputer.
   c. Termasuk ke dalam kunci simetri.

   Adapun teknik-teknik yang digunakan dalam kriptografi klasik (Donni Ariyus, 2008) adalah sebagai berikut :
   a. Teknik Subtitusi
      Substitusi merupakan penggantian setiap karakter dari teks asli dengan karakter lain. Terdapat empat istilah dari substitusi sandi, yaitu :
      1) *Monoalphabet*, yaitu setiap karakter teks sandi menggantikan salah satu karakter teks asli.
      2) *Polyalphabet*, yaitu setiap karakter teks sandi dapat mengganti lebih dari satu macam karakter teks asli.
      3) *Monograf*, yaitu satu enkripsi dilakukan terhadap satu karakter teks asli.
      4) *Polygraph*, yaitu satu enkripsi dilakukan terhadap lebih dari satu karakter teks asli.
   b. Teknik Transposisi
      Teknik transposisi adalah mengubah susunan huruf pada plainteks sehingga urutannya berubah. Plainteks yang dirubah susunan hurufnya seperti ini merupakan cipherteksnya. Nama lain untuk teknik ini adalah permutasi, karena *transpose* setiap huruf di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.
   c. Super Enkripsi

Super enkripsi merupakan suatu konsep dengan menggunakan kombinasi dari dua atau lebih teknik substitusi dan teknik transposisi untuk mendapatkan algoritma yang sulit dipecahkan. Banyak algoritma enkripsi modern yang menggunakan teknik ini sebagai dasar pembuatan algoritmanya.

2. Kriptografi Modern

Enkripsi kriptografi modern berbeda dengan enkripsi kriptografi klasik, karena enkripsi kriptografi modern sudah menggunakan komputer dalam pengoperasiannya yang berfungsi untuk mengamankan data baik yang ditransfer melalui jaringan komputer maupun yang tidak. Hal ini sangat berguna untuk melindungi privasi, integritas data, autentikasi dan anti penyangkalan. Contoh algoritma kriptografi modern adalah *Data Ecryption Standard* (DES), *Advance Encryption Standard* (AES), *International Data Encryption Algorithm* (IDEA), A5, RC4 dan lain-lain.

Berdasarkan kunci yang digunakan algoritma kriptografi dikelompokkan menjadi tiga ([3], yaitu :

1. Kunci Simetri

Kunci ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Kunci ini sudah ada sejak lebih dari 4000 tahun yang lalu. Kegiatan pengiriman pesan dengan menggunakan kunci ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsi pesan yang dikirim. Keamanan dari pesan yang menggunakan kunci simetri ini tergantung kuncinya. Apabila kunci tersebut diketahui oleh orang lain, maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan tersebut. Algoritma yang memakai kunci simetri di antaranya adalah :

a. *Data Encryption Standard* (DES)
b. *Vigenere Cipher*
c. *Affine Cipher*
d. *Digraph Cipher*
e. *Advance Encryption Standard* (AES)
f. *One Time Pad* (OTP)
g. Transposisi *Columnar*

2. Kunci Asimetri

Kunci asimetri sering juga disebut kunci publik, dengan arti kunci yang digunakan untuk melakukan enkripsi dan dekripsi adalah berbeda. Kunci asimetri dibagi menjadi dua bagian :

a. Kunci Umum (*public key*), yaitu kunci yang boleh semua orang tahu (dipublikasikan).
b. Kunci Pribadi (*private key*), yaitu kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci-kunci tersebut saling berhubungan antara satu dengan yang lain. Melalui kunci publik orang dapat mengenkripsi pesan tetapi tidak bisa mendekripsinya. Hanya orang yang memiliki kunci pribadi yang dapat mendekripsi pesan tersebut. Melalui kunci asimetris kita bisa melakukan pengiriman pesan dengan lebih aman daripada dengan kunci simetris.

Algoritma yang memakai kunci publik di antaranya adalah :

a. *Digital Signature Algorithm* (DSA)
b. RSA
c. *Diffie-Hellman*(DH)
d. Kriptografi *quantum* dan lain sebagainya.

3. *Hash function* (fungsi *hash*)

Fungsi hash sering disebut dengan fungsi hash satu arah (*one-way function*), *message digest*, *fingerprint*, fungsi kompresi dan *Message Authentication Code* (MAC). Hal ini merupakan suatu fungsi matematika yang mengambil input panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Fungsi *hash* biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda yang menandakan bahwa pesan tersebut benar-benar dari orang yang diinginkan.

2.2 Algoritma Digraph Cipher

Digraph cipher merupakan *caesar cipher* yang diterapkan pada pasangan huruf. Apabila dibandingkan dengan *caesar cipher* biasa dimana setiap huruf hanya memiliki kemungkinan untuk diganti

oleh 26 huruf alphabet, jumlah kemungkinan yang ditawarkan oleh *digraph cipher* memang jauh lebih banyak yaitu 676 kemungkinan untuk setiap pasangan huruf [8]. Agar proses enkripsi dan dekripsi lebih mudah dengan menggunakan algoritma ini, biasanya dibentuk sebuah tabel acuan yang berukuran 26 x 26 yang berisikan seluruh pasangan untuk setiap kombinasi pasangan huruf dalam alfabet.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	NG	OG	PG	QG	RG	SG	TG	UG	VG	WG	XG	YG	ZG	AG	BG	CG	DG	EG	FG	GG	HG	IG	JG	KG	LG	MG
B	NF	OF	PF	QF	RF	SF	TF	UF	VF	WF	XF	YF	ZF	AF	BF	CF	DF	EF	FF	GF	HF	IF	JF	KF	LF	MF
C	NE	OE	PE	QE	RE	SE	TE	UE	VE	WE	XE	YE	ZE	AE	BE	CE	DE	EE	FE	GE	HE	IE	JE	KE	LE	ME
D	ND	OD	PD	QD	RD	SD	TD	UD	VD	WD	XD	YD	ZD	AD	BD	CD	DD	ED	FD	GD	HD	ID	JD	KD	LD	MD
E	NC	OC	PC	QC	RC	SC	TC	UC	VC	WC	XC	YC	ZC	AC	BC	CC	DC	EC	FC	GC	HC	IC	JC	KC	LC	MC
F	NB	OB	PB	QB	RB	SB	TB	UB	VB	WB	XB	YB	ZB	AB	BB	CB	DB	EB	FB	GB	HB	IB	JB	KB	LB	MB
G	NA	OA	PA	QA	RA	SA	TA	UA	VA	WA	XA	YA	ZA	AA	BA	CA	DA	EA	FA	GA	HA	IA	JA	KA	LA	MA
H	NZ	OZ	PZ	QZ	RZ	SZ	TZ	UZ	VZ	WZ	XZ	YZ	ZZ	AZ	BZ	CZ	DZ	EZ	FZ	GZ	HZ	IZ	JZ	KZ	LZ	MZ
I	NY	OY	PY	QY	RY	SY	TY	UY	VY	WY	XY	YY	ZY	AY	BY	CY	DY	EY	FY	GY	HY	IY	JY	KY	LY	MY
J	NX	OX	PX	QX	RX	SX	TX	UX	VX	WX	XX	YX	ZX	AX	BX	CX	DX	EX	FX	GX	HX	IX	JX	KX	LX	MX
K	NW	OW	PW	QW	RW	SW	TW	UW	VW	WW	XW	YW	ZW	AW	BW	CW	DW	EW	FW	GW	HW	IW	JW	KW	LW	MW
L	NV	OV	PV	QV	RV	SV	TV	UV	VV	WV	XV	YV	ZV	AV	BV	CV	DV	EV	FV	GV	HV	IV	JV	KV	LV	MV
M	NU	OU	PU	QU	RU	SU	TU	UU	VU	WU	XU	YU	ZU	AU	BU	CU	DU	EU	FU	GU	HU	IU	JU	KU	LU	MU
N	NT	OT	PT	QT	RT	ST	TT	UT	VT	WT	XT	YT	ZT	AT	BT	CT	DT	ET	FT	GT	HT	IT	JT	KT	LT	MT
O	NS	OS	PS	QS	RS	SS	TS	US	VS	WS	XS	YS	ZS	AS	BS	CS	DS	ES	FS	GS	HS	IS	JS	KS	LS	MS
P	NR	OR	PR	QR	RR	SR	TR	UR	VR	WR	XR	YR	ZR	AR	BR	CR	DR	ER	FR	GR	HR	IR	JR	KR	LR	MR
Q	NQ	OQ	PQ	QQ	RQ	SQ	TQ	UQ	VQ	WQ	XQ	YQ	ZQ	AQ	BQ	CQ	DQ	EQ	FQ	GQ	HQ	IQ	JQ	KQ	LQ	MQ
R	NP	OP	PP	QP	RP	SP	TP	UP	VP	WP	XP	YP	ZP	AP	BP	CP	DP	EP	FP	GP	HP	IP	JP	KP	LP	MP
S	NO	OO	PO	QO	RO	SO	TO	UO	VO	WO	XO	YO	ZO	AO	BO	CO	DO	EO	FO	GO	HO	IO	JO	KO	LO	MO
T	NN	ON	PN	QN	RN	SN	TN	UN	VN	WN	XN	YN	ZN	AN	BN	CN	DN	EN	FN	GN	HN	IN	JN	KN	LN	MN
U	NM	OM	PM	QM	RM	SM	TM	UM	VM	WM	XM	YM	ZM	AM	BM	CM	DM	EM	FM	GM	HM	IM	JM	KM	LM	MM
V	NL	OL	PL	QL	RL	SL	TL	UL	VL	WL	XL	YL	ZL	AL	BL	CL	DL	EL	FL	GL	HL	IL	JL	KL	LL	ML
W	NK	OK	PK	QK	RK	SK	TK	UK	VK	WK	XK	YK	ZK	AK	BK	CK	DK	EK	FK	GK	HK	IK	JK	KK	LK	MK
X	NJ	OJ	PJ	QJ	RJ	SJ	TJ	UJ	VJ	WJ	XJ	YJ	ZJ	AJ	BJ	CJ	DJ	EJ	FJ	GJ	HJ	IJ	JJ	KJ	LJ	MJ
Y	NI	OI	PI	QI	RI	SI	TI	UI	VI	WI	XI	YI	ZI	AI	BI	CI	DI	EI	FI	GI	HI	II	JI	KI	LI	MI
Z	NH	OH	PH	QH	RH	SH	TH	UH	VH	WH	XH	YH	ZH	AH	BH	CH	DH	EH	FH	GH	HH	IH	JH	KH	LH	MH

Gambar 1. Tabel Acuan

Seperti halnya *playfair cipher*, pada *digraph cipher* juga melakukan operasi terhadap pesan yang akan dienkripsi. Hanya saja operasi yang dilakukan tidak sebanyak operasi yang dilakukan pada *playfair cipher*. Hal yang perlu dilakukan oleh *digraph cipher* hanyalah menuliskan pesan yang akan dienkripsi ke dalam bentuk pasangan huruf dan apabila jumlah huruf di dalamnya ganjil, maka ditambahkan huruf "z" di akhir.

PEMBAHASAN

3.1 Analisa Masalah

Analisa perancangan merupakan kegiatan yang dilakukan untuk menganalisis apa yang akan dirancang termasuk prosedur-prosedur yang dilakukan dan pemodelannya. Tahap analisa menguraikan langkah-langkah perancangan sistem yang akan dibuat serta implementasinya dalam bentuk contoh kasus.

Salah satu teknik pengamanan pesan yang umum digunakan adalah teknik kriptografi. Teknik kriptografi memiliki banyak algoritma untuk mengelabui para pembajak pesan. Teknik kriptografi dengan algoritma yang digunakan mampu merubah seluruh karakter pesan asli menjadi karakter-karakter yang justru tidak memiliki makna yang berkoresponden lagi dengan pesan aslinya. Hal ini lah yang disebut dengan penyandian pesan (proses enkripsi). Semakin rumit algoritma dan kunci yang digunakan, maka hasil sandi yang dihasilkan lebih sulit terpecahkan.

Algoritma kriptografi yang digunakan dalam penelitian ini adalah algoritma *digraph cipher* yang melakukan subtitusi karakter pesan asli berdasarkan tabel acuannya. Algoritma ini melakukan subtitusi karakter A-Z (26 karakter) dengan jumlah kombinasi 676 karakter. Hal ini terjadi karena setiap subtitusi karakter pada tabel acuan menghasilkan dua karakter.

Digraph cipher merupakan adaptasi terhadap teknik klasik lainnya yakni *caesar cipher*. Apabila dalam *caesar cipher* subsitusi dilakukan terhadap setiap huruf, maka *digraph cipher* melakukan subsitusi terhadap setiap pasangan huruf. Tabel acuan berukuran 26 x 26 dibentuk untuk mempermudah proses enkripsi dan dekripsi, dengan tujuan tabel-tabel ini menunjukkan daftar kombinasi pasangan huruf beserta subsitusi setiap karakter *plaintext* yang akan dienkripsi maupun didekripsi. Hasil analisa yang dilakukan pada tabel acuan *digraph cipher*, kombinasi pasangan huruf yang dihasilkan ada sebanyak 676 pasangan huruf, sehingga dapat dikatakan lebih luas dari kombinasi pasangan huruf *caesar cipher*. Seperti halnya *playfair cipher*, pada *digraph cipher* melakukan operasi terhadap pesan yang akan dienkripsi. Hanya saja

operasi yang dilakukan tidak sebanyak operasi yang dilakukan pada *playfair cipher*. Hal yang perlu dilakukan oleh *digraph cipher* hanyalah menuliskan pesan yang akan dienkripsi ke dalam bentuk pasangan huruf yang telah dikelompokkan. Jumlah karakter setiap kelompok adalah dua karakter dan apabila jumlah karakter dalam kelompok didapatkan ganjil, maka ditambahkan huruf "Z" di akhir.

Proses enkripsi dan dekripsi dengan *digraph cipher* diimplementasikan untuk mengenkripsi sebuah pesan yang dikirimkan oleh pengirim kepada penerima pesan. Pesan yang dikirimkan berjumlah 36 karakter abjad (18 kelompok) dan dienkripsi berdasarkan *digraph cipher*.

1. Siapkan tabel acuan *digraph cipher*
2. Siapkan *Plaintext*
   Plaintext = BESOK PAGI KITA KABUR LEWAT PINTU BELAKANG
3. Kelompokkan *plaintext* menjadi 2 karakter setiap kelompok dengan menghilangkan semua spasi.

BE	SO	KP	AG	IK	IT	AK	AB	UR	LE	WA	TP	IN	TU	BE	LA	KA	NG

4. Proses pengecekan jumlah karakter *plaintext*, apabila genap maka proses enkripsi dilanjutkan tetapi apabila jumlah karakter *plaintext* ganjil, maka pada bagian akhir karakter *plaintext* harus ditambahkan huruf z agar jumlahnya menjadi genap.
   Berdasarkan pengelompokkan karakter *plaintext* di atas, maka didapatkan bahwa jumlah karakternya genap, sehingga penambahan karakter "Z" tidak perlu dilakukan.
5. Proses enkripsi
   Mencari persilangan kolom dan baris karakter-karakter setiap kelompok plainteks. Karakter pertama setiap kelompok *plaintext* merujuk pada posisi kolom pada tabel acuan *digraph cipher* dan karakter kedua menunjukkan posisi baris pada tabel acuan *digraph cipher*.
   Kelompok karakter **BE** menjadi **OC**

	A	B	C	D	E	F	G	- - -	Z
A	NG	OG	PG	QG	RG	SG	TG	- - -	MG
B	NF	OF	PF	QF	RF	SF	TF	- - -	MF
C	NE	OE	PE	QE	RE	SE	TE	- - -	ME
D	ND	OD	PD	QD	RD	SD	TD	- - -	MD
E	NC	OC	PC	QC	RC	SC	TC	- - -	MC
F	NB	OB	PB	QB	RB	SB	TB	- - -	MB
--	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	--- ---
Z	N H	O H	P H	Q H	R H	S H	T H	- - -	M H

Kelompok karakter **SO** menjadi **FS**

	A	B	C	- - -	P	Q	R	S	- - -	Z
A	N G	O G	P G	- - -	C G	D G	E G	F G	- - -	M G
B	N F	O F	P F	- - -	C F	D F	E F	F F	- - -	M F
C	N E	O E	P E	- - -	C E	D E	E E	F E	- - -	M E
D	N D	O D	P D	- - -	C D	D D	E D	F D	- - -	M D
M	N U	O U	P U	- - -	C U	D U	E U	F U	- - -	M C
N	N T	O T	P T	- - -	C T	D T	E T	F T	- - -	M B
O	N S	O S	P S	- - -	C S	D S	E S	F S	- - -	M A
--	-- --	-- --	-- -	- - -	-- --	-- --	-- --	-- --	-- --	-- --
Z	N H	O H	P H	- - -	C H	D H	E H	F H	-- --	M H

Kelompok karakter **KP** menjadi **XR**

	A	B	C	D	E	F	G	H	I	J	K	- - -	Z

A	N	G	O	G	P	G	Q	G	R	G	S	G	T	G	U	G	V	G	W	G	X	G	-	-	-	M	G
B	N	F	O	F	P	F	Q	F	R	F	S	F	T	F	U	F	V	F	W	F	X	F	-	-	-	M	F
C	N	E	O	E	P	E	Q	E	R	E	S	E	T	E	U	E	V	E	W	E	X	E	-	-	-	M	E
D	N	D	O	D	P	D	Q	D	R	D	S	D	T	D	U	D	V	D	W	D	X	D	-	-	-	M	D
E	N	C	O	C	P	C	Q	C	R	C	S	C	T	C	U	C	V	C	W	C	X	C	-	-	-	M	C
F	N	B	O	B	P	B	Q	B	R	B	S	B	T	B	U	B	V	B	W	B	X	B	-	-	-	M	B
G	N	A	O	A	P	A	Q	A	R	A	S	A	T	A	U	A	V	A	W	A	X	A	-	-	-	M	A
H	N	Z	O	Z	P	Z	Q	Z	R	Z	S	Z	T	Z	U	Z	V	Z	W	Z	X	Z	-	-	-	M	Z
--	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
P	N	R	O	R	P	R	Q	R	R	R	S	R	T	R	U	R	V	R	W	R	X	R	-	-	-	M	X
--	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Z	N	H	O	H	P	H	Q	H	R	H	S	H	T	H	U	H	V	H	W	H	X	H	-	-	-	M	H

Kelompok karakter **AG** menjadi **NA**

	A		B		C		- - -		Z	
A	N	G	O	G	P	G	-	-	-	M	G
B	N	F	O	F	P	F	-	-	-	M	F
C	N	E	O	E	P	E	-	-	-	M	E
D	N	D	O	D	P	D	-	-	-	M	D
E	N	C	O	C	P	C	-	-	-	M	C
F	N	B	O	B	P	B	-	-	-	M	B
G	N	A	O	A	P	A	-	-	-	M	A
--	-	-	-	-	-	-	-	-	-	-	-
Z	N	H	O	H	P	H	-	-	-	M	H

Kelompok karakter **IK** menjadi **VW**

	A		B		C		D		E		F		G		H		I				Z	
A	N	G	O	G	P	G	Q	G	R	G	S	G	T	G	U	G	V	G	-	-	-	M	G
B	N	F	O	F	P	F	Q	F	R	F	S	F	T	F	U	F	V	F	-	-	-	M	F
C	N	E	O	E	P	E	Q	E	R	E	S	E	T	E	U	E	V	E	-	-	-	M	E
D	N	D	O	D	P	D	Q	D	R	D	S	D	T	D	U	D	V	D	-	-	-	M	D
E	N	C	O	C	P	C	Q	C	R	C	S	C	T	C	U	C	V	C	-	-	-	M	C
F	N	B	O	B	P	B	Q	B	R	B	S	B	T	B	U	B	V	B	-	-	-	M	B
G	N	A	O	A	P	A	Q	A	R	A	S	A	T	A	U	A	V	A	-	-	-	M	A
H	N	Z	O	Z	P	Z	Q	Z	R	Z	S	Z	T	Z	U	Z	V	Z	-	-	-	M	Z
I	N	Y	O	Y	P	Y	Q	Y	R	Y	S	Y	T	Y	U	Y	V	Y	-	-	-	M	Y
J	N	X	O	X	P	X	Q	X	R	X	S	X	T	X	U	X	V	X	-	-	-	M	X
K	N	W	O	W	P	W	Q	W	R	W	S	W	T	W	U	W	V	W	-	-	-	M	W
---	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Z	N	H	O	H	P	H	Q	H	R	H	S	H	T	H	U	H	V	H	-	-	-	M	H

Lakukan hal yang sama untuk mencari *ciphertext* kelompok *plaintext* yang lainnya hingga seluruh kelompok *plaintext*.

6. Hasil proses enkripsi

Plaintext :

BE	SO	KP	AG	IK	IT	AK	AB	UR	LE	WA	TP	IN	TU	BE	LA	KA	NG

Ciphertext :

OC	FS	XR	NA	VW	VN	NW	NF	HP	YC	JG	GR	VT	GM	OC	YG	XG	AA

atau :

Plaintext :

BESOK PAGI KITA KABUR LEWAT PINTU BELAKANG

Ciphertext :

OCFSX RNAV WVNN WNFHP YCJGG RVTGM OCYGXGAA

Proses dekripsi sama seperti pada proses enkripsi, hanya saja sumber karakter-karakter yang dicocokkan berasal dari *ciphertext* sebelumnya.

1. Siapkan *ciphertext* dan tabel acuan *digraph cipher*

   Plaintext :

   OCFSX RNAV WVNN WNFHP YCJGG RVTGM OCYGXGAA
2. Hilangkan semua *space* (karakter kosong)

   OCFSXRNAVWVNNWNFHPYCJGGRVTGMOCYGXGAA
3. Kelompokkan karakter-karakter *ciphertext* sebanyak dua karakter setiap kelompok

OC	FS	XR	NA	VW	VN	NW	NF	HP	YC	JG	GR	VT	GM	OC	YG	XG	AA

4. Proses dekripsi
   a. Huruf pertama *ciphertext* mengacu kepada kolom yang merepresentasikan huruf tersebut.
   b. Huruf kedua *ciphertext* digunakan sebagai acuan baris yang yang merepresentasikan huruf tersebut.

   Kelompok karakter **OC** menjadi **BE**

	A	B	C	D	E	F	G	H	I	J	K	L	---	O	---	Z
A	NG	OG	PG	QG	RG	SG	TG	UG	VG	WG	XG	YG	---	BG	---	MG
B	NF	OF	PF	QF	RF	SF	TF	UF	VF	WF	XF	YF	---	BF	---	MF
C	NE	OE	PE	QE	RE	SE	TE	UE	VE	WE	XE	YE	---	BE	---	ME
--	---	---	---	---	---	---	---	---	---	---	---	---	---		---	---
Z	N H	O H	P H	Q H	R H	S H	T H	U H	V H	WW	XH	YH	---	BH	---	MH

Kelompok karakter **FS** menjadi **SO**

	A	B	C	D	E	F	---	Z
A	N G	O G	P G	Q G	R G	S G	---	M G
B	N F	O F	P F	Q F	R F	S F	---	M F
C	N E	O E	P E	Q E	R E	S E	---	M E
D	N D	O D	P D	Q D	R D	S D	---	M D
E	N C	O C	P C	Q C	R C	S C	---	M C
F	N B	O B	P B	Q B	R B	S B	---	M B
G	N A	O A	P A	Q A	R A	S A	---	M A
--	---	---	---	---	---	---	---	---
S	N O	O O	P O	Q O	R O	S O	---	M O
--	---	---	---	---	---	---	---	---
Z	N H	O H	P H	Q H	R H	S H	---	M H

Kelompok karakter **XR** menjadi **KP**

	A	B	C	D	E	---	X	Y	Z
A	NG	OG	PG	QG	RG	---	KG	LG	MG
B	NF	OF	PF	QF	RF	---	KF	LF	MF
C	NE	OE	PE	QE	RE	---	KE	LE	ME
D	ND	OD	PD	QD	RD	---	KD	LD	MD
E	NC	OC	PC	QC	RC	---	KC	LC	MC
F	NB	OB	PB	QB	RB	---	KB	LB	MB
G	NA	OA	PA	QA	RA	---	KA	LA	MA
H	NZ	OZ	PZ	QZ	RZ	---	KZ	LZ	MZ

I	NY	OY	PY	QY	RY	- - -	KY	LY	MY
--	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -
P	NR	OR	PR	QR	RR	- - -	KR	LR	MR
Q	NQ	OQ	PQ	QQ	RQ	- - -	KQ	LQ	MQ
R	NP	OP	PP	QP	RP	- - -	KP	LP	MP
--	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -
Z	NH	OH	PH	QH	RH	- - -	KH	LH	MH

Kelompok karakter **NA** menjadi **AG**

	A	B	C	D	E	- - -	N	- - -	Z
A	N G	O G	P G	Q G	R G	- - -	AG	- - -	M G
B	N F	O F	P F	Q F	R F	- - -	AF	- - -	M F
C	N E	O E	P E	Q E	R E	- - -	AE	- - -	M E
D	N D	O D	P D	Q D	R D	- - -	AD	- - -	M D
E	N C	O C	P C	Q C	R C	- - -	AC	- - -	M C
F	N B	O B	P B	Q B	R B	- - -	AB	- - -	M B
--	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -
Z	N H	O H	P H	Q H	R H	- - -	A H	- - -	M H

Kelompok karakter **VW** menjadi **IK**

	A	B	C	D	E	- - -	V	W	X	Y	Z
A	NG	OG	PG	QG	RG	- - -	IG	JG	KG	LG	MG
B	NF	OF	PF	QF	RF	- - -	IF	JF	KF	LF	MF
C	NE	OE	PE	QE	RE	- - -	IE	JE	KE	LE	ME
D	ND	OD	PD	QD	RD	- - -	ID	JD	KD	LD	MD
E	NC	OC	PC	QC	RC	- - -	IC	JC	KC	LC	MC
---	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -
W	NK	OK	PK	QK	RK	- - -	IK	JK	KK	LK	MK
X	NJ	OJ	PJ	QJ	RJ	- - -	IJ	JJ	KJ	LJ	MJ
Y	NI	OI	PI	QI	RI	- - -	II	JI	KI	LI	MI
Z	NH	OH	PH	QH	RH	- - -	IH	JH	KH	LH	MH

Kelompok karakter **VN** menjadi **IT**

	A	B	C	D	E	- - -	V	W	X	Y	Z
A	NG	OG	PG	QG	RG	- - -	IG	JG	KG	LG	MG
B	NF	OF	PF	QF	RF	- - -	IF	JF	KF	LF	MF
C	NE	OE	PE	QE	RE	- - -	IE	JE	KE	LE	ME
D	ND	OD	PD	QD	RD	- - -	ID	JD	KD	LD	MD
E	NC	OC	PC	QC	RC	- - -	IC	JC	KC	LC	MC
--	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -
N	NT	OT	PT	QT	RT	- - -	IT	JT	KT	LT	MT
--	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -	- - -
Z	NH	OH	PH	QH	RH	- - -	IH	JH	KH	LH	MH

Karakter untuk kelompok yang lain dicari dengan cara yang sama seperti di atas, sehingga hasil akhir (*plaintext*) yang didapatkan adalah :
ciphertext : **BESOK PAGI KITA KABUR LEWAT PINTU BELAKANG**

KESIMPULAN

Adapun kesimpulan dalam penelitian ini adalah sebagai berikut :

1. Prosedur enkripsi dan dekripsi pesan teks dengan algoritma *Digraph Cipher* dilakukan dengan menuliskan pesan yang akan dienkripsikan ke dalam bentuk pasangan huruf dan apabila jumlah huruf di dalamnnya ganjil, maka ditambahkan huruf "Z" di akhir.

2. Proses enkripsi dan dekripsi dilakukan secara sederhana yaitu melakukan substitusi terhadap pasangan huruf plainteks dengan pasangan yang sesuai dengan tabel *Digraph Cipher* yang ada.
3. Perancangan aplikai penyandian pesan teks berdasarkan algoritma *Digraph Cipher* dilakukan dengan menggunakan bahasa pemograman *Visual basic.Net 2008* dapat memudahkan proses penyandian pesan teks. Aplikasi yang dibangun terdiri dari *form login*, *form* menu utama, *form* enkripsi dan dekripsi, *form* tabel *digraph cipher* dan *form* info.

DAFTAR PUSTAKA

[1] D. Ariyus, "Kriptografi keamanan data dan komunikasi," *Yogyakarta Graha Ilmu*, 2006.
[2] R. Munir, "Algoritma Knapsack," pp. 0–18, 2004.
[3] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.
[4] B. Silaban and T. Limbong, "Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction," *Media Inf. Anal. dan Sist.*, vol. 2, no. 2, pp. 14–20, 2017.
[5] T. Arianti and B. Nadeak, "Perancangan Aplikasi Pembelajaran Kriptografi Algoritma GOST dengan Menggunakan Metode Computer Based Instruction," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 1, no. 1, pp. 40–46, 2019.
[6] T. Limbong, "Pengujian Kriptografi Klasik Caesar Chipper Menggunakan Matlab," *no. Sept.*, vol. 2017, 2015.
[7] H. Sahara, "Implementasi Pengamanan Pesan Chatting menggunakan Metode Vigenere Cipher dan Cipher Block Chainning," *MEANS (Media Inf. Anal. dan Sist.*, vol. 3, no. 2, pp. 173–178, 2018.
[8] R. Santi, "Implementasi Algoritma Enkripsi Playfair pada File Teks," *None*, vol. 15, no. 1, p. 246766, 2010.