Jurnal Riset Komputer (JURIKOM), Vol. 6, No. 5, Oktober 2019
ISSN 2407-389X (Media Cetak)
Hal: 523-530

Pengamanan Pesan Teks E-Mail Menggunakan Metode Algoritma Bifid Dan Feedback Cipher

Siska Wulandari

Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338 Medan, Indonesia

Abstrak

Salah satu aplikasi internet yang banyak digunakan adalah pengiriman pesan secara elektronik, yang disebut e-mail. Seiring dengan berjalannya waktu, pengiriman pesan melalui e-mail menjadi salah satu hal yang penting. Namun ada beberapa ancaman yang tidak tahu pada saat menggunakan e-mail seperti penyadapan isi e-mail, merubah isi e-mail oleh orang yang tidak berkepentingan dan menjadikan e-mail itu tidak asli lagi. Teknik pengamanan pesan teks atau data dikenal dengan nama ilmu kriptografi. Dalam kriptografi terdapat beberapa metode yang cukup penting dalam pengamanan data,untuk menjaga kerahasiaan data salah satunya adalah enkripsi (pengkodean). Dekripsi (teks asli) salah satu algoritma krptografi yaitu bifid cipher dan feedbak cipher. Bifid cipher pertama kali ditemukan oleh Felix Delastelle pada tahun 1901. Bifid cioher mengenkripsikan dengan mengacak posisi baris dan kolom huruf pada pesan yang sesuai dengan papan kunci berbentuk bujur sangkar 5X5 sedangkan Metode Cipher Feedback menggunakan sistem Shift Register, dimana yang diproses terlebih dahulu adalah Initialization Vector dalam algoritma Enkripsi dengan Kunci. Setelah diproses, bit yang dihasilkan akan melalui proses seleksi bit, biasanya bit-bit yang paling kiri, untuk selanjutnya dienkripsi dengan Plaintext untuk menghasilkan Ciphertext. Dengan menerapkan kombinasi dari kedua algoritma yaitu algoritma bifid cipher dan feedback cipher diharapkan pesan yang dikirim dalam e-mail akan dikodekan sehingga pihak yang tidak berkepentingan tidak mengetahui makna pesan yang dikirim. Serta dapat menjaga keaslian dari pesan yang dikirim

Kata Kunci: email, keamanan, Kriptografi, Rahasia, dunia maya.

Abstract

One of the most widely used internet applications is electronic message sending, called e-mail. As time goes by, sending messages via e-mail becomes one of the important things. But there are some threats that do not know when using e-mails such as eavesdropping on e-mail contents, changing e-mail contents by unauthorized people and making e-mails no longer authentic. The technique of securing text messages or data is known as cryptography. In cryptography there are several methods that are quite important in securing data, to maintain data confidentiality one of which is encryption (coding). Decryption (original text) of one of the cryptographic algorithms, namely bifid cipher and feedbak cipher. Bifid cipher was first discovered by Felix Delastelle in 1901. Bifid cioher encrypts by randomizing the position of the row and column of letters in the message that corresponds to the 5X5 square key board while the Cipher Feedback Method uses the Shift Register system, which is processed first is the Initialization Vector in the Encryption with Key algorithm. After processing, the resulting bits will go through a bit selection process, usually the leftmost bits, then encrypted with Plaintext to produce the Ciphertext. By applying a combination of the two algorithms, the bifid cipher algorithm and the feedback cipher, it is expected that the message sent in the e-mail will be coded so that unauthorized parties do not know the meaning of the message being sent. And can maintain the authenticity of the messages sent

Keywords: email, security, Cryptography, Confidential, cyberspace.

1. PENDAHULUAN

Salah satu aplikasi internet yang banyak digunakan adalah pengiriman pesan secara elektronik, yang disebut e-mail. E-mail digunakan sejak awal terbentuknya internet pada tahun 1969 dan e-mail merupakan aplikasi yang ada pada saat awal terbentuknya internet. Penggunaan e-mail juga sudah semakin pesat, e-mail digunakan untuk mengirimkan suatu informasi yang cepat dan efisien. Tak jarang orang menyimpan ataupun mengirim berbagai data penting pada email, seperti informasi akun-akun, nomor rekening relasi, dan masih banyak lainnya. Hal ini di-karenakan orang-orang takut lupa mengenai informasi penting tersebut dan dipilihlah email sebagai tempat penyimpanannya.

Seiring dengan berjalannya waktu, pengiriman pesan melalui e-mail menjadi salah satu hal yang penting. Namun ada beberapa ancaman yang pengguna tidak tahu pada saat menggunakan e-mail seperti penyadapan isi e-mail, merubah isi e-mail oleh orang yang tidak berkepentingan dan menjadikan e-mail itu tidak asli lagi. Karena adanya ancaman keamanan pada e-mail,

Oleh karenanya dibutuhkan suatu proses penyandian atau pengkodean pesan sebelum dilakukan proses pengiriman. Sehingga pesan yang dikirim terjaga kerahasiaannya dan tidak dapat dengan mudah diubah untuk menjaga integritas pesan tersebut.

Bifid cipher pertama kali ditemukan oleh Felix Delastelle pada tahun 1901 yang sampai saat ini mesih berperan sebagai salah satu algoritma penyandian sederhana yang biasa dilakukan hanya dengan menggunakan pensil dan kertas yang cukup aman karena prinsip diffusion yang terkandung didalamnya sedangkan metode Cipher Feedback menggunakan sistem Shift Register, dimana yang diproses terlebih dahulu adalah Initialization Vector dalam algoritma Enkripsi dengan Kunci. Setelah diproses, bit yang dihasilkan akan melalui proses seleksi bit, biasanya bit-bit yang paling kiri, untuk selanjutnya dienkripsi dengan Plaintext untuk menghasilkan Ciphertext. Bit hasil seleksi yang digunakan tergantung besarnya bit blok plaintext yang diinput.

2. LANDASAN TEORI

2.1 Pesan Teks

Berkomunikasi satu sama lain merupakan sifat dasar manusia sejak ada dimuka bumi ini. Cara manusia berkomunikasi dari zaman dulu sampai sekarang terus mengalami perkembangan. Salah satu sarana komunikasi manusia adalah tulisan sebuah tulisan berfungsi untuk menyampaikan pesan kepada pembacanya. Pesan itu sendiri merupakan suatu informasi yang dapat dibaca dan dimengerti maknanya [3].
Pesan terbagi menjadi beberapa bagian seperti :

1. Pesan untuk orang banyak
   Suatu informasi yang ditujukan untuk orang banyak tidak mengandung suatu rahasia
2. Pesan untuk suatu kelompok
   Suatu informasi untuk beberapa orang (kelompok), terkadang bersifat rahasia.
3. Pesan hanya untuk satu orang
   Pesan hanya untuk satu orang sering kali bersifat rahasia
4. Pesan rahasia
   Pesan yang tidak boleh diketahui oleh orang lain selain yang berhak.

Dengan berkembangnya cara pengiriman pesan, berkembang pula cara menyembunyikan pesan dan bagaimana agar orang lain tidak mengetahui isi pesan walau pesan tersebut ditemukan. Disinilah lahir suatu ilmu baru yang disebut dengan kriptografi [3].

2.2 E-mail (Surat Elektronik)

E-mail merupakan sebuah fitur yang kemungkinan besar pasti digunakan oleh semua orang. E-mail adalah surat elektronik, yang memungkinkan semua orang saling berkirim pesan via jaringan internet.keunggulan e-mail adalah mudah dan bisa diakses dimanapun juga [4].

2.3 Keamanan

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian bagi para perancang dan pengelolah sistem informasi. Masalah keamanan sering berada pada urutan setelah tampilan [3]. Saat ini informasi sudah menjadi komoditas yang sangat penting. Kemajuan sistem informasi memberikan banyak keuntungan bagi manusia. Meski begitu aspek negatifnya juga banyak seperti, kejahatan komputer yang mencakup pencurian, penipuan, pemerasan, kompetisi dan lain sebagainya.

2.4 Kriptografi

Kriptografi berasal dari Bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim kesuatu tempat ke tempat lain Kriptoggrafi berfungsi agar data yang dikirim aman dari gangguan orang yang tidak bertanggung jawab, yang disembunyikan menggunakan algoritma kriptografi [3].

2.5 Algoritma Bifid Cipher

Bifid cipher pertama kali ditemukan oleh Felix Delastelle pada tahun 1901 yang sampai saat ini mesih berperan sebagai salah satu algoritma penyandian sederhana yang biasa dilakukan hanya dengan menggunakan pensil dan kertas yang cukup aman karena prinsip diffusion yang terkandung didalamnya. Algoritma ini merupakan salah satu algoritma yang juga menggunakan prinsip dasar playfair cipher dimana pesan akan dienkripsikan dengan mengacak posisi baris dan kolom huruf pada pesan yang sesuai dengan papan kunci yang juga berbentuk bujur sangkar 5 X 5 sama seperti yang diterapkan pada playfair cipher hanya saja tidak ada perluasan papan kunci yang dilakukan pada Bifid cipher ini [1].
Setiap sel pada bujur sangkar diisi dengan huruf yang berbeda secara acak, namun untuk mempermudah mengingat kunci, biasanya digunakan kunci berupa kata ataupun kalimat yang membentuk sebuah arti yang kemudian dihilangkan huruf-huruf berulangnya dan kemudian diisikan pada sel-sel bujur sangkar secara berurut dari kiri ke kanan, dari atas kebawah. Jika panjang kunci tidak mencapai 25 huruf, maka sel pada bujur sangkar yang tersisa akan diisi dengan huruf-huruf sisa pada alfabet yang belum tertulis secara berurut.

2.7 Algoritma Feedback Cipher

Metode ini dilakukan untuk melakukan enkripsi pada aliran kode. Mode ini tidak memerlukan tambahan bit karna jumlah panjang blok sama dengan jumlah panjang teks aslinya. Mode ini bekerja pada mode real time. Motode CFB ini memiliki masukan 8bit yang diproses setiap enkripsi dan teks-teks sebelumnya digunakan sebagai masukan dari algoritma enkripsi. Untuk menghasilkan keluaran yang acak. Output diambil dari 8bit paling kiri untuk kemudian dilakukan operasi XOR dengan teks asli dengan panjang 8 bit sehingga menghasilkan teks kode berikutnya. Input dari enkripsi terdiri dari 8 bit yang digeser ke kiri sebanyak 8bit. Karena terjadi penggeseran maka kekosongan yang ada akan diiisi oleh kode sebelumnya. Input dari enkripsi pada awalnya adalah IV (Initial Value). Jika panjang IV pada register geser 64bit maka keluaran enkripsinya akan memiliki panjang yang sama yaitu 64bit [3].

.

3. ANALISA DAN PEMBAHASAN

Adanya perkembangan teknologi yang sangat pesat pada masa sekarang membuat manusia dapat dengan mudah bertukar in*form*asi pada suatu individu ataupun organisasi sesuai dengan kebutuhan, menggunakan media *internet*. Media *internet* memungkinkan pengguna untuk berkomunikasi secara *real time* namun tanpa jaminan untuk berkomunikasi, pertukaran in*form*asi, penggunaan *E-Mail* sebagai media pengiriman dan penyimpanan pesan melalui media elektronik sudah banyak dilakukan. Terkadang pengiriman dan penyimpanan pesan melalui media elektronik perlu dirahasiakan untuk menjamin keamanan dan keutuhan data Oleh sebab itu maka dibutuhkan sebuah metode penyandian pesan. Ilmu sekaligus seni untuk menjaga keamanan pesan disebut kriptografi.

Metode enkripsi dan dekripsi in*form*asi yang bersifat rahasia sangat diperlukan sehingga jangan sampai diketahui oleh orang lain yang tidak berhak. In*form*asi ini bisa berupa *E-Mail* yang sifatnya rahasia atau pengiriman dokumen rahasia perusahaan melalui Internet.

Dari beberapa kasus yang ditemui pada keamanan pesan teks, dimana masih banyak terjadinya kegagalan pada keamana pesan dikarenakan kurang rumitnya penerapan metode keamana pada sistem keamanan pesan. Jika sistem keamana pesan di terapkan kombinasi dari beberapa metode keamanan pesan, maka akan meminimalisir dan mencegah terjadinya pembobolan pesan.

Dalam penelitian ini penulis membangun algoritma kriptogtafi (yang merupakan kombinasi algoritma kriptografi Bifid *Cipher* dan Feedback *Cipher*), terkait hal tersebut maka penulis nantinya akan menganalisa langkah-langkah kerja algoritma kriptografi Bifid *Cipher* dan Feedback *Cipher* tersebut, sehingga nantinya algoritma kriptografi yang penulis bangun akan memiliki tingkat kesulitan yang lebih tinggi untuk dipecahkan dibandingkan algoritma kriptografi Bifid *Cipher* dan Feedback *Cipher* dioperasikan secara tersendiri. Sebagai penjelasan, proses enkripsi dan dekripsi pada dapat dilihat dibawah ini.

3.1 Enkripsi Bifid *Cipher*

Kunci yang digunakan merupakan 25 huruf alfabet yang disusun secara acak kedalam sebuah bujur sangkar yang dibuat berukuran 5 X 5 dengan menghilangkan huruf J **.** setiap sel pada bujur sangkar diisi dengan huruf yang berbeda secara acak, namun untuk mempermudah mengingat kunci, biasanya digunakan kunci berupa kata ataupun kalimat yang membentuk sebuah arti yang kemudian dihilangkan huruf-huruf berulangnya dan kemudian diisikan pada sel-sel bujur sangkar secara berurut dari kiri ke kanan, dari atas kebawah. Jika panjang kunci tidak mencapai 25 huruf, maka sel pada bujur sangkar yang tersisa akan diisi dengan huruf-huruf sisa pada alfabet yang belum tertulis secara berurut. kunci yang digunakan adalah ” Wulan”

Maka dengan menghilangkan huruf-huruf berulang, kalimat tersebut akan menjadi ”Wulan ” Dengan memasukan huruf-huruf tersebut kedalam sel-sel bujur sangkar dan mengisi sel-sel yang belum terisi dengan huruf-huruf alfabet yang belum tertulis terkecuali hujur *J* maka akan diperoleh kunci yang akan digunakan dalam malakukan penyandian dengan menggunakan algoritma bifid adalah sebagai berikut

Tabel 1. Tabel kunci bifid *cipher*

	1	2	3	4	5
1	S	I	C	A	W
2	U	L	N	D	R
3	B	E	F	G	H
4	K	M	O	P	Q
5	T	V	X	Y	X

Awal proses enkripsi dilakukan dengan mengidentifikasi posisi tiap huruf berdasarkan baris dan kolomnya. Sama seperti aturan pada playfair, huruf *J* pada plainteks terlebih dahulu diubah menjadi huruf *I* . Untuk contoh kasus dengan plainteks ”siscawulandari” akan diperoleh hasil identifikasi sebagai berikut

Kunci : S i s c a w u l a n d a r i
Plainteks : S a n d i p o r t a l m d r s i s c a
Baris : 1 1 2 2 1 4 4 2 5 1 2 4 2 2 1 1 1 1 1
Kolom : 5 4 3 4 2 4 3 5 1 4 2 2 4 5 5 2 5 3 4

Kemudian plainteks tersebut akan dienkripsikan dengan mengacak kordinat posisi dan menjadikannya kordinat posisi yang baru dengan aturan tertentu. Dalam hal ini aturan yang digunakan adalah dengan menjadikan kordinat baris dan kolom menjadi satu baris karakter angka dan kemudian membuatnya menjadi bigram (dipisahkan dua-dua) untuk dijadikan kordinat baru yang isi sel nya merupakan hasil enkripsi yang dilakukan. Proses enkripsi secara sistematis akan diperlihatkan sebagai berikut

Kordianat baris dan kolom dijadikan satu baris karakter angka
1122144251242211111543424351422455253 4
Kemudian pisahkan menjadi bigram yang akan membentuk kordinat baru baris dan kolom
11 22 14 42 51 24 22 11 11 15 43 42 43 51 42 24 55 25 34
Maka *cipher*teks adalah isi dari sel dengan kordinat baru yang terbentuk

Baris : 1 2 1 4 5 2 2 1 1 1 4 4 4 5 4 2 5 2 3
Kolom : 1 2 4 2 1 4 2 1 1 5 3 2 3 1 2 4 5 5 4
*Cipher*teks : S L A M T D L S S W O M O T M D X R G

Maka hasil enkripsi dengan menggunakan metode bifid *cipher* adalah sebagai berikut
Plainteks : S a n d i p o r t a l m d r s i s c a
*Cipher*teks : S L A M T D L S S W O M O T M D X R G

Setelah didapat hasil enkripsi dari bifid *cipher* maka *cipher*teks tersebut menjadi plainteks pada operasi selanjutnya yaitu feedback *cipher*.

3.2 Enkripsi Feedback *Cipher*

Plainteks = SLAMTDLSSWOMOTMDXRG
Kunci = Sisca Wulandari
IV = C_0 = X= 01011000
Ubah teks plainteks dan kunci kedalam bentuk biner

Plainteks=	S	L	A	M	T	D	L
	01010011	01001100	01000001	01001101	01010100	01000100	01001100
	S	S	W	O	M	O	T
	01010011	01010011	01010111	01001111	01001101	01001111	01010100
	M	D	X	R	G		
	01001101	01000100	01011000	01010010	01000111		

Kunci=	S	i	s	c	a		W
	01010011	01101001	01110011	01100011	01100001	00100000	01010111
	u	l	a	n	d	a	r
	01110101	01101100	01100001	01101110	01100100	01100001	01110010

Kemudian lakukan operasi dengan *form*ula
$C_i = P_i \oplus E_k (C_{i-1})$

C_1=

C_0	0	1	0	1	1	0	0	0	
K	0	1	0	1	0	0	1	1	⊕
	0	0	0	0	1	0	1	1	
P_1	0	1	0	1	0	0	1	1	⊕
C_1	0	1	0	1	1	0	0	0	Shif register 1 bit => 10110000

Setelah didapat nilai biner dari C_1, maka konversikan biner tersebut menjadi karakter C_1= 10110000 = °

C_2=

C_1	1	0	1	1	0	0	0	0	
K_2	0	1	1	0	1	0	0	1	⊕
	1	1	0	1	1	0	0	1	
P_2	0	1	0	0	1	1	0	0	⊕
C_2	1	0	0	1	0	1	0	1	Shif register 1 bit => 00101011

Setelah didapat nilai biner dari C_2, maka konversikan biner tersebut menjadi karakter C_2= 00101011 = +

C_3=

C_2	0	0	1	0	1	0	1	1	
K_3	0	1	1	0	1	1	0	0	⊕
	1	1	0	0	0	0	1	1	
P_3	0	1	0	0	0	0	0	1	⊕
C_3	0	0	0	0	0	1	1	0	Shif register 1 bit => 00001100

Setelah didapat nilai biner dari C_3, maka konversikan biner tersebut menjadi karakter C_3= 00001100=

C_4=

C_3	0	0	0	0	1	1	0	0	
K_4	0	1	1	0	0	0	1	1	⊕

	0	1	1	0	1	1	1	1	
P_4	0	1	0	0	1	1	0	1	⊕
C_4									Shif register 1 bit => 01000100
	0	0	1	0	0	0	1	0	

Setelah didapat nilai biner dari C_4, maka konversikan biner tersebut menjadi karakter C_4= 01000100= D

C_5=

C_4	0	1	0	0	0	1	0	0	
K_5	0	1	1	0	0	0	0	1	⊕
	0	0	1	0	0	1	0	1	
P_5	0	1	0	1	0	1	0	0	⊕
C_5									Shif register 1 bit => 11100010
	0	1	1	1	0	0	0	1	

Setelah didapat nilai biner dari C_5, maka konversikan biner tersebut menjadi karakter C_5= 11100010 = â

Lakukan proses yang sama sampai didapat nilai biner dari C_{19}, maka konversikan biner tersebut menjadi karakter C_{19}= 10110100 = ‘

Setelah dilakukan prosesvenkripsi kombinasi *Bifid Cipher* dan *Cipher Feedback* maka *cipher* teks yang dihasilkan adalah °+ D â , V À Ã Õ ÷ £ { ¬ | ‘

3.3 Dekripsi Algoritma *Feedback Cipher*

*cipher*teks = °+ D â , V À Ã Õ ÷ £ { ¬ | ‘

Kunci = Sisca Wulandari

IV = C_0 = X= 01011000

Ubah teks plainteks dan kunci kedalam bentuk biner

10110000	00101011	00001100	01000100	11100010	00001101	00101100
°	+		D	â		,
00010100	01010110	11000000	11000011	11010101	11110111	10100011
	V	À	Ã	Õ	÷	£
01111011	10101100	00001111	01111100	10110100		
{	¬		|	´		

Kunci=

S	i	s	c	a		W
01010011	01101001	01110011	01100011	01100001	00100000	01010111
u	l	a	n	d	a	r
01110101	01101100	01100001	01101110	01100100	01100001	01110010

Kemudian lakukan operasi dengan *form*ula

$P_i = C_i \oplus E_k (P_{i-1})$

Shif register 1 bit biner *cipherteks* => 10110000 => 01011000

P_1=

C_0	0	1	0	1	1	0	0	0	
K	0	1	0	1	0	0	1	1	⊕
	0	0	0	0	1	0	1	1	
C_1	0	1	0	1	1	0	0	0	⊕
P_1									Plainteks = °
	0	1	0	1	0	0	1	1	

Shif register 1 bit biner *cipherteks* C_2 =00101011 => 10010101

P_2=

C_1	1	0	1	1	0	0	0	0	
K_2	0	1	1	0	1	0	0	1	⊕
	1	1	0	1	1	0	0	1	
C_2	1	0	0	1	0	1	0	1	⊕
P_2									Plainteks = +
	0	1	0	0	1	1	0	0	

Shif register 1 bit biner *cipherteks* C_3 =00001100 => 00000110

P_3=

C_2	0	0	1	0	1	0	1	1

K_3	0	1	1	0	1	1	0	0	⊕
	1	1	0	0	0	0	1	1	
C_3	0	0	0	0	0	1	1	0	⊕
P_3	0	1	0	0	0	0	0	1	Plainteks =

Shif register 1 bit biner *cipherteks* C_4 =01000100 => 00100010

P_4=

C_3	0	0	0	0	1	1	0	0	
K_4	0	1	1	0	0	0	1	1	⊕
	0	1	1	0	1	1	1	1	
C_4	0	0	1	0	0	0	1	0	⊕
P_4	0	1	0	0	1	1	0	1	Plainteks = D

Shif register 1 bit biner *cipherteks* C_5 =11100010 => 01110001

P_5=

C_4	0	1	0	0	0	1	0	0	
K_5	0	1	1	0	0	0	0	1	⊕
	0	0	1	0	0	1	0	1	
C_5	0	1	1	1	0	0	0	1	⊕
P_5	0	1	0	1	0	1	0	0	Plainteks = â

Sampai *ciphertik* C_{19}

Shif register 1 bit biner *cipherteks* C_{19} = 10110100 => 01101001

P_{19}=

C_{18}	0	1	1	1	1	1	0	0	
K_{19}	0	1	1	0	0	0	0	1	⊕
	0	0	0	1	1	1	0	1	
C_{19}	0	1	0	1	1	0	1	0	⊕
P_{19}	0	1	0	0	0	1	1	1	Plainteks = ‘

Maka hasil dari dekripsi operasi feedback *cipher* adalah “°+Dâ,VÀÃÕ÷£{¬|‘”. Setelah didapat hasil dekripsi daru *cipher* feedback maka plainteks tersebut di dekripsikan kembali menggunakan bifid *cipher* untuk mendapatkan teks asli pada operasi selanjutnya yaitu bifid *cipher*.

3.4 Dekripsi Algoritma *Bifid Cipher*

Awal proses enkripsi dilakukan dengan mengidentifikasi posisi tiap huruf berdasarkan baris dan kolomnya. Sama seperti aturan pada playfair, huruf *J* pada plainteks terlebih dahulu diubah menjadi huruf *I*. Untuk contoh kasus dengan *cipher*teks ” °+Dâ,VÀÃÕ÷£{¬|‘” akan diperoleh hasil identifikasi sebagai berikut

Kunci : Sisca Wulandari

*Cipher*teks : S L A M T D L S S W O M O T M D X R G

Baris : 1 2 1 4 5 2 2 1 1 1 4 4 4 5 4 2 5 2 3

Kolom : 1 2 4 2 1 4 2 1 1 5 3 2 3 1 2 4 5 5 4

Tabel 2. Tabel kunci bifid *cipher* proses dekripsi

	1	2	3	4	5
1	S	I	C	A	W
2	U	L	N	D	R
3	B	E	F	G	H
4	K	M	O	P	Q
5	T	V	X	Y	X

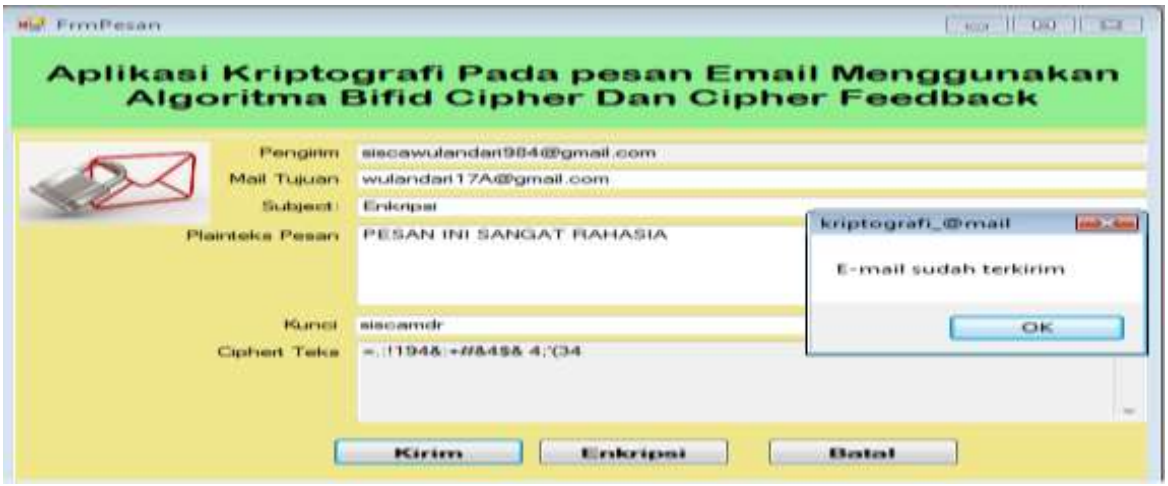
Kemudian *ciphertext* tersebut akan didekripsikan dengan mengembalikan kordinat posisi dan menjadikannya kordinat posisi yang baru dengan aturan tertentu. Dalam hal ini aturan yang digunakan adalah dengan menjadikan kordinat baris dan kolom menjadi satu baris karakter angka dan kemudian membuatnya menjadi bigram (dipisahkan dua-dua) untuk dijadikan kordinat baru yang isi sel nya merupakan hasil dekripsi yang dilakukan. Proses dekripsi secara sistematis akan diperlihatkan sebagai berikut

Kordianat baris dan kolom dijadikan satu baris
karakter angka
1122144251242211111543424351422455 2534
Kemudian pisahkan menjadi bigram yang akan membentuk kordinat baru baris dan kolom kemudian dibaca secara vertikal.
1122144251242211111
5434243514224552534
Maka plainteks adalah isi dari sel dengan kordinat baru yang terbentuk
Baris : 1 1 2 2 1 4 4 2 5 1 2 4 2 2 1 1 1 1 1
Kolom : 5 4 3 4 2 4 3 5 1 4 2 2 4 5 5 2 5 3 4
Plainteks : S a n d i p o r t a l m d r s i s c a

4. IMPLEMENTASI

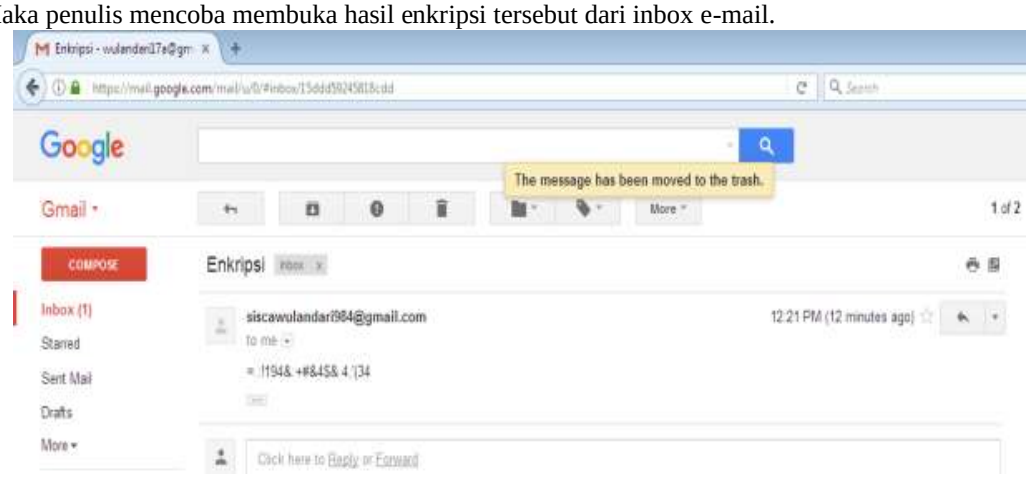
Pada bab ini, penulis akan menampilkan tampilan hasil perancangan yang telah dijelaskan pada bab sebelumnya. Tampilan aplikasi dilakukan setelah tahap analisis, perancangan aplikasi dan pembuatan interface selesai dilakukan. Implementasi ini dilakukan untuk menyelesaikan sistem yang ada dalam dokumen rancangan sistem dan interface yang telah disetujui. Berikut adalah hasil implementasi aplikasi keamanan pesan email dapat dilihat pada gambar dibawah ini:

1. Form menu kirim e-mail merupakan interface untuk mengirim pesan e-mail kepada penerima, pada form ini nantinya pesan asli akan dikodekan menjadi pesan rahasia. Tampilan form kirim e-mail dapat dilihat pada gambar dibawah ini.



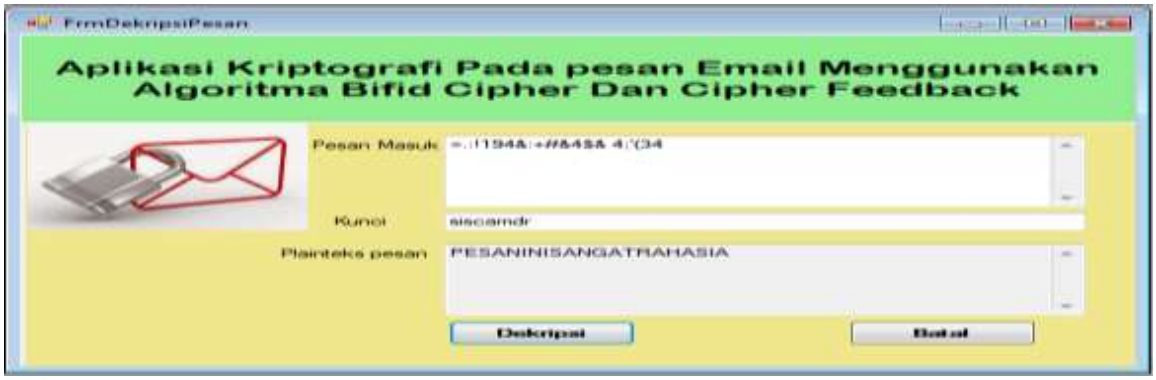
Gambar 1. Form kirim e-mail

Setelah tampil e-mail sudah terkirim langkah selanjutnya adalah melihat pada e-mail tujuan apakah cipher tersebut telah terkirim. Maka penulis mencoba membuka hasil enkripsi tersebut dari inbox e-mail.



Gambar 2. Hasil Enkripsi pada inbox email

2. Form menu pesan masuk merupakan interface untuk mendekripsikan pesan kode yang masuk dari inbox e-mail, pada form ini nantinya pesan code akan dideskripsikan menjadi pesan asli. Tampilan form pesan masuk. Langkah pertama yang dilakukan untuk proses dekripsi adalah mengcopy isi pesan masuk yang berupa sandi kedalam aplikasi dekripsi pesan, kemudian inputkan kunci yang digunakan didalam proses enkripsi, lalu pilih tombol dekripsi. Pada textboxt plainteks pesan maka akan tampil pesan asli (plainteks) adalah sebagai berikut:



Gambar 2. Form Dekripsi.

5. KESIMPULAN

Berdasarkan hasil penelitian yang penulis lakukan maka dapat diambil beberapa kesimpulan yaitu :

1. Aplikasi email ini dapat digunakan untuk memberikan keamanan dalam pengiriman pesan. Sehingga pihak pengirim dan penerima pesan dapat memberikan rasa aman dalam penyampaian pesan tersebut.
2. Pihak-pihak yang tidak berkepentingan didalamnya diharapkan tidak dapat mengetahui isi pesan asli karena enkripsi yang dilakukan oleh aplikasi tersebut.
3. Perangkat lunak yang dibuat dapat langsung diintegrasikan ke email, sehingga memudahkan user untuk melakukan transaksi email dengan hasil pesan yang telah terenkripsi.

REFERENCES

[1] A.S. Permata, "Studi Penggabungan Metode Bifid Cipher pada Algoritma Playfair," ITB, pp. 1-6, 2010.
[2] S.Sansani, "Penerapan Mode Blok Cipher CFB pada Yahoo Messenger," ITB, pp. 1-7, 2010.
[3] D. Ariyus, Pengantar Ilmu Kriptografi: Teori Analisis Dan Implementasi. Yogyakarta : Andi, 2008.
[4] A. Zaki, Trik Mengamankan Komputer untuk Pemula. Jakarta: Alex Media Komputindo, 2009.
[5] R.Munir, Matematika Diskrit. Bandung: Informatika, 2007.
[6] A. Kadir, Pengenalan Algoritma Pendekatan Secara Visual dan Interaktif Menggunakan RAPTOR. Yogyakarta: Andy, 2013.
[7] A. Nugroho, Rekayasa Perangkat Lunak Berorientasi Objek Dengan Metode USDP (unified Software Development Process). Yogyakarta : Andi, 2010.
[8] W. Gata and G. Gata, Sukses Membangun Aplikasi Penjualan Dengan Java. Jakarta : PT. Alex Media Komputindo, 2013.
[9] E. Winarno ST M.Eng and Ali Zaki SmitDev Comunity, Step by Step Visual Basic.NET. Jakarta: PT. Alex Media Komputindo, 2012.
[10] Dodit Suprianto, Membuat Aplikasi Dekstop Menggunakan Mysql Dan VB.NET Secara Profesional. Jakarta : Media Kita, 2010.
[11] Y. Praptomo. PHS, Teknik Improvisasi Algoritma Kriptografi Klasik Dan Implementasinya. Yogyakarta.