KRIPTOGRAFI MONOALFABETIK DAN POLIALFABETIK APLIKASI DAN KOMPARASI DALAM PENGAMANAN *DATABASE* BANK SOAL

Muhammad Safii[1], Vidy[2]
[1] Manajemen Informatika, STMIK Balikpapan
[2] Teknik Informatika, STMIK Balikpapan
[1,2]Jl. Letjen ZA Maulani Rt. 35 No. 9 Balikpapan 76114
E-mail : msafii@stmikbpn.ac.id[1)], vidy@stmikbpn.ac.id[2)]

ABSTRAK

Perancangan sistem pengamanan kunci jawaban database bank soal dilakukan untuk menghindari dan meminimalisir pencurian atau penggunaan file yang tidak sah. Pada kriptografi terdapat banyak algoritma yang telah berkembang, diantaranya adalah subtitusi monoalfabetik dan subtitusi polyalfabetik. Teknik yang akan digunakan dalam pengamanan kunci jawaban bank soal yaitu salah satunya dengan membandikan dua metode monoalfabetik dan subtitusi polyalfabetik.
Pada penelitian ini dilakukan analisa komparasi kemamanan antara subtitusi monoalfabetik dan subtitusi polyalfabetik untuk di terapkan dalam pengamanan database bank soal. Kemudian dilakukan pengujian diantara dua metode tersebut, metode manakah yang paling aman untuk di terapkan dalam aplikasi keamanan kunci jawaban database bank soal.

***Kata kunci** : Kriptografi, bank soal, monoalfabetik, polyalfabetik*

1. PENDAHULUAN

Dalam lingkungan pendidikan pasti ada yang namanya ujian untuk bisa naik ke kelas atau tahapan selanjutnya. Ujian yang telah terkomputerisasi dalam bentuk soal pilihan ganda pasti memiliki bank soal serta kunci jawaban. Bank soal dan kunci jawaban tersebut dapat tertanam didalam script aplikasi dan dapat juga berupa database bank soal baik online maupun tidak. Kumpulan data berupa bank soal yang tersimpan dalam bentuk database merupakan sebuah aset yang sangat penting bagi organisasi. Semakin pentingnya aset tersebut maka organisasi tersebut akan melakukan pengamanan terhadap aset tersebut agar tidak dapat digunakan oleh pihak yang tidak berkepentingan. Kunci jawaban bank soal menjadi salah satu target yang diincar oleh pihak yang tidak berhak menggunakannya untuk keperluan mereka.

Perancangan sistem pengamanan kunci jawaban database bank soal dilakukan untuk menghindari dan meminimalisir pencurian atau penggunaan file yang tidak sah. Pada kriptografi terdapat banyak algoritma yang telah berkembang, diantaranya adalah subtitusi monoalfabetik dan subtitusi polyalfabetik. Teknik yang akan digunakan dalam pengamanan kunci jawaban bank soal yaitu salah satunya dengan membandikan dua metode monoalfabetik dan subtitusi polyalfabetik.

Salah satu metode enkripsi database adalah dengan menggunakan Enkripsi subsitusi monoalphabetik dan subtitusi polialphabetik. Dari kedua metode enkripsi tersebut dapat kita bandingkan manakah metode yang paling baik untuk pengamanan kunci jawaban database bank soal.

Tabel 1.Tabel Bank Soal yang Telah Terenkripsi

No	Soal	Kunci_ jawaban
1	b2+$0&<!}/&<1/)<G<a<}!} <*0J4,/!<}!})}%<[	$
2	u}+$<~2(}+<*"/2}(}+<!}/&<,"/ }0&<0&01"*H<(" 2})&<[	$
3	u}+$<~2(}+<*"fdgdfb/(}+<!}/cfDfre <,"/}0&<0&01"*H<(" 2})&<[	-
4	fdgdfb/(}+<!}/cfDfre<,"/}0& <0&01"*H<("2})&<[&^6 yvT^R	@

Dapat dilihat pada tabel 1 soal ujian dan kunci jawaban telah terenkripsi menjadi chipertext. Tabel diatas merupakan tabel yang field antara soal dan kunci jawaban menjadi satu. Hal ini tentu saja akan membingungkan penyusup. Tetapi teknik ini mempunyai kelemahan, dikarenakan penggunaan teknik enkripsi yang tidak maksimal dan tidak tepat. Dapat dilihat pada tabel 1 field kunci jawaban pada no. 1 dan no. 2 memiliki chipertext yang sama yaitu kharakter '$', yang dapat dianalisi soal ujian no.1 dan no.2 memiliki pola jawaban yang sama, kemungkinan A dan A, B dan B, atau bahkan mungkin D dan D.

Harapan dari penelitia ini, menghasilkan suatu metode yang terbaik untuk pengamanan database bank soal dengan tujuan peserta ujian tidak dapat mengetahui jawaban yang ada pada soal tersebut walaupun mereka dapat melihat databasenya, dan juga sebagai

pembelajaran tentang materi ilmu keamanan computer dengan salah satunya adalah mempelajari ilmu kriptografi.

2. RUANG LINGKUP PENELITIAN

Penelitian tentang *kriptografi* dengan teknik yang sama telah banyak dilakukan antara lain :

1. Perbandingan Kriptografi Ciper Subtitusi Homofonik dan Poligram dengan Caesar Chiper (Syafa'at, 2011)
2. Kombinasi Steganografi Bit Matching dan Kriptografi Des untuk Pengamanan Data (Prasetyoi, 2013)
3. Analysis of cipher text size produced by various Encryption Algorithms (Arora , 2011)

Dalam penelitian syafaat, penulis mencoba membandingkan teknik pengamanan kriptografi dengan menggunakan metode ciper substitusi homofonik dan poligram dengan metode cesar chipper untuk mengidentifikasikan serta menguraikan algoritma kriptografi yang dibahas serta membandingkannya, diuraikan pada bagian hasil dan pembahasan. Algoritma kriptografi yang dibahas adalah algoritma cipher subtitusi homofonik (homophonic subtitution cipher) dan cipher subtitusi poligram (polygram substitution cipher).

Pada penelitian Prasetyo dilakukan kombinasi steganografi dan kriptografi untuk pengamanan data dengan tidak mengubah kualitas media cover. Metode steganografi yang digunakan dengan melakukan pencocokan bit pesan pada bit MSB citra. Proses pencocokan dilakukan secara divide and conquer. Hasil indeks posisi bit kemudian dienkripsi menggunakan algoritma kriptografi Data Encryption Standard (DES). Masukkan data berupa pesan teks, citra, dan kunci. Output yang dihasilkan berupa chiperteks posisi bit yang dapat digunakan untuk merahasiakan data. Untuk mengetahui isi pesan semula diperlukan kunci dan citra yang sama.

Dalam jurnal penelitian arora membahas tentang studi dan perbandingan International Data Encryption Algorithm (IDEA) dengan Data Encryption Standard (DES). IDEA adalah algoritma kriptografi simetri yang beroperasi dalam bentuk blok 64 bit. IDEA ini mengenkripsi plaintext tmenjadi chiperteks dalam delapan putaran. Algoritma ini membagi plaintext yang akan dienkripsi menjadi empat blok, masing-masing terdiri dari enam belas bit. Lima puluh dua berupa kunci (sub-keys) yang terdiri dari enam belas bit dibangkitkan dari kunci utama (master-key) yang terdiri 128 bit. Lalu pada setiap putarannya digunakan enam kunci. Setelah itu dilakukan transformasi final dengan empat kunci untuk membalikkan posisi ke operasi dasar.

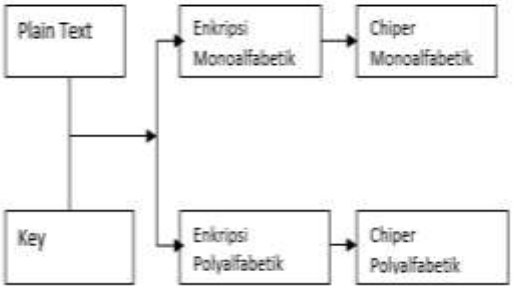
Sedangkan pada penelitian ini, Komparasi subtitusi monoalfabetik dan subtitusi polialfabetik untuk pengamanan database bank soal ini merupakan penelitian untuk mengetahui hasil komparasi keamanan database kunci jawaban bank soal khusus untuk soal pilihan ganda. Objek yang digunakan pada penelitian ini adalah berupa mengenkripsi database dari soal-soal pilihan ganda yang telah di buat oleh dosen atau guru untuk melaksanakan ujian. Sedangkan metode kriptografi yang digunakan dalam komparasi penelitian ini adalah metode Caesar chipher dan vigenere chipper yang mana dua metode ini merupakan salah satu dasar untuk belajar ilmu kriptografi.

3. METODELOGI DAN PERANCANGAN PENELITIAN

Penelitian ini mempergunakan pendekatan dari metode analisis komparatif. Metode analisis komparatif adalah metode untuk membandingkan hasil analisis terhadap dua atau lebih fenomena berupa kesamaan dan perbedaan tersebut. Penelitian Komparatif merupakan penelitian deskriftif yang ingin mencari jawaban secara mendasar tenntang sebab akibat , dengan menganalisis factor-faktor penyebab terjadinya ataupun munculnya suatu fenomena tertentu. Pada penelitian ini yang dibandingkan adalah hasil dari keamanan metode kriptografi subtitusi monoalfabetik dan subtitusi polyalfabetik untuk pengamanan kunci jawaban database bank soal.

Adapun kerangka kerja penelitian digambarkandengan tahapan proses yang dilakukan dalam penelitian agar penelitian dapat berjalan dengan baik dan tujuan yang telah ditetapkan dapat tercapai. Pada penelitian ini penulis menggunakan empat tahapan kerangka kerja penelitian sebagai berikut :

1. Studi literatur :Mempelajari dan memahami teori-teori yang menjadi pedoman dan referensi guna penyelesaian masalah yang dibahas dalam tesis ini dan mempelajari penelitian yang relevan dengan masalah yang diteliti.
2. Pengumpulan data : Mengumpulkan data-data yang berhubungan dengan organisasi yang penulis teliti dengan mengumpulkan dokumen organisasi, melakukan pengamatan dan wawancara dengan pihak-pihak yang terkait.
3. Perancangan Sistem



Gambar 1. Kerangka Perancangan Sistem

4. Pembuatan Laporan : Pada tahapan pembuatan laporan dilakukan setelah kegiatan penelitian menghasilkan metode yang terbaik dalam pengamanan database bank soal sesuai dengan tujuan penelitian.

3.2 Subjek dan Objek penelitian

Subjek dalam penelitian ini adalah komparasi subtitusi monoalfabetik dan subtitusi polialfabetik dalam menerapkan ilmu kriptografi . Sedangkan objek dalam penelitian ini adalah penerapan hasil dari komparasi untuk pengamanan kunci jawaban database bank soal berbasis aplikasi dekstop.

3.3 Analisi Pengumpulan Data

Pengumpulan data dilakukan untuk memperoleh informasi yang dibutuhkan dalam rangka mencapai tujuan penelitian. Tujuan yang diungkapkan dalam bentuk hipotesis merupakan jawaban sementara terhadap pertanyaan penelitian. Proses pengumpulan data dilakukan dengan studi kepustakaan. Peneliti mengambil bahan dan sumber-sumber yang berkaitan dengan topik yang dibahas dengan mencari di buku-buku, artikel, materi perkuliahan dan website-website yang ada di Internet. Adapun jenis data yang dikumpulkan terdiri atas data primer dan data sekunder. Data primer yaitu data yang diperoleh berasal dari website yang membahas algoritma kompresi data khususnya kriptografi dan metode Subtitusi Monoalphabetic dan subtitusi Polyalphabetic . Data sekunder yaitu data yang berasal dari buku yang membahas tentang kriptografi dan Subtitusi Monoalphabetic dan subtitusi Polyalphabetic secara tidak langsung.

3.4 Analisis Perangcangan Database

Dalam analisis pembutan database bank soal pada umumnya field pertanyaan dan field jawaban menjadi satu tabel, sehingga peserta ujian dapat memprediksi jawaban yang ada walaupun telah terenkripsi. Pada umumnya soal yang bersifat pilihan ganda hanya memiliki satu jawaban saja yaitu A, B, C atau D. Bentuk dari tabel data base dapat kita lihat pada tabel dibawah ini:

Tabel 2. Desain tabel database bank soal

Field	Type	Keterangan
No	Varchar (5)	Menampilkan nomor yang sedang dikerjakan, dan bersifat primary key.
Pertanyaan	Text	Menampilkan pertanyaan – pertanyaan yang akan dikerjakan.
Jwb_a	Text	Menampilkan pilihan jawaban, untuk jawaban A.
Jwb_b	Text	Menampilkan pilihan jawaban, untuk jawaban B.
Jwb_c	Text	Menampilkan pilihan jawaban, untuk jawaban C.
Jwb_d	Text	Menampilkan pilihan jawaban, untuk jawaban D.
Jawaban	Varchar (1)	Menampilkan pilihan jawaban, untuk jawaban yang benar.

4. PEMBAHASAN

Berdasarkan data yang telah dianalisa dan dikumpulkan dengan menggunakan metode teknik pengumpulan data, baik data primer maupun data sekunder, maka diperoleh hasil sebagai berikut:

1. Hasil Observasi

Berikut ini adalah hasil pengamatan yang dilakukan peneliti terhadap sistem yang berjalan selama penelitian:

1) Dalam awal perencanaan terlebih dahulu peneliti memahami tentang metode-metode dan algoritma kriptografi yang di peroleh dari berbagai sumber, baik melaului website maupun melalui buku-buku yang membahas tentang ilmu kriptografi.
2) Setelah memahami algoritma dan metode kriptografi subtitusi monoalphabetic dan metode polyalphabetic maka kita dapat membandingkan diantara dua metode tersebut yang paling aman untuk diterapkan dalam keamanan sistem kunci jawaban database bank soal.
3) Menganalisa database bank soal untuk menerapkan kedalam aplikasi apakah tabel antara filed pertanyaan dan field jawaban di jadikan satu tabel atau dibuat terpisah.

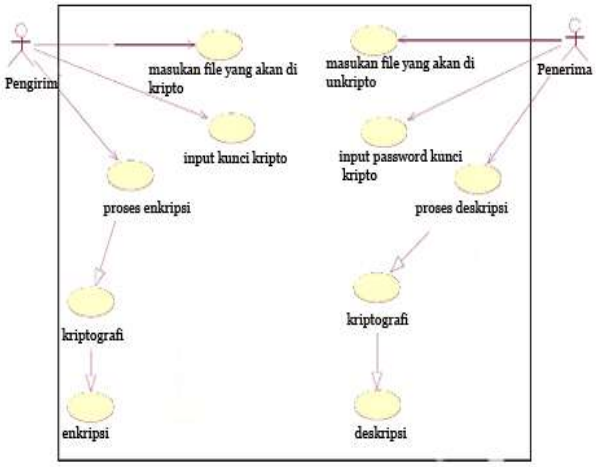
2. Studi Dokumentasi

Berikut ini adalah hasil dari studi dokumentasi:

1) Peneliti mengambil data mengenai peraturan dan tata tertib pelaksanaan UTS dan UAS pada panitia pelaksana untuk dipelajari lebih lanjut sebelum di implementasikan kadalam aplikasi dalam pembutan soal UTS dan UAS.
2) Peneliti mengambil data mengenai Mata kuliah dan jumlah sks pada bagian akademik melalui buku pedoman STMIK Balikpapan tahun 2017.

4.1 Pembahasan analisis data pemodelan

Dalam bahasa pemodelan ini, penulis menggunakan 2 (dua) buah aktor yaitu pengirim dan penerima. Dalam analisis data pomodelan terdapat dua aktor penting dalam proses transaksi data yang akan di enkrpsi dan deskripsikan, yang pertama adalah aktor sebagai pengirim data dan yang kedua adalah aktor sebagai penerima data. Di bawah ini adalah use case diagram yang penulis pakai untuk mengimplementasikan kedalam sebuah model :



Gambar 2. *Use case* aktor

Pada gambar diatas dijabarkan bahwasannya terdapat dua aktor yang mempunyai tugas dan peranan yang berbeda. Aktor pertama adalah aktor pengirim yang bertugas sebagai orang yang memasukan file atau data untuk di kripto dengan cara memasukan kunci kripto lalu melakukan proses enkripsi dan dihasilkan berupa kriptografi yang telah terenkripsi menjadi chipertext (Ci). Selanjutnya tugas aktor pengirim melakukan transfer data ke aktor penerima dengan menyerahkan file yang telah di enkripsi beserta keytext (Ki) untuk kemudian di lakukan proses unkripto dengan cara membuka file yang telah dienkripsi dengan memasukan keytext untuk mendapatkan hasil chipertext menjadi plaintext (Pi).

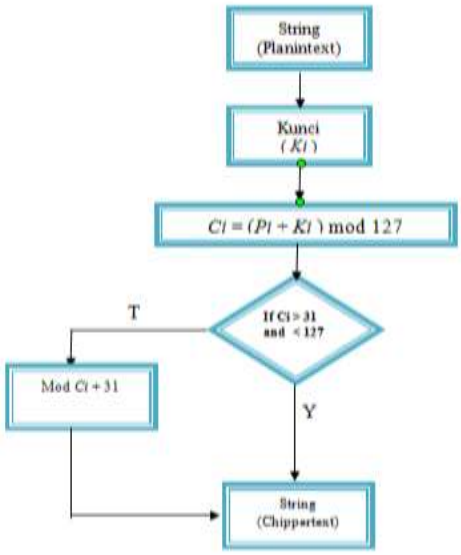
4.2 Subtitusi Monoalfabetic

Dalam penelitian ini metode algoritma caesar chipper kita kombinasikan dengan kode ASCII untuk kita gunakan dalam mengamankan kunci jawaban bank soal. Kode Standar Amerika untuk Pertukaran Informasi atau ASCII (American Standard Code for Information Interchange) merupakan suatu standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal. Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks.

Jumlah kode ASCII adalah 255 kode. Kode ASCII 0..127 merupakan kode ASCII untuk manipulasi teks; sedangkan kode ASCII 128..255 merupakan kode ASCII untuk manipulasi grafik. Kode ASCII sendiri dapat dikelompokkan lagi kedalam beberapa bagian:

1. Kode yang tidak terlihat simbolnya seperti Kode 10(Line Feed), 13(Carriage Return), 8(Tab), 32(Space)
2. Kode yang terlihat simbolnya seperti abjad (A..Z), numerik (0..9), karakter khusus (~!@#$%^&*()_+?:”{})
3. Kode yang tidak ada di keyboard namun dapat ditampilkan. Kode ini umumnya untuk kode-kode grafik.

Adapun alur algoritma enkripsi caesar chipper kombinasi dengan kode ASCII dapat di lihat pada gambar 3. dibawah ini.



Gambar 3. Alur algoritma enkripsi caesar chipher kombinasi kode ASCII

Algoritma program enkripsi dengan menggunakan metode Caesar dapat di lihat pada script dibawah ini :

ENKRIPSI CAESAR

```
Dim data, newdata As String
Dim n, hasil, kode, key As Integer
data = text_user.Text
// VARIABEL data diambil dari plaintext
n = Len(data)
//n adalah jumalah karakter dari plaintext
“data”
// “new data” adalah variabel untuk
chipertext
//“hasil” nilai ASCII asli dari teks
// “kode” nilaii ASCII yang sudah di
tambah KEY
For i = 1 To n
       hasil = Asc(Mid(data, i, 1))
       //mengambil nilai Ascii dari teks
       If (hasil>31 And hasil<127) Then
           kode = (hasil + key) Mod 127
       //menambah nilai ASCII dengan KEY
           If (kode < 31) Then
              kode = kode + 31
           End If
       Else
            kode = hasil
       End If
       newdata = newdata + Chr(kode)
Next i
Print(newdata)
```

Contoh :

Misalkan String yang akan dienkripsi adalah “STMIK” dan kunci yang akan digunakan untuk mengenkripsi adalah “41”. String “kriptografi” akan dikombinasikan dengan kode ASCII mod 127, kemudian dilakukan operasi enkripsi terhadap karakter kode ASCII pada String tersebut, maka selanjutnya akan didapatkan hasil dari enkripsi “STMIK” adalah “#(,*

Jika dibuat tabel subtitusinya maka tabel pertama Pi (plainteks) abjad normal sebagai acuan dan kemudian tabel kedua Nilai dari plaintext (Pi) dan tabel ke tiga adalah Kunci enkripsinya (Ki), tabel ke empat adala nilai hasi mod dan tabel kelima adalah hasil cipherteks (Ci). Adapun tabelnya dapat dilihat pada tabel 3 dibawah ini :

Tabel 3. Contoh kombinasi caesar chipper dan kode ASCII

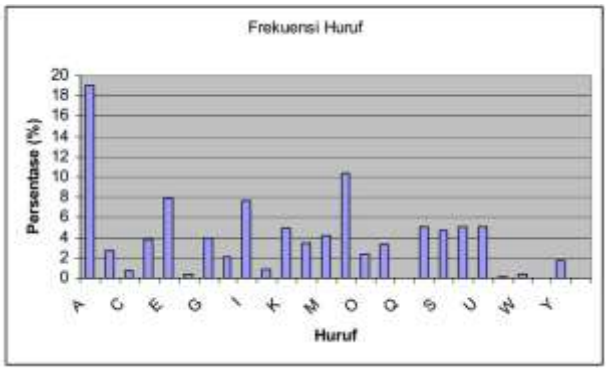
Plaintext (*Pi*)	S	T	M	I	K
Nilai	83	84	77	49	75
Key (*Ki*)	41	41	41	41	41
Nilai mod	34	35	40	44	42
Chippertext (*Ci*)	“	#	(	,	*

Contoh 1. Pesan
STMIK
disamarkan (enskripsi) menjadi
“#(,*
Penerima pesan men-dekripsi chiperteks dengan menggunakan tabel substitusi, sehingga chiperteks
“#(,*
dapat dikembalikan menjadi plainteks semula:
STMIK

Pada monoalphabetic substitution cipher maka satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain, sehingga pola enkripsinya lebih mudah diketahui, karena satu huruf pada ciphertext pasti merepresentasikan satu huruf pada plaintext.

Salah satu cara untuk bisa memecahkan penyandian dengan cara monoalphabetic subsitution cipher adalah dengan melakukan analisa frekwensi munculnya huruf dalam suatu bahasa. Berapa sering suatu huruf muncul dalam suatu bahasa tertentu bisa memberi petunjuk huruf-huruf yang muncul pada ciphertext asal diketahui plaintext yang digunakan berbahasa apa. Agar diperoleh pendekatan yang maksimal, maka sebaiknya dilakukan terhadap ciphertext yang cukup panjang, karena jika plaintextnya terlalu pendek, maka tingkat ketelitiannya akan menjadi rendah.

Grafik berikut memperlihatkan persentase frekwensi huruf dalam bahasa Indonesia:



Gambar 4. Frekwensi huruf dalam bahasa indonesia

Pada gambar diatas dilakukan analisa terhadap kemungkinan munculnya huruf dalam bahasa Indonesia. Dari 1000000 (satu juta) karakter, maka huruf ‘A’ menduduki peringkat tertinggi yaitu di atas 19%, huruf ‘N’ menduduki peringkat kedua yaitu sekitar 10% dan huruf ‘I’ menduduki peringkat selanjutnya yaitu 8%. Jika kita melakukan kriptografi sustitusi dengan cara monoalphabetic substitution cipher, maka satu karakter dari ciphertext merepresentasikan satu huruf dari plaintext. Jika diketahui bahwa plaintextnya bahasa Indonesia dan dilakukan analisa frekwensi munculnya huruf terhadap ciphertext tersebut, maka prosentasi munculnya suatu huruf pada ciphertext akan mendekati prosentasi muculnya huruf yang diwakilinya dalam plaintext. Sehingga jika, pada ciphertext, huruf ‘D’ mendekati 19%, maka akan sangat mungkin bahwa huruf ‘D’ adalah huruf ‘A’, begitu juga dengan huruf-huruf lainnya.

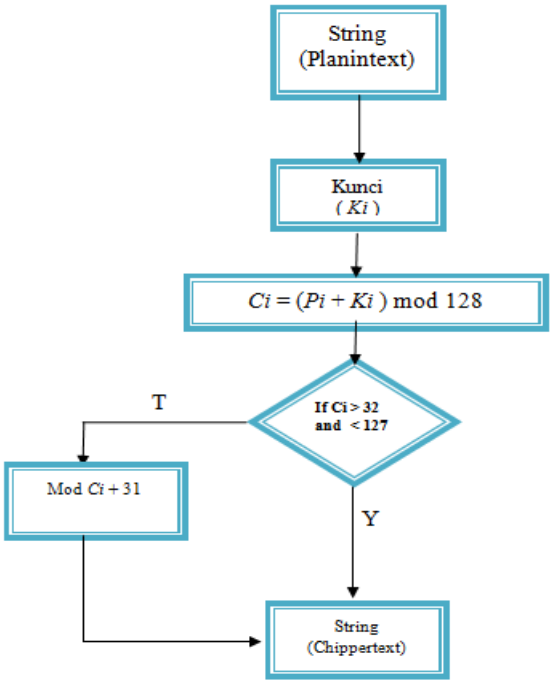
4.3 Subtitusi Polyalfabetic

Dalam Subtitusi Polyalphabetic salah satu metode kriptografi yang dikenal adalah vigenere chiper. Sandi vigenere adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Pada kriptografi Vigenere, plaintext akan dienkripsi dengan pergeseran huruf seperti pada kriptografi Caesar tetapi setiap huruf di dalam plaintext akan mengalami pergeseran yang berbeda. Kunci pada kriptografi Vigenere adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat berulang sepanjang plaintext, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada plaintext. Pergeseran setiap huruf pada plaintext akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada plaintext.Sandi vigenere merupakan bentuk sederhana dari sandi substitusi polialfabetik.

Contoh, jika plaintext adalah “Sebutkan Otak Komputer” dan kunci adalah Eresha maka proses enkripsi yang terjadi adalah sebagai berikut:

Plaintext : Sebutkan Otak Komputer
Key : eresha
Chipertext : 8XGh\L&`$B\B010bqQ:fje

Adapun alur algoritma *Vegenere chipper* kombinasi dengan kode ASCII dapat di lihat pada gambar dibawah ini.



Gambar 5. Alur algoritma enkripsi *vigenere chipher* kombinasi kode ASCII

Jika dibuat tabel subtitusinya maka tabel pertama Pi (plainteks) abjad normal sebagai acuan dan kemudian tabel kedua Nilai dari plaintext (Pi) dan tabel ke tiga adalah Kunci enkripsinya (Ki), tabel ke empat adalah nilai dari kunci enkripsi, tabel kelima adalah nilai dari penjumlahan hasil mod dan tabel keenam adalah hasil cipherteks (Ci). Adapun tabelnya dapat dilihat pada gambar dibawah ini :

Pi	S	E	B	u	t	k	a	N		O	T	a	k
Ni	83	101	98	117	116	107	97	110	32	79	116	97	107
Ki	E	R	E	s	h	a	E	R	e	s	H	a	E
Ni	69	114	101	115	104	97	69	114	101	115	104	97	69
mod	56	88	71	104	92	76	38	96	36	66	92	66	48
Ci	8	X	G	h	\	L	&	`	$	B	\	B	0
Pi		K	o	m	p	u	t	e	r				
Ni	32	75	111	109	112	117	116	101	114				
Ki	r	e	s	h	a	E	r	e	s				
Ni	114	101	115	104	97	69	114	101	115				
mod	49	48	98	113	81	58	102	74	101				
Ci	1	0	b	q	Q	:	f	J	e				

Gambar 6. Contoh Enkripsi kombinasi Vigeneree chipper dan kode ASCII

Pada contoh diatas kata kunci Eresha diulang sedemikian rupa hingga panjang kunci sama dengan panjang plainteksnya. Jika dihitung dengan rumus enkripsi vigenere plainteks huruf pertama S (yang memiliki nilai Pi=83) akan dilakukan pergeseran dengan huruf E (yang memiliki Ki=69) maka prosesnya sebagai berikut:

$$Ci = E(p_i) = (P_i + Ki) \bmod 127 \quad (1)$$

atau

$$Ci = E(Pi) = (Pi + Ki) - 127$$

bila hasil penjumlahan *Pi* dan *Ki* lebih dari 127 . Bila hasil *Ci* lebih kecil dari 32 maka hasil nilai *Ci* di tambahkan dengan nilai 31

Ci = (Pi + Ki) mod 127
= (83 + 69) mod 127
= 152 mod 127
= 152 - 127
= 25 + 31
= 56

Ci=56 maka huruf ciphertext dengan nilai 56 adalah 8. Algoritma enkripsi subtitusi polialphabetik dengan metode enkripsi *Viginere chipper* dapat dituliskan sebagai berikut:

```
Dim J As Integer
Dim Jum As Integer
Dim sKey As String
Dim nKata As Integer
Dim nKunci As Integer
Dim sKata As String
Dim sPlain As String = ""
Dim nEnc As Integer

J = 0
sKata = plain.Text
Jum = Len(sKata)
sKey = kunci.Text
    For i = 1 To Jum
        If J = Len(sKey) Then
           J = 1
        Else
           J = J + 1
        End If
        nKata = Asc(Mid(sKata, i, 1)) + 0
        nKunci = Asc(Mid(sKey, J, 1)) + 0
        nEnc = ((nKata + nKunci) Mod 256)
        sPlain = sPlain & Chr((nEnc))
     Next i
chiper.Text = sPlain
```

4.4 Hasil perbandingan analisa database

Salah satu aspek yang terpentik dalam keamana basis data adalah proteksi terhadap pengaksesan, pembacaan informasi, pemodifikasian dan pengrusakan data oleh pihak yang tidak mempunyai kewenangan. Keamanan basis data juga berarti menjaga penyalahgunaan basis

data baik secara sengaja, misalnya pengambilan data atau pembacaan data, pengubahan data dan penghapusan data oleh pihak yang tidak berwenang, maupun secara tidak sengaja, misalnya kerusakan selama transaksi, anomali yang disebebkan oleh akses basis data konkuren, anomali yang disebebkan oleh pendistirbusian data pada beberapa komputer dan logika error yang mengancam kemampuan transaksi untuk mempertahankan konsistensi basis data.

Tabel 4. Table database dengan kunci jawaban menjadi satu

No	Soal	Kunci_ jawaban
1	b2+$0&<!}/&<1/)<G<a<}!} <*0J4,/!<}!})}%<[	$
2	u}+$<~2(}+<*"/2}(}+<!}/& <,"/}0&<0&01"*H<(" 2})&<[	$
3	u}+$<~2(}+<*"fdgdfb/2}(}+<!} /cfDfre<,"/}0&<0&01"*H<(" 2})&<[	-
4	^%$^$2(}+<*"fdgdfb/2}(}+<!} /cfDfre<,"/}0&<0&01"*H<(" 2})&<[*&Y&*Y766&B*&&^&*^Buy767%^%^	9
5	^&7)(2(}+<*"fdgdfb/2}(}+<!} /cfDfre<,"/}0&<0&01"*H<(" 2})&<*(*&^^=_+)*&*&5654%$#5[	P
6	I*&*y^68u}+"fdgdfb/2}(}+<!} /cfDfre<,"/}0&<0&01"*H<(" 2})&<[)()8907897yh767U&tyu76G75567%%%&	+
7	*&*y^68u}+"fdgdfb/2}(}+<!} /cfDfregHK ut)()(*t y%^Z utTuiy 7ty6&Yugt67 t6dsr DdttdD6t(&*&%%^#$vt6%^$#	$

Pada tabel diatas terdapat contoh database bank soal yang mana tabel database antara soal dan kunci jawaban di gabung menjadi satu. Pada contoh database di atas menggunakan metode kriptografi caesar dan viginere. Dapat kita liahat pada field kunci jawaban terdapat sebuah karakter jawaban yang telah terenkripsi terdiri dari satu jawaban saja yaitu A,B,C,D atau E. Dari karakter jawaban tersebut terdapat karakter yang sama yaitu simbol $, sehingga peserta ujian dapat menebak karakter huruf apa sebagai pengganti simbol $ tersebut. Peserta dapat menebak karakter tersebut dengan cara mencari soal yang mudah terlebih dahulu kemudian mencari jawaban yang sudah pasti benarnya. Contoh bila Jawaban soal nomor satu adalah A yang kemudian karakter enkripsinya adalah $ maka untuk jawaban nomor dua adalah sama yaitu A. Sehingga untuk penerapan pengaman database bank soal dengan menggunakan tabel antara field soal dan kunci jawaban dijadikan menjadi satu kurang efektif.

Tabel 5. Table database dengan kunci jawaban dipisah dari table soal

No	Soal
1	b2+$0&<!}/&<1/)<G<a<}!}<*0J4,/! <}!})}%<[
2	u}+$<~2(}+<*"/2}(}+<!}/&<,"/}0& <0&01"*H<(" 2})&<[
3	u}+$<~2(}+<*"fdgdfb/2}(}+<!}/cfDfre <,"/}0&<0&01"*H<(" 2})&<[
4	^%$^$2(}+<*"fdgdfb/2}(}+<!}/cfDfre <,"/}0&<0&01"*H<(" 2})&<[*&Y&*Y 766&B*&&^&*^Buy767%^%^
5	^&7)(2(}+<*"fdgdfb/2}(}+<!}/cfDfre <,"/}0&<0&01"*H<(" 2})&<*(*&^^= _+)*&*&5654%$#5[
6	I*&*y^68u}+"fdgdfb/2}(}+<!}/cfDfre <,"/}0&<0&01"*H<(" 2})&<[)()8907897yh767U&tyu76G75 567%%&^%&

Pada tabel diatas merupakan tabel soal yang terdiri dari field no soal dan isi soal. Dapat kita lihat pada tabel diatas untuk field kunci jawaban dibuat tabel tersendiri sehingga terpisah dari tabel soal. Hal ini diharapkan agar peserta ujian tidak dapat mengetahui kunci jawabn bank soal yang mana untuk tabel kunci jawaban telah dibuat secara terpisah.

Tabel 6. Table database kunci jawaban Caesar dan kunci jawaban Vigeneree

Jawaban
(*(@$R*$$R((@$*@@

Jawaban
(*(!#34$%&^*&*(()__=?><bZ?><

Pada tiga tabel contoh di atas kita melihat tabel bank soal dan Kunci jawaban di buat terpisah, tujuan dari dibuatnya tabel tersebut untuk memudahkan dalam proses enkripsi kunci jawaban. Pada tabel 6 yang merupakan tabel kunci jawaban dengan menggunakan metode viginere. Jawaban yang semula terdiri dari lima huruf yaitu A,B,C,D dan E pada saat proses enkripsi terdapat banyak karakter simbol yang berbeda. Cintoh bisa saja karakter simbol * yang pertama adalah jawaban dengan untuk huruf A sedangkan pada karakter yang sama * yang kedua belum tentu jawaban tersebut adalah untuk kunci jawaban A melainkan B atau C. Hal ini disebabkan karena unuk metode viginere menggunakan kunci lebih dari satu tergantung karakter yang dibuat oleh pengirim. Semakin panjang kunci yang dibuat maka akan semakin rumit peserta ujian untuk menebak karakter enkripsi yang ada di tabel kunci jawaban. Hal ini sangat menyulitkan bagi para peserta ujian yang ingin mengetahui kunci jawaban bank soal yang ingin berbuat tidak benar dalam proses ujian.

4.5 Hasil Perbandingan Metode Monoalfabetik dan Polyalfabetik

Dari penjelasan diatas mulai pembahasan subtitusi monoalphabetik, subtitusi polialphabetik dan perbandingan database bank soal dapat kita ambil ketahui pebandingan antara masing-masing metode subtitusi. Yang pertama kita melihat dari unsur perbandingan diantaranya adalah unsur proses perhitungan, proses keamanan, proses database dan proses penggunaan aplikasi.

Tabel 7. Table hasil perbandingan monoalfabetik dan polyalfabetik

No	Unsur	Monoalphabetik	Polialphabetik
1	Proses Perhitungan	Proses perhitungan lebih cepat bila ada karakter plaintext yang sama	Proses perhitungan membutuhkan waktu yang lama karena walaupun karakter Plaintext sama tapi karena kunci textnya berbeda maka harus tetap di hitung
2	Keamanan	Hasil enkripsi masih dapat ditebak karena penggunaan kunci yang sama	Hasil enkripsi sangat sulit dipecahkan atau ditebak karena kuncitext yang di pakai mempunyai karakter yang panjang
3	Database	Karakter yang terdapat dalam database masih terdapat karakter yang sama	Karakter enkripsi yang terdapat dalam database lebih bervariasi dan jarang ada yang sama walaupun Plaintextnya sama
4	Penggunaan	Cocok sebagai aplikasi pembelajaran khusus kriptografi dasar	Cocok untuk penerapan aplikasi yang bersifat rahasia bagi perusahaan atau kenegaraan

Dari tabel diatas, dapat diambil sebagai perbandingan kelebihan subtitusi polialphabetik dari metode subtitusi monoalphabetic dalam hal keamanan kunci jawaban bank soal adalah:

1. Subtitusi polialphabetik lebih aman daripada subtitusi monoalphabetik untuk pengamanan kunci jawaban database bank soal. Hal ini dikarenakan setiap huruf *Plaintext* satu dengan yang lain dapat berbeda hasilnya saat di enkripsi.
2. Waktu Proses yang diperlukan Subtitusi Polialfabetik lebih lama di bandingkan dengan proses Subtitusi Monoalphabetik dikarenakan Algoritma yang di baca lebih panjang.
3. Karakter yang terdapat pada Subtitusi polialfabetik lebih banyak dibandingkan dengan karakter yang ada pada Subtitusi Monoalfabetik

Metode Subtitusi Polialfabetik lebih cocok digunakan untuk mengamankan aplikasi yang bersifat rahasia kenegaraan atau perusahaan sedangkan untuk metode subtitusi monoalphabetik dapat digunakan pada aplikasi pembelajaran dasar metode keamanan komputer.

5. KESIMPULAN

Dari hasil penelitian yang dilakukan mulai dari tahap awal hingga proses pengujian, dapat disimpulkan bahwa dengan adanya penelitian ini diharapkan dapat menambah wawasan ilmu dalam bidang keamanaan komputer. Dari uraian di atas, dapat diambil kesimpulan kelebihan subtitusi polialphabetik dari metode subtitusi monoalphabetik dalam hal keamanan kunci jawaban bank soal adalah:

1. Subtitusi polialphabetik lebih aman daripada subtitusi monoalphabetik untuk pengamanan kunci jawaban database bank soal. Hal ini dikarenakan setiap huruf *Plaintext* satu dengan yang lain dapat berbeda hasilnya saat di enkripsi.
2. Waktu proses yang diperlukan subtitusi polialfabetik lebih lama di bandingkan dengan proses subtitusi monoalphabetik dikarenakan algoritma yang di baca lebih panjang.
3. Karakter yang terdapat pada subtitusi polialfabetik lebih banyak dibandingkan dengan karakter yang ada pada subtitusi monoalfabetik
4. Metode subtitusi polialfabetik lebih cocok digunakan untuk mengamankan aplikasi yang bersifat rahasia kenegaraan atau perusahaan sedangkan untuk metode subtitusi moanoalphabetik dapat digunakan pada aplikasi pembelajaran dasar metode keamanan komputer.

6. SARAN

Disarankan pada penelitian berikutnya perbandingan teknik enkripsi kunci jawaban dengan metode kriptografi yang terbaru, seperti MD5, Hash, RSA, atau metode baru lainnya.

7. PUSTAKA

Andrea, R. 2013.Teknik Pengamanan Kunci Jawaban dengan Metode Enkripsi, Prosiding SeNAIK, pp. 154-156. http://jurnal.wicida.ac.id/index.php/senaik/article/view/134

Arora, Mani. 2011. Analysis of cipher text size produced by various Encryption Algorithms" Jurnal Internasional ISSN : 0975-5462 , Vol. 3 No. 7 July 2011.

Budy. 2013. Analisis Perbandingan Algoritma Kriptografi AES, DES dan IDEA yang Tepat untuk Perangkat mobile" Tesis Universitas Atma Jaya Yogyakarta.

H. Kridalaksana, A., Rangan, A. Y. and Ansharie, A. 2017. Enkripsi Data Audio Menggunakan Metode Kriptografi RSA, Sebatik, 17(1), pp. 6-10

Munir, Rinaldi, Kriptografi, Penerbit Informatika, Bandung, Oktober 2006.

Stallings, William. 2011. Cryptography and Network Security Principles and Practice Fifth Edition, Pearson Education, ISBN 13: 978-0-13-609704-4,

Sugiyono. 2010. Metode Penelitian Kuantitatif, Kualitatif dan R&D. Bandung: Alfabeta

Syafa'at, Achmad, 2011. Perbandingan Kriptografi Ciper Subtitusi Homofonik dan Poligram dengan Caesar Chiper" Tesis Universitas Langlang Buana.

Ukkas, M., Andrea, R. and Anggen, A. B. P. 2017. Teknik Pengamanan Data Dengan Steganografi Metode End Of File (EOF) Dan Kriptografi Vernam Cipher, Sebatik, 17(1), pp. 20-26.

Ward, Annie W. & Murray-Ward, Mildred. 2004. Guidelines for the Development of Item Banks. Modul pembelajaran NCME. dalam Instructional Topics in Educational Measurement(ITEMS). http://www.ncme.org/pubs/items/25.pdf diakses 4 Juni 2017

Publikasi ini dibiayai oleh:
Direktorat Riset dan Pengabdian Masyarakat
Direktorat Jenderal Penguatan Riset dan Pengembangan
Kementerian Riset, Teknologi, dan Pendidikan Tinggi
sesuai dengan Kontrak Penelitian Tahun Anggaran 2018