BAB II

TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Aplikasi tentang kriptografi seperti ini pernah dibuat sebelumnya oleh Anjar Setyo Nugroho (2010) telah dibuat PENERAPAN KRIPTOGRAFI PADA SMS MOBILE DENGAN METODE VIGENERE CIPHER dengan bahasa pemrograman Java 2 Micro Edition (J2ME), yang berisikan pembuatan aplikasi untuk keamanan data short message service (SMS) dengan metode Vigenere Cipher. Pada karya ilmiah ini bertujuan untuk mengembangkan aplikasi tersebut agar mampu mengkompresi data sms untuk menghemat biaya sms.

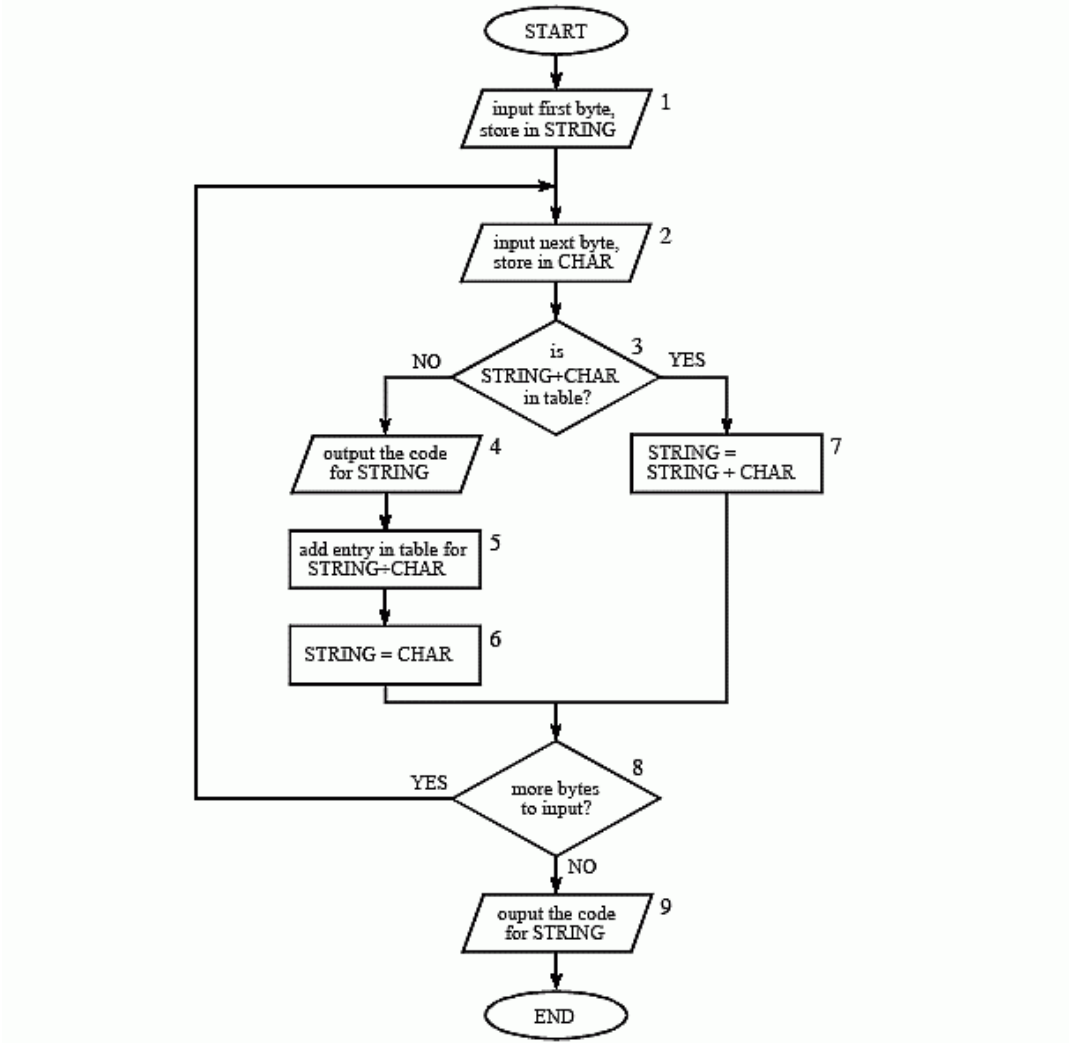
2.2 Dasar Teori

2.2.1 Algoritma *LZW*

Algoritma LZW dikembangkan dari metode kompresi yang dibuat oleh Ziv dan Lempel pada tahun 1977. Algoritma ini melakukan kompresi dengan menggunakan *dictionary*, di mana fragmen-fragmen teks

digantikan dengan indeks yang diperoleh dari sebuah "kamus". Prinsip sejenis juga digunakan dalam kode Braille, di mana kode-kode khusus digunakan untuk merepresentasikan kata-kata yang ada.

Pendekatan ini bersifat *adaptif* dan efektif karena banyak karakter dapat dikodekan dengan mengacu pada *string* yang telah muncul sebelumnya dalam teks. Prinsip kompresi tercapai jika referensi dalam bentuk *pointer* dapat disimpan dalam jumlah bit yang lebih sedikit dibandingkan *string* aslinya. *Dictionary* diinisialisasi dengan semua karakter dasar yang ada : {'A'..'Z','a'..'z','0'..'9'}.



Gambar 2.1 Algoritma LZW

Kegunaan : LZW banyak dipergunakan pada UNIX, GIF,V.42 untuk modem.

Algoritma Kompresi LZW(*Lempel-Ziv-Welch)* :

BEGIN

s = next input character;

while not EOF

```
{
c = next input character;
if s + c exists in the diactionary
s = s + c
else
{
Output the code for s;
Add string s + c to the dictionary with a new code
 = c;
}
}
END
```

Contoh Soal : ABABBABCABABBA

Dengan mengikuti algoritma LZW maka di dapatkan penyelesaian dalam bentuk tabel berikut :

Tabel Penyelesaian Algoritma LZW

P	C	KODE	STRING	OUTPUT
		1	A	
		2	B	
		3	C	
A	B	4	AB	1
B	A	5	BA	2
A	B			
AB	B	6	ABB	4
B	A			
BA	B	7	BAB	5
B	C	8	BC	2
C	A	9	CA	3
A	B			
AB	A	10	ABA	4
A	B			
AB	B			
ABB	A	11	ABBA	6
A	EOF			1

2.2.2 Vigenere Cipher

Vigenere Cipher merupakan salah satu cipher yang terkenal. Vigenere Cipher termasuk copher substitusi abjad-majemuk (*polyalphabethic substitution cipher*).

Diplublikasikan oleh diplomat (*sekaligus seorang kriptologis*) Perancis, Blaise de Vigenere pada Abad 16, Tahun 1586. Sebenarnya Glovan Batista Belaso telah menggambarkannya untuk pertama kali pada Tahun 1553 seperti ditulis pada buku *La Cifra del Sig*. Algoritma ini baru dikenal luas 200 tahun kemudian dinamakan kode Vigenere. Vigenere merupakan pemicu perang sipil di Amerika dan kode Vigenere digunakan oleh Tentara Konfiderasi (*Confiderate Army*) pada Perang Sipil Amerika (*American Civil War*). Kode Vigenere berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan Abad 19.

Teknik substitusi Vigenere dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser.

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

Kunci dengan 6 huruf kode jika ditukar dengan angka akan menjadi K=(2,8,15,7,4,17), dan teks aslinya “This Cryptosystem is Not Secure”.

T	H	I	S	C	R	I	P	T	O	S	I	S	T
19	7	8	18	2	17	24	15	19	14	18	24	18	19
2	8	15	7	4	17	2	8	15	7	4	17	2	8
21	15	23	25	6	8	0	23	8	21	22	15	20	1

E	M	I	S	N	O	T	S	E	C	U	R	E
4	12	8	18	13	14	19	18	4	2	20	17	4
15	7	4	17	2	8	15	7	4	17	2	8	15
19	19	12	9	15	22	8	25	8	19	22	25	19

Teks asli : THISCRIPTOSISTEMISNOTSECURE

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

Teks kode : VPXZGIAXIVWPUBTTMJPWIZITWZT

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

2.2.3 J2ME *(Java 2 Micro Edition)*

J2ME *(Java Micro Edition)* merupakan tulang punggung bagi perkembangan teknologi m-commerce saat ini. Beberapa keunggulan dari penggunaan J2ME adalah :

a. Menciptakan aplikasi yang bersifat portable.

b. Sistem keamanan yang baik.

c. Aplikasi bisa digunakan dalam mode *offline* dan *online*.

2.2.4 MIDP dan MIDlet

MIDP *(Mobile Information Device Profile)* adalah profil yang menefinisikan model aplikasi yang bisa dijalankan pada device dengan resource terbatas dan memungkinkannya untuk digunakan oleh beberapa aplikasi MIDP secara bersama-sama.

MIDlet adalah sebutan untuk aplikasi yang berjalan dengan konfigurasi MIDP. Aplikasi MIDlet adalah bagian dari kelas "javax.microedition.midlet.MIDlet" yang dedefinisikan pada MIDP. MIDlet berupa sebuah kelas abstrak yang merupakan sub kelas dari bnetuk dasar aplikasi sehingga antar muka aplikasi J2ME dan aplikasi manajemen pada perangkat dapat berbentuk siklus hidup MIDlet.

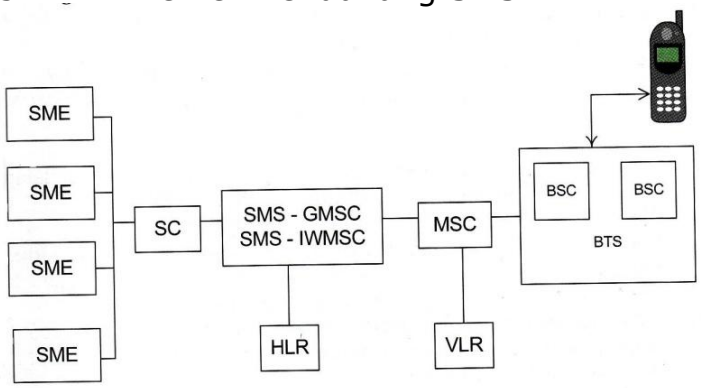
2.2.5 SMS

Adalah salah satu fasilitas dari teknologi GSM yang memungkinkan *Mobile Station* (MS) mengirim dan menerima pesan singkat berupa text dengan kapasitas maksimal 160 karakter. Pengiriman SMS yang menggunakan kanal signaling yang merupakan kanal kendali dan memiliki 2 tipe:

a. SMS *Point to Point*, yaitu pengiriman SMS hanya dari satu MS ke MS tertentu.

b. SMS *Broadcast*, yaitu pengiriman SMS ke beberapa MS sekaligus, misalnya dari operator keseluruh pelanggan.

2.2.5.1 Elemen Pendukung SMS



Gambar 2.2 Elemen jaringan penyusunan layanan SMS

Elemen jaringan penyusun yang mutlak ada pada layanan SMS adalah :

a. SME *(Short Message Entity)*, merupakan tempat penyimpanan dan pengiriman pesan yang akan dikirimkan ke suatu MS tertentu.

b. SC *(Service Center)*, bertugas untuk menerima *message* dari SME dan melakukan forwarding ke alamat MS yang dituju.

c. SMS-GMSC *(Short Message Service – Gateway MSC)*, melakukan penerimaan *message* dari SC dan memeriksa parameter yang ada. Selain itu GMSC juga mencari alamat MS yang dituju dengan bantuan HLR,dan mengirimkan kembali ke MSC yang dimaksud.

d. SMS-IWMSC *(Short Message Service-Interworking MSC)*, berperan dalam SMS Message Originating, yaitu menerima pesan dari MSC.

2.2.6 *Unified Modeling Languange* (UML)

Sebuah bahasa yang telah menjadi standar dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak. UML menawarkan sebuah standar untuk merancang model sebuah sistem. Untuk membuat suatu model, UML memiliki diagram grafis sebagai berikut :

a. Use-case diagram

b. Class diagram

c. Sequence diagram

d. Activity Diagram

Diagram-diagram tersebut diberi nama berdasarkan sudut pandang yang berbeda-beda terhadap sistem dalam proses analisis atau rekayasa.