IMPLEMENTASI ALGORITMA VIGENERE MENGGUNAKAN MIKROKONTROLER UNTUK PENGIRIMAN SMS PADA SISTEM PEMANTAU PENGANGKUTAN ZAT RADIOAKTIF

Adi Abimanyu, Nurhidayat, Jumari
Pusat Teknologi Akselerator Dan Proses Bahan – BATAN
abimanyu.adi@batan.go.id, jumari@batan.go.id, nurhid@batan.go.id

ABSTRAK

IMPLEMENTASI ALGORITMA VIGENERE MENGGUNAKAN MIKROKONTROLER UNTUK PENGIRIMAN SMS PADA SISTEM PEMANTAU PENGANGKUTAN ZAT RADIOAKTIF. *Aspek keselamatan dan keamanan zat radioaktif dari pengirim sampai dengan penerima merupakan hal yang harus dijamin supaya tidak membahayakan manusia. Pada umumnya pemantauan pengangkutan zat radioaktif dilakukan dengan percakapan melalui komunikasi telepon untuk mengetahui lokasi dan laju paparan zat radioaktif. Dari aspek keamanannya, komunikasi percakapan melalui telepon mudah diinterpretasikan oleh orang lain, disamping itu kemungkinan terjadinya human-error cukup tinggi. Layanan SMS dikenal mudah dalam hal penggunaan sehingga layanan SMS dapat digunakan sebagai pengganti percakapan melalui komunikasi telepon untuk memantau laju paparan radiasi dan posisi zat radioaktif dalam pengangkutan zat radioaktif. Sistem pemantau pengangkutan zat radioaktif yang akan dikembangkan mengimplementasi algoritma vigenere menggunakan mikrokontroler untuk mengirimkan SMS (Short Message Service) untuk berkomunikasi. Pengujian yang dilakukan adalah pengujian enkripsi dan deskripsi serta waktu komputasi yang dibutuhkan. Dari hasil pengujian didapatkan bahwa telah berhasil diimplementasikan algoritma vigerene untuk mengenkripsi dan mendeskripsi pesan pada sistem pemantau pengangkutan zat radioaktif dan waktu komputasi yang diperlukan untuk mengenkripsi dan mendeskripsi data adalah 13,05 ms untuk 36 karakter serta 13,61 untuk 37 karakter. Sehingga untuk setiap satu karakter diperlukan waktu komputasi 0,56 ms.*

Kata kunci: vigenere, mikrokontroler, SMS

ABSTRACT

IMPLEMENTATION VIGENERE ALGORITHM USING MICROCONTROLER FOR SENDING SMS IN MONITORING RADIOACTIVE SUBTANCES TRANSPORT SYSTEM. *Aspects of safety and security of radioactive substances from the sender to the receiver is to be secured for not to harm humans. In general, monitoring the transport of radioactive materials is done by communication with a telephone conversation to determine the location and rate of exposure radioactive substances. From the aspect of safety, communication through telephone conversations easily interpreted by others, in addition the possibility of human-error is quite high. SMS service is known for its ease in terms of use so that SMS can be used as a substitute for communication through telephone conversations to monitor the rate of radiation exposure and the position of radioactive substances in the transport of radioactive substances. The system monitors the transport of radioactive materials developed by implement vigenere algorithms using a microcontroller for sending SMS (Short Message Service) to communicate. Tests was conducted to testing encryption and description and computation time required. From the test results obtained they have been successfully implemented vigerene algorithm to encrypt and decrypt the messages on the transport of radioactive monitoring system and the computational*

time required to encrypt and decrypt the data is 13.05 ms for 36 characters and 13.61 for 37 characters. So for every single character require computing time 0.56 ms.

Keywords: vigenere, microcontroller, SMS

PENDAHULUAN

Pemanfaatan zat radioaktif saat ini telah meliputi berbagai macam bidang seperti bidang kedokteran (radiologi), pertanian (mutasi genetik pengembangan bibit unggul), industri (pengujian kualitas las) dan lain sebagainya. Hal ini mengakibatkan. permintaan akan zat radioaktif semakin bertambah sehingga produksi zat tersebut juga semakin meningkat. Zat radioaktif didefinisikan sebagai zat yang mengandung inti atom tidak stabil, atau setiap zat yang memancarkan radiasi pengion dengan aktivitas jenis lebih besar dari 70kBq/kg [1].

Untuk membawa zat radioaktif dari tempat produksi ke lokasi pemanfaatannya diperlukan pengangkutan zat radioaktif, mengingat bahaya radioaktif bagi manusia. Pengangkutan zat radioaktif [2] didefinisikan sebagai pemindahan zat radioaktif dari satu tempat ke tempat lain melalui jaringan lalu-lintas umum dengan sarana angkutan darat, air dan udara. Pengangkutan zat radioaktif melibatkan pengirim, pengangkut dan penerima. Pengirim [2] adalah orang atau badan yang menyiapkan pengiriman untuk pengangkutan zat radioaktif dan dinyatakan dalam dokumen pengangkutan. Pengangkut adalah orang atau badan yang melakukan pengangkutan zat radioaktif dan penerima adalah orang atau badan yang menerima zat radioaktif dari pengirim dan dinyatakan dalam dokumen pengangkutan.

Aspek keselamatan dan keamanan zat radioaktif dari pengirim sampai dengan penerima merupakan hal yang harus dijamin supaya tidak membahayakan manusia. Pada umumnya pemantauan pengangkutan zat radioaktif dilakukan dengan percakapan melalui komunikasi telepon untuk mengetahui lokasi dan laju paparan zat radioaktif. Masalah keamanan [3] merupakan salah satu aspek terpenting dari sebuah sistem informasi. Dari aspek keamanannya, komunikasi percakapan melalui telepon mudah diinterpretasikan oleh orang lain, disamping itu kemungkinan terjadinya *human-error* cukup tinggi, sehingga timbul ide untuk mengembangkan suatu sistem pemantau pengangkutan zat radioaktif yang lebih aman.

Layanan SMS dikenal mudah dalam hal penggunaan sehingga layanan SMS dapat digunakan sebagai pengganti percakapan melalui komunikasi telepon untuk memantau laju paparan radiasi dan posisi zat radioaktif dalam pengangkutan zat radioaktif. Sistem pemantau pengangkutan zat radioaktif yang akan dikembangkan menggunakan fasilitas SMS (*Short Message Service*) yang tersandi untuk berkomunikasi. Melalui pesan yang tersandi maka informasi posisi dan laju paparan radiasi zat radioaktif tidak mudah diinterpretasikan oleh pihak yang tidak berhak.

Untuk mengirimkan informasi yang aman melalui SMS maka isi SMS perlu disandikan, karena data yang dikirimkan melalui SMS berupa teks sederhana sehingga sangat mudah untuk diketahui isinya oleh orang yang tidak berhak. Penyandian SMS telah banyak dilakukan Ardiyanto pada tahun 2011 [4] mengaplikasikan algoritma Caesar pada SMS berbasis JME. Sebelumnya pada tahun 2010 Nugroho [5] juga telah melakukan modifikasi SMS menggunakan metode vigenere Modifikasi SMS banyak diaplikasikan pada penggunaan mobile phone (handphone) menggunakan pemrograman JAVA.

Pada penelitian ini penyandian SMS dilakukan dengan menggunakan mikrokontroler. ATMega8 sebagai pemroses enkripsi dan deskripsi data lokasi dan laju paparan radiasi. Metode enkripsi dan deskripsi menggunakan algoritma vigenere dengan tabel vigenere numerik desimal sehingga diharapkan informasi yang dikirimkan melalui SMS pada sistem pemantau pengangkutan zat radioaktif menjadi lebih aman.

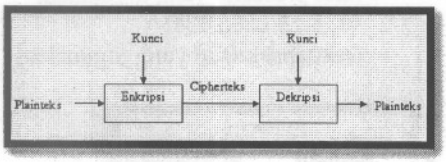
TEORI

Kriptografi

Kriptografi berasal dari bahasa Yunani, yang dalam bahasa Inggris berarti *secret writing*. Kriptografi pada dasarnya sudah ada dan digunakan sejak zaman dahulu. Sejarah mencatat bahwa bangsa Mesir (4000 tahun yang lalu) menggunakan alat yang bernama *hieroglyph* yang tidak standar untuk menulis pesan. Sedangkan di Yunani, kriptografi sudah digunakan 400 BC dan alat yang digunakan pada saat itu bernama *scytale* [6].

Sistem kriptografi (*cryptosystem*) terdiri dari Algoritma kriptografi (*cipher*), *Plainteks* (teks asli), *Ciphertext* (teks terenkripsi) dan Kunci. Algoritma kriptografi (*cipher*) menurut Munir [6]adalah fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan. Pesan itu sendiri adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan tersebut juga dinamakan sebagai *plainteks* (teks asli). Pesan atau

plainteks kemudian diproses oleh sistem kriptografi (*cryptosystem*) untuk dienkripsi atau didekripsi. Jenis pesan atau plainteks yang diproses oleh *cryptosystem* dapat berupa teks, citra, suara, video, basis data dan sebagainya. Enkripsi adalah proses menyandikan teks asli menjadi teks terenkripsi. Sedangkan dekripsi adalah proses mengembalikan cipherteks kembali menjadi plainteks. Berikut ini adalah contoh diagram sistem kriptografi [6].



Gambar 1 Diagram sistem kriptografi [6]

Vigenere *Chiper*

Sandi vigenere adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi caesar berdasarkan huruf-huruf pada kata kunci. Sandi vigenere merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Giovan Batista Belaso menjelaskan metode ini dalam buku *La cifra del. Sig.* Giovan Batista Belaso (1553); dan disempurnakan oleh diplomat Perancis Blaise de Vigenère, pada 1586. Pada abad ke-19, banyak orang yang mengira Vigenère adalah penemu sandi ini, sehingga, sandi ini dikenal luas sebagai " Sandi vigenere " [7].

Tabel 1. Tabel vigenere[7]

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

Sandi vigenere sebenarnya merupakan pengembangan dari sandi caesar. Pada sandi caesar, setiap huruf teks asli digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi caesar dengan geseran 3, A menjadi D, B menjadi E and dan seterusnya. Sandi vigenere terdiri dari beberapa sandi caesar dengan nilai geseran yang berbeda.

Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut Tabel vigenere yang ditunjukkan pada Tabel 1. Tabel vigenere berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang.

Enkripsi (penyandian) dengan sandi vigenere juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$P_i=(C_i-K_i) \bmod 26$

atau

$C_i=(P_i+K_i)-26$

Jika hasil penjumlahan P_i dan K_i lebih dari 26, rumus dekripsi vigenere:

$P_i=(C_i-K_i) \bmod 26$

Dan jika hasil pengurangan C_i dengan K_i minus

$P_i=(C_i-K_i) + 26$

dengan:
C_i = nilai desimal karakter teks terenkripsi ke-i
P_i = nilai desimal karakter teks asli ke-i
K_i = nilai desimal karakter kunci ke-i
Nilai desimal karakter:
A=0 B=1 C=2 ... Z=25

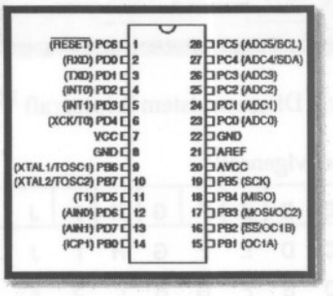
Mikrokontroler ATMega8

Mikrokontroler adalah suatu alat elektronika digital yang mempunyai masukan dan keluaran serta kendali dengan program yang bisa ditulis dan dihapus dengan cara khusus, cara kerja mikrokontroler sebenarnya membaca dan menulis data. Mikrokontroler merupakan sistem komputer yang seluruh atau sebagian besar elemennya dikemas dalam satu chip IC. Mikrokontroler ATMega8 merupakan mikrokontroler keluarga AVR dengan kemampuan yang sangat baik dan harganya relatif murah. Konfigurasi pin mikrokontroler ATMega8 ditunjukkan pada Gambar 2.

Tiga buah timer/counter yang dimiliki oleh mikrokontroler ATMega8 pada penelitian ini digunakan sebagai timer untuk menghitung waktu komputasi pada modul enkriptor dan sebagai counter untuk menghitung banyaknya pulsa yang masuk pada modul monitor radiasi. Perhitungan periode timer1 dirumuskan sebagai berikut [8]:

$$T = \frac{((TCNT_1 + 1)x \text{ Prescaler})}{f_{osc}} \quad (1)$$

dengan :
T = periode (detik)
$TCNT_1$ = nilai register $TCNT_1$ (0-65535)
Prescaler = nilai prescaler yang digunakan (1, 8,16,256,1024)
f_{osc} = frekuensi kristal yang digunakan



Gambar 2. Konfigurasi pin mikrokontroler ATMega8

SMS

SMS adalah suatu fasilitas untuk mengirim dan menerima suatu pesan singkat berupa teks melalui telepon seluler. Salah satu kelebihan SMS adalah biaya yang murah [9]. Selain itu SMS merupakan metode *store* and *forward* sehingga keuntungan yang didapat adalah pada saat telepon seluler penerima tidak dapat dijangkau, tidak aktif atau diluar service area, penerima tetap dapat menerima SMS apabila telepon seluler sudah aktif kembali. Menurut Khang [10], SMS merupakan fitur layanan GSM, dan merupakan teknologi yang memungkinkan pengiriman dan penerimaaan pesan dalam bentuk teks. Data yang dapat dibawa oleh SMS sangat terbatas.

AT-Command

AT-Command adalah sekumpulan perintah yang digunakan untuk berkomunikasi melalui serial port. Dalam hal ini, *AT-Command* merupakan sekumpulan perintah yang menghubungkan antara mikrokontroler dengan modem untuk berkomunikasi menggunakan SMS.

AT Command bertugas mengirim atau menerima data ke atau dari *SMS-Center*. *AT Command* tiap-tiap *SMS device* bisa berbeda-beda, tetapi pada dasarnya sama. Beberapa *AT Command* yang penting untuk SMS yaitu [11]:

• AT+CMGS : untuk mengirim SMS, syntak yang digunakan adalah AT+CMGS="no tujuan" enter

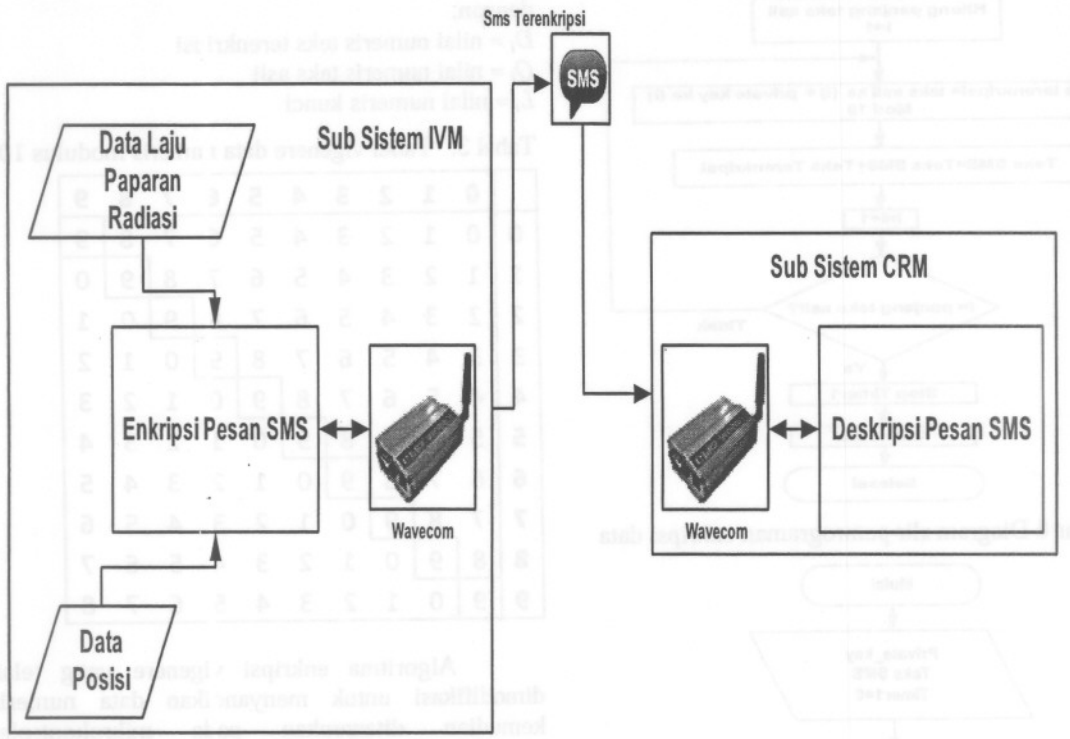
isi pesan control z.

• AT+CMGL : untuk membaca seluruh SMS yang tersimpan, *syntak* yang digunakan adalah AT+CMGL="ALL"

• AT+CMGR : untuk membaca SMS dengan indek tertentu, *syntak* yang digunakan adalah AT+CMGR=indeks SMS.

• AT+CMGD : untuk menghapus SMS, *syntak* yang digunakan adalah AT+CMGD=indeks SMS

Metodologi



Gambar 3. Blok diagram sistem enkripsi dan deskripsi pengiriman SMS pada sistem pemantau pengangkutan zat radioaktif

Blok diagram Implementasi algoritma vigenere menggunakan mikrokontroler untuk pengiriman SMS pada sistem pemantau pengangkutan zat radioaktif ditunjukkan pada Gambar 4.

Sistem pemantau pengangkutan zat radioaktif terdiri dari sub sistem IVM yaitu sub sistem yang terpasang pada kendaraan pengangkut zat radioaktif dan sub sistem CRM yaitu sub sistem yang terpasang pada ruang kendali (ruang monitor).

Proses enkripsi dilakukan pada bagian sub sistem IVM dengan input data laju paparan radiasi dan data posisi, yang kemudian dikirimkan melalui SMS oleh modem wavecom.

Proses deskripsi dilakukan pada bagian sub sistem CRM dengan input berupa SMS terenkripsi yang dikirimkan oleh sub sistem IVM Modul.

Pada penelitian ini data yang akan disandikan adalah data numeris yang meliputi data laju paparan radiasi, data tanggal, data jam dan data posisi, dengan format data yang ditunjukkan pada Tabel 2.

Sehingga algoritma vigenere yang digunakan harus dimodifikasi pada bagian Tabel vigenere karakter alfabet menjadi data numeris. Tabel vigenere data numeris untuk data 0 sampai dengan 9 (modulo 10) ditunjukkan pada Tabel 3.

Tabel 2. Format data yang akan dienkripsi

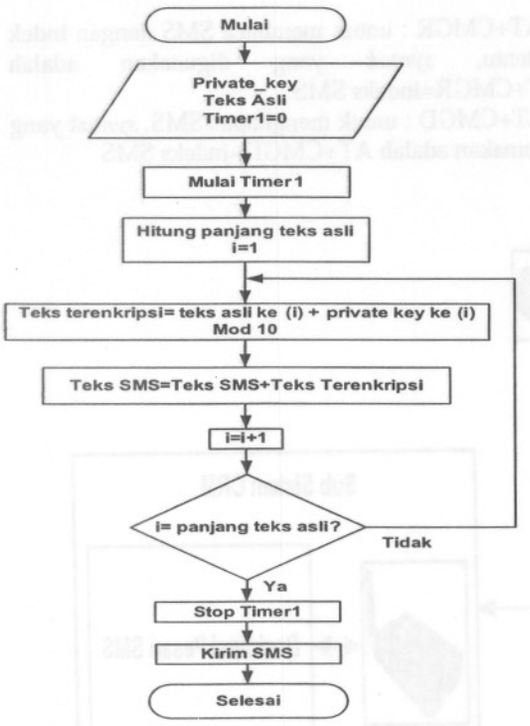
No	Data	Panjang data	Contoh
1	Jam	6 karakter	102530
2	Tanggal	6 karakter	260713
3	Lintang	8 karakter	07466960
4	Bujur	9 karakter	110248605
5	Posisi lintang	2 karaketer	83 untuk Selatan 78 untuk Utara
6	Posisi bujur	2 karakter	69 untuk Timur 87 untuk Barat
7	Laju paparan radiasi	3-4 karakter	011

Penyandian vigenere data numeris modulo 10 secara matematis dirumuskan sebagai berikut:

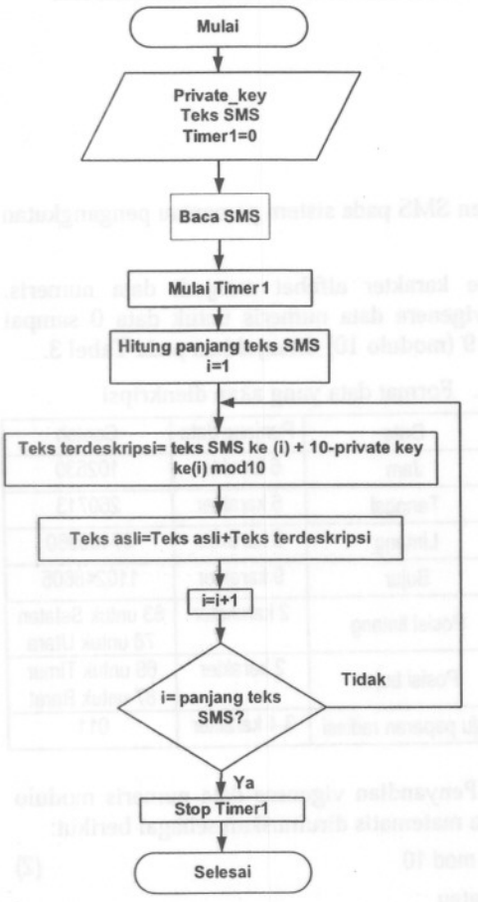
$$Q_i=(D_i-L_i) \bmod 10 \quad (2)$$

atau

$$Q_i=(D_i+L_i)-10 \quad (3)$$



Gambar 6 Diagram alir pemrograman enkripsi data



Gambar 7 Diagram alir pemrograman deskripsi data

Jika hasil penjumlahan Q_i dan L_i lebih dari 10, rumus dekripsi vigenere :

$$Q_i=(D_i-L_i) \bmod 10 \quad (4)$$

Dan jika hasil pengurangan *Di* dengan *Li* minus

$$Q_i=(D_i-L_i) + 10 \quad (5)$$

dengan:
D_i = nilai numeris teks terenkripsi
Q_i = nilai numeris teks asli
L_i = nilai numeris kunci

Tabel 3. Tabel vigenere data numeris modulus 10

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Algoritma enkripsi vigenere yang telah dimodifikasi untuk menyandikan data numeris kemudian ditanamkan pada mikrokontroler pengirim SMS dan mikrokontroler penerima SMS. Diagram alir pemrograman enkripsi dan deskripsi SMS menggunakan mikrokontroler ditunjukkan pada Gambar 6 dan 7. Perhitungan waktu komputasi yang dibutuhkan untuk melakukan enkripsi dan deskripsi menggunakan timer1 yang kemudian dikonversi dalam satuan waktu menggunakan persamaan (1).

Pada penelitian ini *private key* (kunci) yang digunakan adalah 1528400211125623749821539408762486319 yang merupakan sekumpulan karakter data numeris. Kunci tersebut dapat diubah sesuai keinginan pengguna.

Untuk mengetahui unjuk kerja dari implementasi algoritma vigenere menggunakan mikrokontroler untuk mengirimkan SMS pada sistem pemantau pengangkutan zat radioaktif perlu dilakukan pengujian. Pengujian itu terdiri dari:

Pengujian enkripsi pesan dan deskripsi pesan

Pengujian ini perlu dilakukan untuk mengetahui apakah data sebelum dienkripsi dan sesudah enkripsi sama.

Pengujian waktu komputasi enkripsi dan deskripsi

Pengujian ini dilakukan untuk mengetahui berapa waktu yang dibutuhkan oleh mikrokontroler dalam mengenkripsi dan mendeskripsi pesan. Panjang pesan yang akan dienkripsi dan dideskripsi berdasarkan jumlah data laju paparan radiasi, jam, tanggal dan posisi yang berjumlah 37 data.

HASIL DAN PEMBAHASAN

Berdasarkan pengujian yang telah dilakukan didapatkan data pengujian enkripsi pesan dan deskripsi pesan yang disajikan pada Tabel 4.

Tabel 4. Uji enkripsi dan deskripsi pesan dengan *private key* = 152840021112562374982153940876248-6319

No	Teks Asli	Teks Terenkripsi	Teks Terdeskripsi
1.	10253026071307466960110248605836901 1	254370281825536933583255326824507642	10253026071307466960110248605 8369011
2.	10260026071307466960110248605836900 5	254440281825536933583255326824507636	10260026071307466960110248605 8369005
3.	10280226071307466960110248605836900 5	254642281825536933583255326824507636	10280226071307466960110248605 8369005
4.	10285326071307466960110248605836901 1	254693281825536933583255326824507642	10285326071307466960110248605 8369011
5.	10561326071307466697110248528836913 86	257453281825536930853255325054507769 5	10561326071307466697110248528 83691386

Pada pengujian enkripsi dan deskripsi pesan SMS seperti yang terlihat pada Tabel 2, bahwasanya teks asli terdiri dari 36 karakter numeris dan maksimal 37 karakter numeris dapat dienkripsi menggunakan algoritma vigenere dengan kunci 152840021112562374982153940876248 6-319. Teks terenkripsi yang dikirimkan melalui SMS kemudian dideskripsi juga menggunakan algoritma vigenere didapatkan teks asli yang sama persis dengan teks asli sebelum dienkripsi. Sehingga proses enkripsi dan deskripsi pesan SMS yang dilakukan oleh mikrokontroler telah berfungsi dengan baik.

Waktu komputasi yang digunakan oleh mikrokontroler untuk melakukan operasi enkripsi dan deskripsi pesan ditunjukkan pada Tabel 5 dan Tabel 6

Tabel 5. Waktu komputasi enkripsi dan deskripsi 36 karakter numeris

No	Waktu komputasi enkripsi (ms)	Waktu komputasi deskripsi (ms)
1	13,05	13,05
2	13,05	13,05
3	13,05	13,05
4	13,05	13,05
5	13,05	13,05
6	13,05	13,05
7	13,05	13,05
8	13,05	13,05
9	13,05	13,05
10	13,05	13,05

Pada Tabel 5 dan Tabel 6 ditunjukkan bahwa waktu komputasi yang diperlukan untuk enkripsi dan deskripsi adalah sama yaitu untuk 36 karakter numeris diperlukan waktu 13,05 ms dan untuk 37 karakter numeris diperlukan 13,61 ms jadi untuk setiap satu karakter numeris dapat dihitung sebagai berikut:

$$waktu\ komputasi\ 1\ karakter = 13{,}61 - 13{,}05$$
$$= 0{,}56\ \text{ms}$$

Tabel 6. Waktu komputasi enkripsi dan deskripsi 37 karakter numeris

No	Waktu komputasi enkripsi	Waktu komputasi deskripsi
1	13,61	13,61
2	13,61	13,61
3	13,61	13,61
4	13,61	13,61
5	13,61	13,61
6	13,61	13,61
7	13,61	13,61
8	13,61	13,61
9	13,61	13,61
10	13,61	13,61

KESIMPULAN

Dari hasil pengujian didapatkan kesimpulan sebagai berikut:

1. Algoritma enkripsi vigenere berhasil diaplikasikan untuk mengenkripsi dan mendeskripsikan pesan SMS menggunakan mikrokontroler pada sistem pemantau pengangkutan zat radioaktif.

2. Waktu komputasi yang diperlukan untuk mengenkripsi dan mendeskripsi pesan adalah 13,05 ms untuk data 36 karakter dan 13,61 ms untuk 37 karakter, sehingga untuk 1 karakter diperlukan waktu komputasi 0,56 ms.

UCAPAN TERIMAKASIH

Diucapkan terimakasih kepada Bpk. I Wayan Mustika dan Ibu Litasari dari UGM atas masukan dan bantuan pengembangan algoritma vigenere serta saudari Dwi Yuliansari dari Balai Elektromekanik PTAPB atas bantuan perancangan dan pembuatan perangkat keras.

DAFTAR PUSTAKA

1. ***Undang Undang Ketenaganukliran No 10/1997*** *Tentang Ketenaganukliran Pasal 1 Ayat 9*, 10, 1997.
2. **BAPETEN. (4 Juni 2013)**. *Petunjuk Pengisian Formulir Persetujuan Pengiriman Zat Radioaktif*. Available: http://www.bapeten.go.id/download.php?fid=344&filename=Petunjuk_Pengisian_Formulir_Persetujuan_Pengiriman.doc&target=document.
3. **D. Ariyus**, *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi*. Yogyakarta: Andi Offset, 2008.
4. **Ardiyanto**, "Implementasi Algoritma Kriptografi Caesar Chiper Pada Aplikasi SMS Telepon Selular Berbasis J2ME," S1, Jurusan Teknik Informatika AMIKOM, Yogyakarta, 2011.
5. **B. K. Nugroho**, "Aplikasi Enkripsi SMS Pada Telepon Seluler Berbasis J2ME Dengan Metode Vigenere Cipher," S1, Program Studi Teknik Informatika Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Diponegoro, Semarang, 2010.
6. **R. Munir. (2010, 12 Maret 2012)**. *Pengantar Kriptografi*. Available: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Pengantar%20Kriptografi.ppt
7. **Anonim, (2012, 29 April 2012)**. *Sandi Vigenère*. Available: http://id.wikipedia.org/wiki/Sandi_Vigen%C3%A8re
8. **C. Kuhnel**, *BASCOM Programming of Microcontrollers with Ease: An Introduction by Program Examples*. USA: Universal Publishers/uPUBLISH.com, 2001.
9. **A. Ibrahim**, "Pengembangan Sistem Informasi Monitoring Tugas Akhir Berbasis Short Massage Service (SMS) Gateway di Fasilkom Unsri," *JUSI* vol. I, 2011.
10. **B. Khang**, *Trik Pemrograman Aplikasi Berbasis SMS*: Elex Media Komputindo, 2002.
11. **Ismail**. (2010, 29 April 2012). *Perancangan Sistem Pelayanan Pemesanan Nomor Antrian Online Melalui SMS Berbasis Mikrokontroler*. Available: http://elib.unikom.ac.id/files/disk-1/395/jbptunikompp-gdl-ismailnim1-19709-9-babii.pdf

Tanya Jawab

Kussigit Santoso

- Apakah ada error deteksinya?
- Bagaimana cara melakukan error deteksinya ?
- Komunikasi sms menggunakan apa ?

Adi Abimanyu

- *Ada.*
- *Menggunakan panjang data yang dikirimkan.*
- *Menggunakan modem WAVECOM dengan perubah AT-COMMAND.*

Agus Taftazani

- Berapa dana yang dibutuhkan untuk membuat alat tersebut ?
- Apakah modem dapat digantikan menggunakan *handphone* ?
- Kenapa harus dilakukan enkripsi ?

Adi Abimanyu

- *Tidak sampai 1 juta rupiah*
- *Dapat*
- *Agar informasi yang dikirimkan melalui sms tidak dapat dengan mudah dipahami oleh orang yang tidak berhak.*