

**IMPLEMENTASI ALGORITMA ENKRIPSI DENGAN METODE
MODIFIKASI *VIGENERE CIPHER* DALAM APLIKASI PENGIRIMAN
SMS PADA PONSEL *BLACKBERRY***

SKRIPSI



disusun oleh

Dyan Hari Widodo

07.11.1471

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2011**

**IMPLEMENTASI ALGORITMA ENKRIPSI DENGAN METODE
MODIFIKASI *VIGENERE CIPHER* DALAM APLIKASI PENGIRIMAN
SMS PADA PONSEL *BLACKBERRY***

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Dyan Hari Widodo

07.11.1471

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2011**

PERSETUJUAN

SKRIPSI

**Implementasi Algoritma Enkripsi Dengan Metode Modifikasi Vigenere
Cipher dalam Aplikasi Pengiriman SMS Pada Ponsel Blackberry**

yang dipersiapkan dan disusun oleh

Dyan Hari Widodo

07.11.1471

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 2 Februari 2011

Dosen Pembimbing,

Ema Utami, Dr., S.Si, M.Kom

NIK. 190302037

PENGESAHAN

SKRIPSI

**Implementasi Algoritma Enkripsi Dengan Metode Modifikasi Vigenere
Cipher dalam Aplikasi Pengiriman SMS Pada Ponsel Blackberry**

yang dipersiapkan dan disusun oleh

Dyan Hari Widodo

07.11.1471

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Februari 2011

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

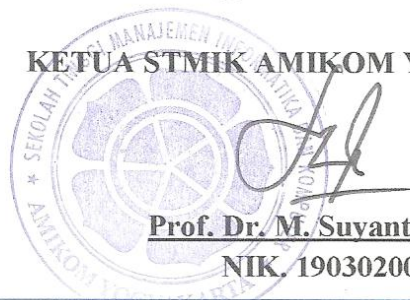
Ema Utami, Dr., S.Si, M.Kom
NIK. 190302037

Emha Taufiq Lutfhi, ST, M.Kom
NIK. 190302125

Kusrini, Dr., M.Kom
NIK. 190302098

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 Februari 2011

KETUA STMIK AMIKOM YOGYAKARTA



Prof. Dr. M. Suvanto, MM.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 2 Februari 2011



Dyan Hari Widodo

07.11.1471

HALAMAN PERSEMBAHAN

Thanks To :

- Allah SWT atas pembelajarannya yang diberikan pada hambaMu ini, dan ampunilah hambaMu ini yang “ terkadang harus memilih jalan yang salah untuk menemukan suatu kebenaran “. Atas petunjuk serta rahmat dan ridloMu-lah saya dapat menyelesaikan skripsi ini dengan lancar dan tanpa hambatan yang berarti.
- Kedua orangtua saya, Bapak Tejo dan Ibuk Hartini tercinta, terimakasih banyak atas doa, semangat dan semua yang telah diberikan kepadaku, tanpa kalian saya tidak akan seperti ini. Terutama bagi ibuk Hartini, terimakasih banyak atas kasih sayang, perhatian, dan bimbingan yang engkau berikan kepada saya, semoga mendapatkan balasan dari Allah SWT.
- Keluarga dan saudara-saudara saya, Eyang Sis Jumali , Eyang Sugirah (Alm), Bulek Mamik , Pakdhe Manto, Budhe Sri, Mas Don, Mbak Novi, dan semua keluarga dan saudara-saudaraku yang telah memberikan banyak motivasi bagi saya.
- Keluarga Bapak Joko, Ibuk Erly, Qiqi, Dek Ucha, Dek Utha, Dek Bagas terimakasih atas do'a, dukungan, semangat yang telah diberikan kepada saya. Spesial untuk Rizqya Syura Esvandiary yang telah banyak memberikan motivasi dan waktunya untuk menemani saya menyelesaikan skripsi ini.
- Ibu Ema Utami, S.Si, M.Kom selaku Dosen Pembimbing, yang telah banyak meluangkan waktu untuk membimbing dan mengarahkan sehingga skripsi ini dapat terselesaikan.
- Bapak Dony Ariyus, M.Kom yang telah banyak memberikan banyak pengetahuan tentang ilmu Kriptografi.
- Sahabat-sahabat terbaikku disaat suka dan duka WANTED Crew: Rezky Kurniawan Hutabarat, Bagus Paripurna, Sidik Cahya

Hidayat, Rony Bachtiar Effendi, Guntur Susilo Putra, Gubtha Mahendra Putra, Fuaddani Septian Suryana, Risky Adi Nugoho, Muhammad Arsyi, Sugeng Triyono, Jamal Abdul Naser, Syarifah Shinta Paramita Dewi Alqadri, Rizqya Syura Esvandiary, Lailiy Shofa, Putri Zainal, Nadia Helena Nelwan.

- Prastian dan Halimah, terimakasih atas partisipasinya meminjamkan ponsel Blackberry nya untuk uji coba sewaktu pendadaran.
- Kawan-kawan kelas S1-TI-B 2007, setelah lebih kurang 4 tahun kita bersama, akhirnya kita berpisah juga kawan, semoga persahabatan kita tetap abadi.
- Serta berbagai pihak yang tidak bisa penulis sebutkan satu persatu, Terimakasih untuk semuanya.

Saya harap halaman persembahan ini cukup dapat menyampaikan rasa terimakasih yang sangat dalam dari penulis untuk semua yang telah membantu dalam menyelesaikan skripsi dan yang telah mengisi hari-hari penulis dalam menempuh kuliah.

Penulis

Dyan Hari Widodo

HALAMAN MOTTO

- ❖ *“ Jika ada niat dan kemauan , kita pasti bisa “*
- ❖ *“ Hinaan orang = motivasi “*
- ❖ *“ Dimana ada jalan disitu ada peluang “*
- ❖ *“ Ibarat nasi sudah jadi bubur, yang sudah berlalu biarlah berlalu, saatnya benahi diri tuk jadi yang lebih baik “*
- ❖ *“ Hal pertama untuk menjadi seorang pemimpin adalah dengan menjadi pelayan “ (John C.Maxwell)*
- ❖ *“ Sukses itu tergantung usaha “ (Sophocles)*
- ❖ *“ Kekalahan bukanlah kegagalan yang terburuk, tidak mencoba adalah kegagalan sejati “ (George Edward Woodberry)*
- ❖ *“ Buat masa depan anda dengan masa depan, bukan dari masa lalu “ (Werner Erhard)*
- ❖ *“ Mendapatkan kepercayaan adalah pujian yang lebih besar daripada dicintai “ (George McDonald)*

KATA PENGANTAR

Alhamdulillah, puji syukur kehadirat Allah SWT atas limpahan rahmat dan kemudahan-Nya sehingga penulis dapat menyelesaikan laporan skripsi dengan judul Implementasi Algoritma Enkripsi Dengan Metode Modifikasi *Vigenere Cipher* Dalam Aplikasi Pengiriman SMS Pada Ponsel *Blackberry*.

Penulisan Laporan ini dimaksudkan untuk melengkapi salah satu syarat dalam menyelesaikan studi di Jurusan Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer “AMIKOM” Yogyakarta.

Dalam proses penyusunan dan penulisan skripsi, penulis menyadari bahwa kemampuan penulis terbatas. Oleh karena itu, penulis menyampaikan terimakasih kepada pihak-pihak yang turut terlibat dari awal proses hingga akhir, antara lain:

1. Bapak Prof.Dr.M.Suyanto,MM selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Bapak Ir.Abas Ali Pangera,M.Kom selaku Ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ibu Ema Utami, S.Si, M.Kom selaku Dosen Pembimbing, yang telah banyak meluangkan waktu untuk membimbing dan mengarahkan sehingga skripsi ini dapat terselesaikan.
4. Bapak Emha Taufiq Lutfhi, ST, M.Kom dan Ibu Khusrini, Dr., M.Kom selaku Dosen Penguji, terimakasih atas saran dan kritiknya yang merupakan langkah awal penyempurnaan skripsi ini.

5. Seluruh Dosen STMIK AMIKOM Yogyakarta yang telah memberikan ilmunya pada penulis.
6. Semua pihak yang telah memberikan bantuan kepada penulis yang tidak dapat penulis sebutkan satu persatu.

Penulis sadar bahwa dalam penyusunan laporan skripsi ini masih banyak yang perlu dikoreksi lebih lanjut, maka penulis dengan senang hati menerima kritik dan saran demi perbaikan selanjutnya. Semoga laporan ini dapat berperan sebagaimana mestinya.

Yogyakarta, 2 Februari 2011

Penulis

Dyan Hari Widodo

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
PENYATAAN KEASLIAN.....	iv
HALAMAN PERSEMBAHAN.....	v
MOTTO.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR.....	xv
DAFTAR LAMPIRAN.....	xvii
INTISARI.....	xviii
ABSTRAKSI.....	xix
BAB I. PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah.....	5
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	6
1.6 Metode Penelitian.....	6
1.7 Sistematika Penulisan Laporan.....	8

1.8 Jadwal Penelitian.....	10
BAB II. LANDASAN TEORI.....	11
2.1 Tinjauan Pustaka	11
2.1.1 Kesimpulan	17
2.2 Kriptografi.....	18
2.2.1 Pengertian Kriptografi.....	18
2.2.2 Macam-macam Kriptografi.....	19
2.2.2.1 Kriptografi Klasik	19
2.2.2.2 Kriptografi Modern	20
2.2.3 Macam-macam Algoritma Kriptografi	20
2.2.3.1 Algoritma Simetri	20
2.2.3.2 Algoritma Asimetri	22
2.2.3.3 Fungsi Hash.....	23
2.2.4 Tujuan Kriptografi	23
2.2.5 Jenis-jenis Serangan Terhadap Kriptografi.....	25
2.2.6 Keamanan Algoritma Kriptografi	25
2.3 Vigenere Cipher	25
2.3.1 Kelebihan dan kekurangan Kode Vigenere.....	36
2.4 Metode Kasiski	37
2.5 Modifikasi Vigenere Cipher.....	38
2.5.1 Bagan Alir Kerja Enkripsi Keseluruhan	42
2.6 Perangkat Lunak Yang Digunakan	45
2.6.1 Java.....	45

2.6.2 Eclipse Galileo	45
2.6.3 <i>Code Signing Blackberry</i>	47
BAB III. ANALISA DAN PERANCANGAN SISTEM	49
3.1 Analisa Perancangan Sistem	49
3.1.1 Kebutuhan Perangkat Lunak	49
3.1.2 Strategi Perancangan Perangkat Lunak.....	50
3.1.3 Deskripsi Perangkat Lunak	51
3.2 Perancangan Sistem	52
3.2.1 Flowchart Sistem.....	53
3.2.1.1 Bagan Alir Sistem	53
3.2.1.2 Pseudocode Program Enkripsi dan Dekripsi.....	56
3.2.2 Diagram Arus Data Sistem / <i>Data Flow Diagram</i> (DFD).....	61
3.2.2.1 Diagram Konteks (<i>context diagram</i>).....	61
3.2.2.2 <i>Data Flow Diagram</i>	62
3.3 Perancangan Antar Muka.....	65
3.4 Perancangan Script Program	68
3.4.1 Script Enkripsi dan Dekripsi	68
3.4.1.1 Enkripsi Vigenere.....	68
3.4.1.2 Dekripsi Vigenere	69
3.4.1.3 Enkripsi ADVC.....	70
3.4.1.4 Dekripsi ADVC.....	70
3.4.1.5 Enkripsi pada Kunci	71
3.4.1.6 Enkripsi Substitusi	72

3.4.1.7 Dekripsi Substitusi	72
BAB IV. UJI COBA SISTEM.....	74
4.1 Tujuan Uji Coba Sistem	74
4.1.1 Pengujian Aplikasi	75
4.1.1.1 Mengaktifkan Menu <i>Encrypt</i> Dan <i>Decrypt</i> Pada Aplikasi SMS <i>Blackberry</i>	75
4.1.1.2 Pengiriman dan Penerimaan Pesan Teks.....	76
4.1.2 Uji Coba Operator dan Handphone.....	81
4.1.3 Pengujian Aplikasi dengan Implementasi	82
4.1.4 Pengujian Pada Telepon Seluler	84
4.2 Hasil Pengujian	86
4.3 Pembahasan dan Pengujian Enkripsi Dekripsi ADVC	86
4.3.1 Pembahasan Enkripsi ADVC.....	87
4.3.2 Pembahasan Dekripsi ADVC.....	99
4.3.3 Pengujian Algoritma ADVC	103
BAB V. PENUTUP.....	104
5.1 Kesimpulan	104
5.2 Saran.....	105
DAFTAR PUSTAKA.....	106
LAMPIRAN.....	108
Kode ASCII.....	108
Script Program Enkripsi	109
Script Program Dekripsi.....	113

DAFTAR TABEL

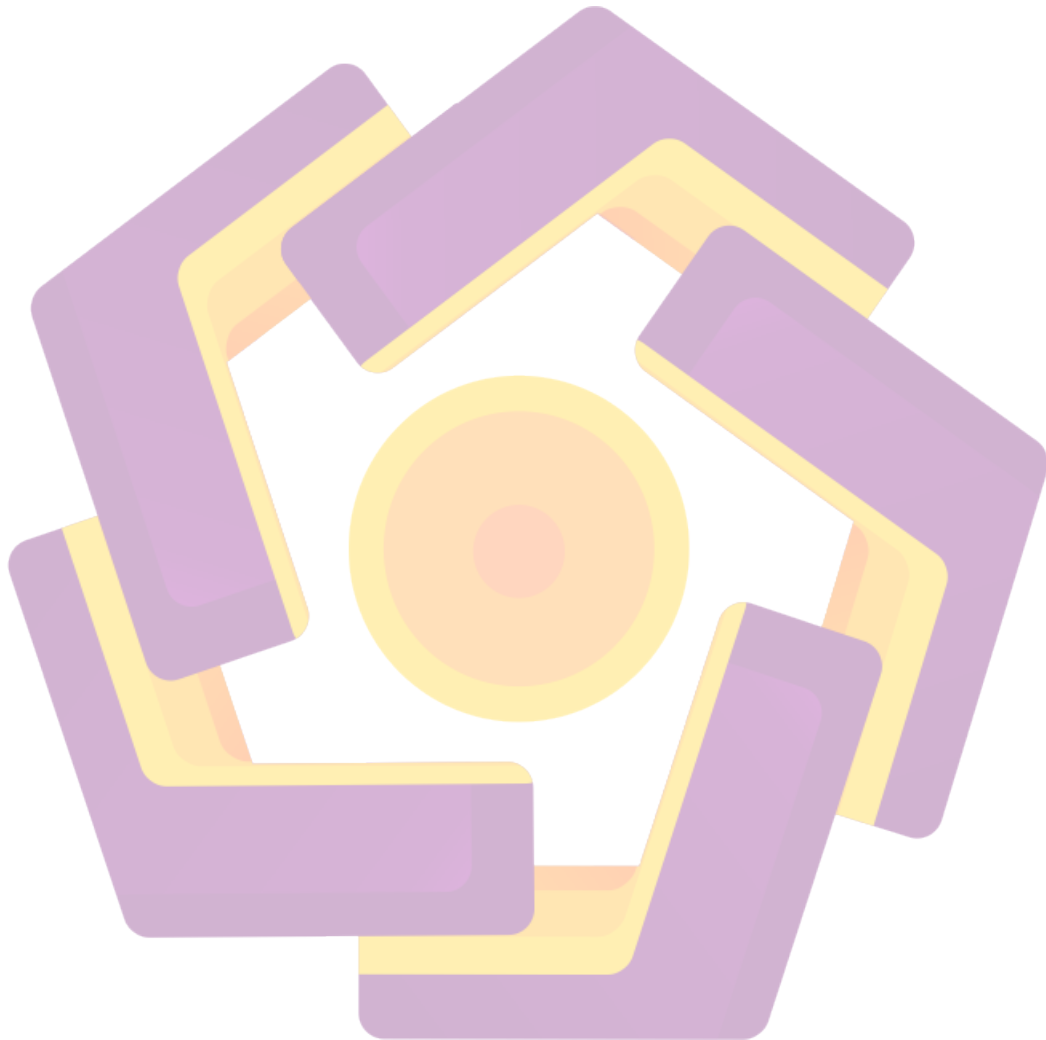
	Halaman
Tabel 1.1 Tabel Jadwal Penelitian	10
Tabel 2.4 Tabel Bujursangkar <i>Vigenere</i>	32
Tabel 2.5 Tabel Enkripsi huruf T dengan kunci H	34
Tabel 2.6 Tabel Proses untuk mencari plainteks dari cipherteks huruf A dan H.....	36
Tabel 2.7 Tabel karakter atau simbol di ponsel Qwerty <i>Blackberry</i>	41
Tabel 2.8 Proses Substitusi tabel simbol di ponsel Qwerty <i>Blackberry</i>	41
Tabel 3.2 Pseudocode Enkripsi dan Dekripsi <i>Vigenere</i> Cipher	56
Tabel 3.3 Pseudocode Enkripsi dan Dekripsi <i>ADVC</i>	58
Tabel 3.4 Pseudocode Enkripsi dan Dekripsi pada Substitusi	59
Tabel 3.5 Pseudocode Enkripsi pada Kunci	60
Tabel 4.12 tabel lingkungan pengujian	84
Tabel 4.13 tabel implementasi pada ponsel <i>Blackberry OS</i>	85
Tabel 4.14 Tabel karakter atau simbol di ponsel Qwerty <i>Blackberry</i>	98
Tabel 4.15 Proses Substitusi tabel simbol di ponsel Qwerty <i>Blackberry</i>	98
Tabel 4.16 Proses Substitusi tabel simbol di ponsel Qwerty <i>Blackberry</i>	99

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Skema proses enkripsi dan dekripsi	19
Gambar 2.2 Skema Algoritma kriptografi kunci simetri	21
Gambar 2.3 Skema Algoritma kriptografi kunci Asimetri	22
Gambar 2.9 Bagan Enkripsi hasil dari modifikasi Vigenere Cipher	43
Gambar 2.10 Bagan Dekripsi hasil dari modifikasi Vigenere Cipher.....	44
Gambar 3.1 Flowchart Sistem SMSlockcrypt	55
Gambar 3.6 DCD level 0 Aplikasi Perangkat Lunak SMSlockcrypt	61
Gambar 3.7 DCD level 1 Aplikasi Perangkat Lunak SMSlockcrypt	63
Gambar 3.8 Rancangan <i>Form</i> About.....	66
Gambar 3.9 Rancangan <i>Form</i> Encrypt SMS	66
Gambar 3.10 Rancangan <i>Form</i> Decrypt SMS.....	67
Gambar 4.1 Tampilan Menu About.....	75
Gambar 4.2 Menu <i>Encrypt</i> dan <i>Decrypt</i> pada aplikasi SMS <i>Blackberry</i>	76
Gambar 4.3 Proses pengiriman pesan teks biasa	76
Gambar 4.4 Proses penerimaan pesan teks biasa	77
Gambar 4.5 Proses penulisan enkripsi pesan teks.....	78
Gambar 4.6 Proses pengiriman enkripsi pesan teks	78
Gambar 4.7 Notifikasi enkripsi pesan teks sudah terkirim.....	79
Gambar 4.8 Proses penerimaan enkripsi pesan teks	79
Gambar 4.9 Tampilan notifikasi bukan ciphertext	80

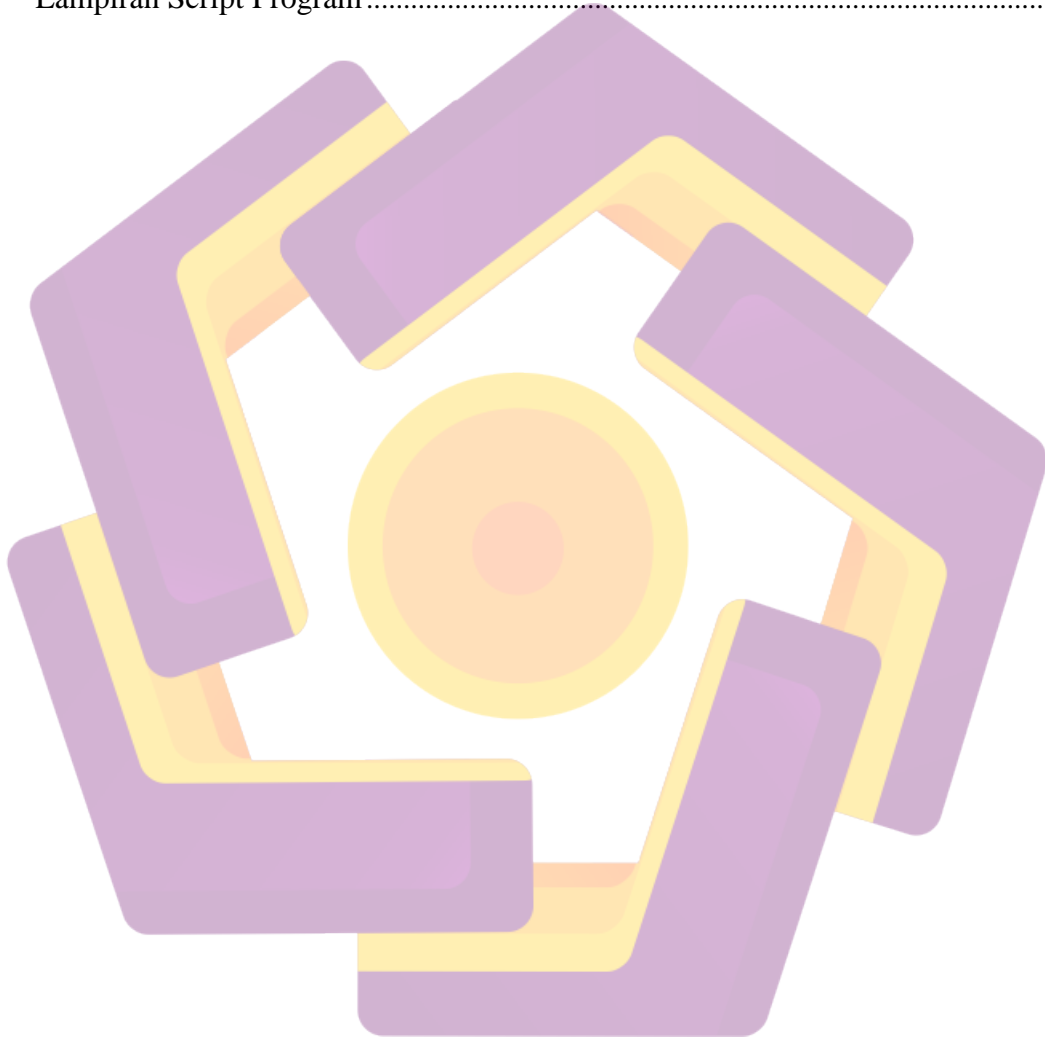
Gambar 4.10 Proses dekripsi menggunakan key yang salah..... 80

Gambar 4.11 Proses dekripsi pesan teks 81



DAFTAR LAMPIRAN

	Halaman
Lampiran Kode ASCII.....	108
Lampiran Script Program.....	109



INTISARI

Saat ini pengguna *BlackBerry* terus meningkat jumlahnya, terutama di pasar Indonesia. Hal ini tidak lepas karena kecanggihan teknologi koneksi internet dan berbagai banyak macam aplikasi yang disediakan *BlackBerry* itu sendiri, sehingga banyak pengguna yang puas ketika menggunakan *BlackBerry*. Tentunya koneksi terus-menerus ini harus mendapat pengamanan khusus, apalagi jika terdapat data penting yang hendak dikirim atau diterima.

Teknologi SMS sampai hari ini tetap menjadi media komunikasi yang populer oleh masyarakat, selain mudah digunakan biayanya juga lebih murah. Tapi di sisi lain dari teknologi SMS juga memiliki kelemahan. Teknologi SMS tidak menjamin keamanan dan kerahasiaan pesan yang dikirim. Beberapa risiko juga merupakan ancaman bagi keamanan termasuk spoofing SMS, SMS mengintai, dan intersepsi SMS. Dari beberapa ancaman terhadap risiko seperti pesan SMS, maka perlu untuk membangun sebuah aplikasi yang mampu mengamankan dan menyimpan pesan SMS rahasia, sehingga dalam hal terjadi ancaman dan pesan yang dibuka, isi pesan tetap rahasia. Salah satu solusi untuk mengamankan dan menjaga pesan untuk mengenkripsi pesan SMS sebelum pengiriman.

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang menerapkan suatu metode cipher substitusi abjad majemuk. Algoritma ini sudah dapat dipecahkan melalui metode Kasiski, maka sebab itu dilakukanlah modifikasi agar algoritma yang baru lebih sulit untuk dipecahkan dengan metode tersebut.

Kata kunci: SMS, Enkripsi, Dekripsi, *BlackBerry*, *Vigenere Cipher*

ABSTRACT

Currently BlackBerry users continues to increase, especially in the Indonesian market. This is not out because of technological sophistication of Internet connections and many many kinds of applications that provided the BlackBerry itself, so that many users are satisfied when using a BlackBerry. Obviously this constant connection should receive special protection, especially if there are important data that would be sent or received.

SMS technology to this day remains a popular communication media by the public, in addition to easy to use cost is also cheaper. But on the other side of the SMS technology also has its disadvantages. SMS technology does not guarantee the security and confidentiality of messages sent. Some risks are also a threat to the security including SMS spoofing, SMS spy, and SMS interception. Of the several threats against risks such as SMS messages, it is necessary to build an application that is able to secure and keep confidential SMS messages, so that in the event of a threat and that message is opened, the contents of the message remain confidential. One solution to secure and maintain the message to encrypt the message before sending.

Vigenere cipher is a classical cryptographic algorithm which employs an alphabet substitution cipher method compound. This algorithm has to be solved through the method Kasiski, then why perform the modification for the new algorithm is more difficult to be solved with such methods.

Keywords: SMS, Encryption, Decryption, BlackBerry, Vigenere Cipher