Penerapan Kode Huffman dan Kriptografi pada Teknologi SMS

M.Auriga Herdinantio – NIM 13506056
Teknik Informatika Institut Teknologi Bandung, email:if16056@students.if.itb.ac.id

Abstract – *Komunikasi memiliki peranan penting dalam kehidupan sosial saat ini. Dalam berkomunikasi pesan teks merupakan sarana yang sering digunakan selain layanan suara. Salah satu cara berkomunikasi menggunakan pesan teks adalah SMS. Secara umum SMS tidak menjamin kerahasiaan dan keutuhan pesan yang dikirimkan oleh pengguna. Oleh karena pesan-pesan teks yang dikirim pengguna terkadang merupakan pesan yang rahasia dan pribadi, sehingga kerahasiaan pesan menjadi sangat penting untuk dijaga dari orang-orang yang tidak berhak mendapatkannya, sehingga dibutuhkan suatu sistem keamanan dalam menyampaikan pesan tersebut. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Selain itu karena masalah keterbatasan memori, maka dibutuhkan sebuah mekanisme pengamanan yang unik dalam menangani permasalahan tersebut agar besar data yang ditransmisikan diusahakan seminimal mungkin dan tetap menjaga kerahasiaanya. Kode Huffman adalah solusi untuk masalah tersebut. Makalah ini membahas tentang penerapan kode Huffman dan kriptografi dalam teknologi sms. Kode Huffman digunakan pada aplikasi penghemat sms sedangkan metode kriptografi digunakan pada aplikasi sms rahasia.*

Kata Kunci: *komunikasi, sms, kode Huffman, kriptografi.*

1. PENDAHULUAN

Saat ini, perkembangan teknologi sangat pesat. Begitu pula dengan teknologi informasi. Orang dapat dengan mudah dan cepat saling bertukar informasi , sehingga secara mudah bisa mengetahui apa yang terjadi di belahan bumi yang lain.

Ada bermacam-macam cara berkomunikasi, bisa lewat telepon, fasimile, e-mail dan masih banyak lagi yang lainnya.

Salah satu cara yang digemari orang saat ini adalah teknologi sms, selain karena tarifnya yang murah cara penggunaannya pun mudah. Dengan mengetikan pesan kepada orang yang diinginkan dan mengirimkannya, mereka sudah bisa berkomunikasi.

Namun penggunaan teknologi ini pun masih memiliki kekurangan. Salah satunya adalah apabila kita ingin mengirimkan pesan melebihi jumlah karakter yang telah ditentukan oleh ponsel yang kita punya, kita harus membayar tarif yang lebih. Hal tersebut kadang menjengkelkan, karena kelebihan tersebut biasanya hanya beberapa karakter saja.

Cara yang paling sering dilakukan untuk mengatasinya adalah dengan menggunakan singkatan-singkatan yang umum dipakai. Meski demikian, seringkali kita harus menyerah karena hampir semua kata mungkin sudah kita singkat, namun jumlah pesan yang telah kita ketikkan tetap melebihi karakter yang telah ditentukan.

Kekurangan yang lainnya adalah apabila sang pengirim ingin pesan tersebut hanya bisa dibuka atau dibaca kembali oleh pembaca tertentu yang memiliki kuncinya sesuai dengan keinginan sang pengirim.

Oleh karena itu, pada kesempatan kali ini, penulis akan memaparkan penggunaan kode Huffman dan teknik kriptografi untuk mengatasi kekurangan-kekurangan tersebut.

2. APLIKASI PENGHEMAT SMS

Pesan yang dikirim saat berkomunikasi seringkali berukuran terlalu besar sehingga memerlukan waktu yang lama. Selain itu dalam penyimpanan data, file yang cukup besar memakan ruang yang besar.

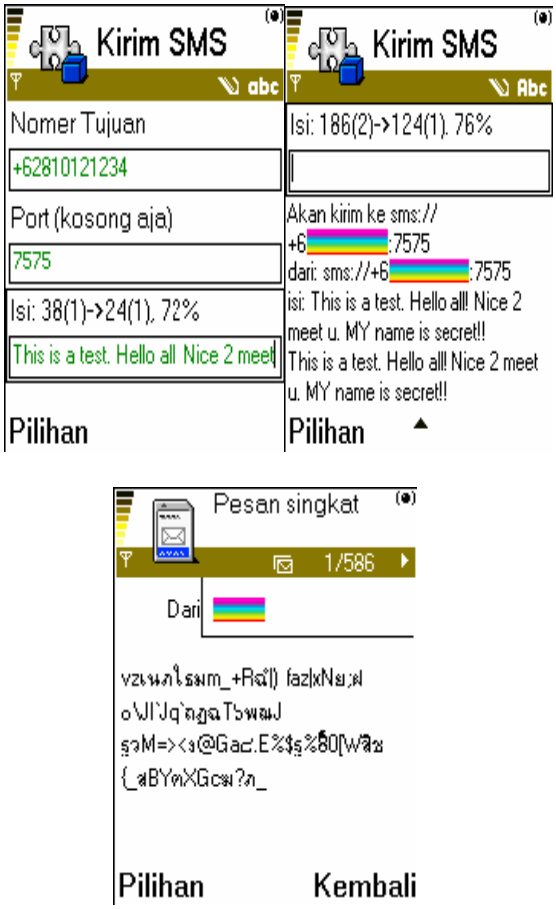
Masalah–masalah tersebut dapat diatasi dengan mengkodekan pesan atau isi arsip sesingkat mungkin, sehingga waktu dan ruang yang digunakan dapat seminimal mengkin.

Salah satu metode yang biasa digunakan pada metode kompresi data adalah kode Huffman. Pada aplikasi penghemat sms, kode Huffman digunakan untuk mengurang jumlah bit yang digunakan

Selain Huffman, beberapa teknik kompresi yang populer seperti LZ dapat pula digunakan. Dalam aplikasi SMS Zipper, digunakan metode kompresi yang khusus. Teknik kompresinya disusun oleh S. Rein, C. Guehmann, dan F.H.P. Fitzek yang dipublikasikan melalui jurnal bergengsi IEEE Data Compression Conference (DCC), IEEE Computer Society Press. Snowbird, UT berjudul “Low Complexity Compression of Short Messages” tahun 2006.

Aplikasi ini dibuat oleh para *programmer* dari universitas Aalborg, Denmark. Aplikasi ini istimewa

disamping karena teknik kompresinya yang luar biasa sehingga mempu meng-kompresi hingga 50%, aplikasinya juga tersedia dalam berbagai bahasa baik versi Java maupun Symbian. Namun untuk membacanya, tetap membutuhkan aplikasi khusus.



Gambar 1: Tampilan aplikasi Penghemat SMS

3. APLIKASI SMS RAHASIA

Kriptografi (*cryptography*) adalah proses menjaga keamanan informasi yang dikirim melalui jaringan publik dengan enkripsi yang membuat informasi tidak dapat dibaca oleh orang yang tidak mempunyai *key* untuk mendeskripsinya.

Kriptografi merupakan salah satu teknik untuk mengubah sebuah data agar hanya penerima yang berhak yang dapat membaca data tersebut.

Pada metode vigenere cipher, karakter plaintext dibagi sesuai dengan karakter kunci. Masing-masing karakter diubah ke dalam angka yang menunjukkan indeks karakter tersebut dalam abjad (indeks tersebut bisa dibuat secara acak sehingga sulit untuk menebaknya). Angka dari plaintext dijumlah dengan angka dari kunci dan hasilnya diubah kembali menjadi karakter-karakter sehingga menjadi ciphertext-nya.

Metode ini tergolong aman dan cukup sederhana sehingga tidak akan membebani ponsel karena prosesnya yang sederhana. Aplikasi ini menggunkan bahasa pemrograman J2ME(Java 2 MicroEdition) sehingga hanya dapat digunakan pada ponsel yang mendukung Java.

Adapun arsitektur teknologi J2ME meliputi konfigurasi dan profil. Konfigurasi merupakan bagian yang berisi JVM dan library. Terdapat kofigurasi yang disediakan untuk alat-alat kecil seperti ponsel dan PDA, yaitu CLDC (*Connected Limited Device Configuration*). Profil menyediakan kelas-kelas yang tidak terdapat pada level konfigurasi. Profil yang sering digunakan adalah MIDP (*Mobile Information Device Profile*). Kofigurasi dan profil telah disediakan oleh perusahaan pembuat alat dan telah diletakkan pada ponsel tersebut.

Aplikasi ini tidak melibatkan masalah jaringan dan dibuat untuk mengamankan isi pesan yang bersifat rahasia/penting, seperti pengiriman PIN, transaksi keuangan yang bersifat rahasia, rahasia perusahaan/negara/perseorangan lewat SMS. Selain itu, dengan menggunakan aplikasi ini, SMS yang akan terbaca di provider adalah ciphertext-nya, atau jika salah memasukkan nomor tujuan maka SMS tidak akan dimengerti oleh orang yang menerima pesan.

Penyelesaiannya adalah sebagai berikut, sebelum melakukan pengiriman SMS atau penerimaan SMS terenkripsi, aplikasi ini sudah harus terpasang di kedua belah pihak (ponsel pengirim dan hanphone penerima). Sebelum user mengirimkan SMS, SMS (sebagai plaintext) tersebut akan dibaca, kemudian dienkripsi dengan menggunakan aplikasi yang sudah terpasang pada ponsel pengirim sehingga SMS tersebut akan menjadi ciphertext. Kemudian SMS (ciphertext) tersebut barulah dikirim. Setelah SMS sampai ke ponsel penerima, SMS (ciphertext) tersebut akan dibaca, kemudian didekripsi dengan menggunakan aplikasi yang sama yang ada pada ponsel penerima sehingga kembali menjadi pesan aslinya.

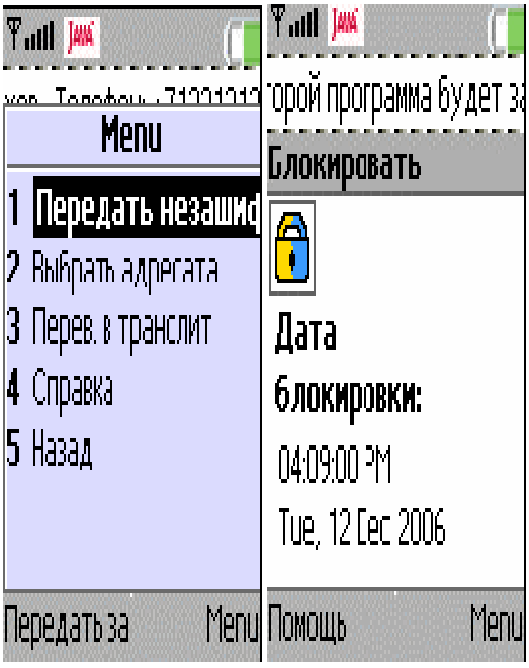
Kriptografi yang digunakan adalah Kriptografi Asymmetric Key. Apabila menggunakan *symmetric key* adalah kedua pihak harus memiliki *key* yang sama. *Key* tersebut harus dikirimkan secara aman menuju penerima dari beberapa sebab sehingga key dapat dicuri dan digunakan untuk mendekripsi sebuah *message*.

Dengan menggunakan *asymmetric keys*, pengirim mengenkripsi pesan dengan menggunakan *public key* penerima. Kemudian penerima mendekripsi pesan tersebut menggunakan *private key*. *Private key* hanya dimiliki oleh penerima. Antara *private* dan *public key* merupakan komplemen matematis sehingga pesan yang terenkripsi menggunakan *public key* dapat terdekripsi menggunakan *private key*. Hal tersebut secara komputasi juga sulit untuk membuat private key ulang menggunakan public key.

Berikut adalah contoh aplikasi lain yang tidak menggunakan J2ME :

a. Aplikasi SMSProtector

Aplikasi ini merupakan aplikasi gratis yang telah diterjemahkan oleh banyak programmer dalam banyak bahasa misalnya Jerman dan Rusia. Sayangnya belum ada yang mencoba untuk menerjemahkan aplikasi ini ke dalam bahasa Indonesia.
Aplikasi ini memiliki kemampuan tambahan untuk tidak saja mengacak pesan SMS tapi juga data nomor yang ada di *phonebook*. Algoritma yang digunakan adalah DES seperti halnya kebanyakan aplikasi sejenis.
Satu lagi kehebatan dari aplikasi ini adalah kompatibilitas dengan ponsel lain yang belum ter-*install* aplikasi ini didalamnya. Ketika sebuah pesan (tidak teracak) yang dikirimkan ke pengguna lain, maka data SMS yang tersimpan dalam direktori *sent* dari ponsel si pengirim akan berupa pesan yang teracak, namun SMS yang diterima adalah SMS normal (yang tidak teracak) tadi



Gambar 2: Aplikasi SMSProtector dalam bahasa Rusia

b. Aplikasi SMS 007
SMS 007 merupakan salah satu versi berbayar dari aplikasi SMS Rahasia yang cukup canggih sekaligus popular. Harga aplikasi ini ditawarkan seharga 39 USD.
Algoritma yang digunakannya adalah symmetric cipher (AES) yang termasuk rumit. Pesan SMS yang dikirmkan oleh aplikasi ini tidak dapat diterjemahkan siapapun yang tidak memiliki otorisasi termasuk didalamnya adalah operator.

Gambar 3: Aplikasi SMS 007

4. CARA KERJA APLIKASI

4.1 Cara Kerja Penghemat SMS
Teknik yang biasa digunakan adalah teknik kompresi memanfaatkan tabel Huffman yang tetap untuk setiap karakter dalam SMS.
Langkah awalnya adalah menyusun tabel bit yang baru untuk semua karakter yang akan digunakan (lihat tabel 1). Masing-masing karakter terdiri atas prefik dan body.
Prefik menunjukkan jenis karakter misalnya huruf besar atau kecil, dan body berisi bit datanya. Dalam tabel tersebut, tidak semua karakter ditampilkan, namun hanya sebagian saja.

Tabel 1. Kode Huffman

Karakter	Prefik	Body	Hasil
a	0	0000	00000
b		00101	000101
c		1101	01101
d		01011	001011
f		11001	011001
g		10101	010101
h		1000	01000
i		0001	00001
j		110001001	0110001001
k		1100011	01100011
l		1001	01001
m		10100	010100
n		0110	00110
o		0100	00100
p		10110	010110
A	100	0000	1000000
B		00101	10000101
C		1101	1001101
D		01011	10001011
F		11001	10011001
G		10101	10010101
H		1000	1001000
I		0001	1000001
J		110001001	10011000100
space	101	1	1011
e		0	1010
!	110	0011	1100011
“		0110	1100110
‘		0100	1100100
0	111	0000	1110000
1		0001	1110001
3		0011	1110011
4		0100	1110100

Sebagai perbandingan, perhatikan contoh beberapa karakter dari tabel ASCII 7 bit standar yang menjadi representasi karakter SMS normal di Tabel 2.

Tabel 2 . ASCII 7 bit

Kode ASCII	Karakter
0110000	0
0110001	1
0110010	2
1000000	@
0111111	?
1000001	A
1000010	B
1000011	C
1100001	a
1100010	b

Sebagai ilustrasi, mari kita menerjemahkan sebuah pesan berikut : Hallo monica
Terdapat 12 karakter (termasuk spasi) yang jika masing-masing karakter terdiri atas 7 bit, maka pesan tersebut akan terdiri atas 84 bit.
Menurut tabel yang baru,inilah hasil adaptasi karakter-karakter tersebut.

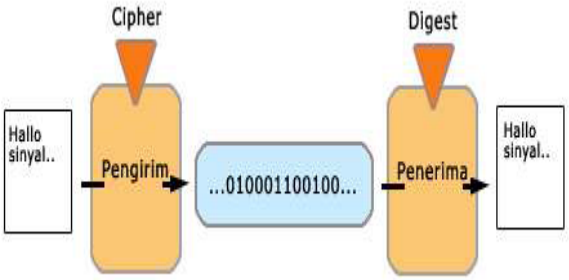
Tabel 3. Hasil Adaptasi

Karakter	Kode	Jumlah bit
H	1001000	7
a	0000	5
l	01001	5
l	01001	5
o	00100	5
space	1011	4
m	010100	6
o	00100	5
n	00110	5
i	00001	5
c	01101	5
a	0000	5
TOTAL		62

Coba bandingkan hasil kompresinya. Dengan cara biasa membutuhkan 84 bit dan dengan menggunakan kompresi diperlukan hanya 62 bit untuk sebuah pesan yang sama.
Jadi setidaknya ada 22 karakter yang dihemat atau sekitar 35%. Meski yang dihemat cukup banyak, untuk membaca pesan yang dikirimkan harus menggunakan aplikasi pembaca yang khusus. Jika tidak maka pesan yang terkirim tidak akan terbaca.

4.2 Cara Kerja SMS Rahasia

Dalam sebuah aplikasi yang mengedepankan unsur keamanan, tentunya salah satu bagian utama yang akan diimplementasikan adalah metode enkripsi atau pengacakan terhadap pesan yang diketikkan.
Konsepnya adalah bagaimana kemudian kode yang telah diacak tersebut dapat dibuka atau dibaca kembali hanya oleh pembaca tertentu yang memiliki kuncinya sesuai dengan keinginan sang pengirim.



Gambar 4 : Proses Enkripsi

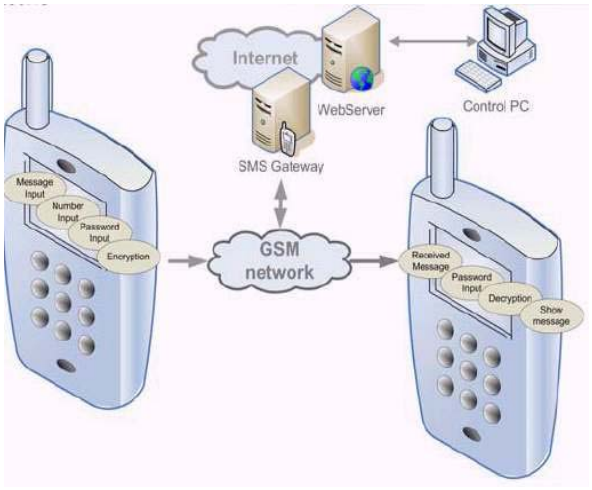
Istilah untuk pengacak pesan ini adalah cipher, namuun beberapa lebih senang menyebut dengan *salt*, sedangkan pembukanya sering disebut dengan *digest*.

Algoritma atau metode enkripsi yang dapat digunakan pada aplikasi ponsel sangat dipengaruhi oleh kemampuan dan kecepatan pemrosesan dari handset yang bersangkutan, serta ukuran dari aplikasi yang dihasilkan setelah metode tersebut diterapkan.
Pemilihan metode enkripsi mana yang digunakan sangatlah penting dan mempengaruhi berapa waktu rata-rata yang dibutuhkan untuk memproses pesan yang diketikkan untuk kemudian dikirimkan ke penerima yang dimaksud. Karena keterbatasan ponsellah yang membuat rata-rata metode enkripsi yang diterapkan masihlah cukup sederhana dibandingkan berbagai metode enkripsi yang banyak berkembang saat ini.
Salah satunya diterapkan dalam pustaka Bouncy Castle. Dalam tabel 3, data yang ada ditentukan berdasarkan waktu pemrosesan rata-rata terhadap 100 karakter yang diketikkan secara acak.
Hasil pengacakan terhadap sebuah pesan tersebut tidak lagi berupa pesan yang dapat dibaca atau diterjemahkan secara langsung oleh mata manusia yang membacanya data yang diacak akan berupa data biner atauu dikenal dengan istilah data bit alias binary digit misalnya 010000100010001.

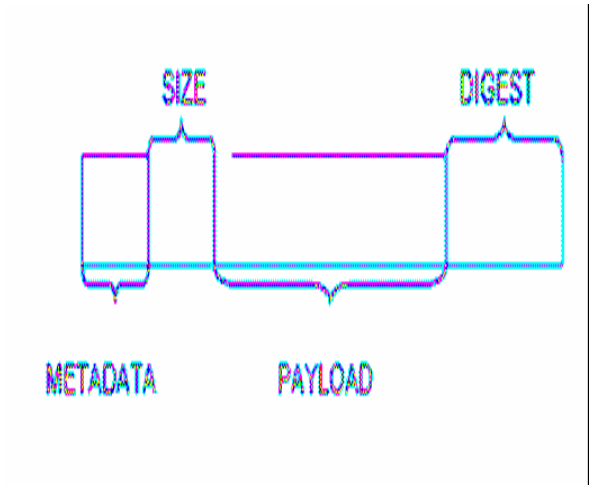
Tabel 4. Waktu Pemrosesan

Algoritma	Waktu Rata (ms)
DES	787
3DES	1997
AES-Fast	601
AES-Middle	1463
AES-Light	1432
Rijandael	3858
Blowfish	501
IDEA	881
RC2	1107
RC5	542

Selanjutnya, data yang telah dikodekan tersebut harus dibungkus dan kemudian dikirimkan ke alamat yang dituju. Secara umum tak ada yang khusus ketika data yang ada dikirimkan melalui carrier dan jaringan yang dimiliki operator.
Artinya secara teknis sebuah data maksimum yang dapat dikirimkan tetaplah sama dengan ukuran 160 karakter, Dalam implementasinya, pesan SMS yang dikirimkan ini dapat berupa teks standar dimana 1 karakter direpresentasikan dengan 7 bit data maupun dalam bentuk biner atau bit. 1 bit adalah unit satuan dasar penyimpan informasi terkecil. Jadi jika dijumlah, maksimal ada 1120 bit.
Jadi selama aplikasi mengirim 1 SMS jumlah bit masih berjumlah 1120 maka pesan tetap akan dianggap sebagai satu pesan SMS yang utuh.
Selanjutnya data-data bit tersebut disusun dalam bentuk larik dan dibungkus sesuai dengan format standar sebuah pesan SMS. Sebuah pesan SMS terdiri dari beberapa array bit yang berisi header yang memuat data-data ukuran dan informasi tambahan lainnya, data pesan yang telah diacak, dan terakhir dan kadang-kadang adalah *digest* alias kunci pembukanya.



Gambar 5: Proses Pengiriman SMS



Gambar 6: Proses Pembungkusan Data

Karena sifat aplikasi yang rahasia, dan sesuai dengan karakter dengan aplikasi Java SMS yang Peer to Peer alias titik ke titik, maka si pengguna hanya dapat membuka pesan yang diterimanya menggunakan aplikasi yang sama.
Didalam aplikasi tersebut umumnya terdiri dari pengirim dan penerima dimana masing-masing mengandung baik cipher maupun digest yang unik dan ditetapkan sebagai standar oleh pembuat aplikasi tersebut.
Untuk membuat lebih privat lagi, pengiriman dapat dilakukan dengan menggunakan nomor port khusus yang dapat ditentukan oleh kedua aplikasi baik pengirim dan penerima terlebih dahulu sebelumnya.
Dan aplikasi ini sebenarnya adalah aplikasi ‘lepas’ yang tidak bergantung pada situasi carrier dan jaringan operator, jadi sangat menarik ketika operator dan content provider di Indonesia kemudian membungkusnya menjadi sebuah layanan berlangganan.

5. KESIMPULAN

Kode Huffman dan kriptografi dapat diterapkan dalam berbagai aspek. Salah satunya dalam teknologi sms,untuk mengatasi kekurangan yang terdapat dalam teknologi ini.

Kekurangan – kekurangan tersebut diantaranya adalah apabila kita ingin mengirimkan pesan melebihi jumlah karakter yang telah ditentukan oleh ponsel yang kita punya dan saat kita ingin pesan tersebut hanya bisa dibuka atau dibaca kembali oleh orang tertentu yang memiliki kuncinya sesuai dengan keinginan kita.

Untuk mengatasi kekurangan yang pertama digunakanlah aplikasi penghemat sms. Aplikasi ini menggunakan kode Huffman untuk mengurangi jumlah bit yang digunakan

Kekurangan yang kedua dapat diatasi oleh aplikasi sms rahasia. Aplikasi ini menggunakan teknik kriptografi *asymmetric key*. Dengan menggunakan teknik ini, pesan kita hanya bisa dibuka atau dibaca kembali oleh orang tertentu yang memiliki kuncinya sesuai dengan keinginan kita.

DAFTAR REFERENSI

[1] Munir, Rinaldi. 2003. *Matematika Diskrit.* Bandung. Informatika

[2] ---, http:// www.cryptography.com. waktu akses : 23 Desember 2006 10.44 WIB

[3] ---,http:// dahlan.unimal.ac.id waktu akses : 26 Desember 2006 20.47 WIB

[4] ---,http://www. kagakribet.com waktu akses : 23 Desember 2006 10.32 WIB

[5] ---, http://www.kamusti.web.id waktu akses : 26 Desember 2006 20.24 WIB

[6] ---,http://www.ti.usd.ac.id/ waktu akses : 26 Desember 2006 20.13 WIB