IMPLEMENTASI METODE RSA DAN MD5 CHECKSUM APPLICATION DALAM KRIPTOGRAFI

Nur Alia Syafitri[1], Aqmal Maulana[2], dan Saffira Lindra Putri[3]
1. Departemen Research & Development PT. Collega Inti Pratama
Talavera Office Park 6th-7th Floor
Jl. TB Simatupang Kav. 22-26
Jakarta, Indonesia 12430
E-mail: nuralia.syafitri@gmail.com
2. Droidlime
Komplek Ruko Pakkita
Jl. AMD-XKav. 18 Blok A4
Tangerang, Indonesia 15156
E-mail: Aqmal_maulana@yahoo.com
3. Departemen Project Management PT. Collega Inti Pratama
Talavera Office Park 6th-7th Floor
Jl. TB Simatupang Kav. 22-26
Jakarta, Indonesia 12430
E-mail: saffiralindra@gmail.com

Abstract

Encription is an encode process which can process either a message or an information. This method is done so not all of the people in this world can read or access the information. People who can access the information are people who have "key". The purpose of encription is to protect the information's secret and its security from leak of information and to make sure that only authorized people who can access the information. Meanwhile to make sure about message's condition, we need error detection. In other words, error detection is a process to make sure the information's realibilty when it is being sent until it arrives to the acceptor. With the help of encription and error detection, the security and originality of information can be protected. For encription, the writer uses RSA method. RSA method is chosen because it is one of the most-difficult-to-break encription method. RSA is an acronym of some family names that come from Ron Rivest, Adi Shamir, and Leonard Adleman. With this method, the sender can create and also release a public key that come from 2 prime numbers and auxilary value. Meanwhile for error detection, the writer uses MD5 Checksum Application Method. MD5 is one of hash function that usually used in cryptograhy. MD5 creates 128-bit of hash value (16 bytes) in the form of text and 32 digits of hexadecimal number.

Keywords: *Encryption, Error Detection, Cryptograhpy, RSA, MD5*

Abstrak

Enkripsi merupakan sebuah proses encoding pesan atau informasi. Hal ini dilakukan sehingga tidak semua orang dapat membaca maupun mengakses informasi tersebut. Orang-orang yang dapat mengakses informasi hanyalah orang-orang yang memiliki "kunci". Tujuannya adalah untuk menjaga kerahasiaan dan keamanan dari bocornya informasi yang dikirimkan serta memastikan bahwa hanya orang-orang yang berhak yang dapat mengakses informasi tersebut. Sementara untuk memastikan kondisi pesan yang dikirim, diperlukan skema error detection. Error detection akan memastikan kehandalan data pada saat dikirim hingga sampai kepada penerima pesan. Dengan adanya enkripsi dan error detection, keamanan serta keaslian pesan atau informasi yang dikirim dapat dijaga. Untuk enkripsi, penulis menggunakan metode RSA.

RSA dipilih karena merupakan salah satu metode enkripsi yang paling sulit ditembus. RSA sendiri merupakan singkatan dari nama keluarga para pembuatnya, yakni Ron Rivest, Adi Shamir, dan Leonard Adleman. Dengan metode ini, si pengguna secara tidak langsung akan menciptakan sekaligus merilis sebuah kunci publik berdasarkan dua bilangan prima besar bersamaan dengan auxilary value. Sedangkan untuk error detection dari pesan yang dikirim, penulis menggunakan metode MD5 Checksum Application. MD5 merupakan salah satu fungsi hash yang biasa digunakan dalam kriptografi. MD5 menghasilkan hash value 128-bit (16-byte) dalam format teks berupa angka hexadesimal sebanyak 32 digit.

Kata kunci: Enkripsi, Error Detection, Kriptografi, RSA, MD5

PENDAHULUAN

Enkripsi merupakan sebuah proses encoding pesan maupun informasi sehingga tidak semua orang dapat membaca maupun mengakses informasi tersebut. Hanya orang-orang tertentu yang memiliki "kunci" yang dapat mengakses informasi tersebut. Hal ini dilakukan untuk menjaga kerahasiaan dan keamanan dari bocornya informasi yang dikirimkan serta memastikan bahwa hanya orang-orang yang berhak yang dapat mengakses informasi tersebut.

Di dalam skema enkripsi, pesan atau informasi yang belum diencode atau dengan kata lain masih dalam bentuk semula dikenal dengan plaintext. Sedangkan pesan atau informasi yang sudah diencode, dikenal dengan ciphertext. Chiphertext sendiri tidak akan bisa dibaca maupun diakses jika belum didekripsi oleh penerima pesan.

Sementara untuk memastikan bahwa pesan yang dikirim tidak rusak, cacat, dan mengalami perubahan, diperlukan skema error detection. Dengan kata lain, error detection akan memastikan keandalan data pada saat dikirim hingga sampai kepada penerima pesan. Dengan adanya enkripsi dan error detection, keamanan serta keaslian pesan atau informasi yang dikirim dapat dijaga.

Untuk enkripsi, penulis menggunakan metode RSA. RSA dipilih karena merupakan salah satu metode enkripsi yang paling sulit ditembus. RSA sendiri merupakan singkatan dari nama keluarga para pembuatnya, yakni Ron Rivest, Adi Shamir, dan Leonard Adleman. Dengan metode ini, si pengguna secara tidak langsung akan menciptakan sekaligus merilis sebuah kunci publik berdasarkan dua bilangan prima besar bersamaan dengan auxilary value. Jika bilangan prima tersebut cukup besar nominalnya, hanya orang-orang yang memiliki pengetahuan tentang bilangan prima saja yang dapat mendecode pesan yang dikirim.

Sedangkan untuk error detection dari pesan yang dikirim, penulis menggunakan metode MD5. MD5 merupakan salah satu fungsi hash yang biasa digunakan dalam kriptografi. MD5 menghasilkan hash value 128-bit (16-byte) dalam format teks berupa angka hexadesimal sebanyak 32 digit. MD5 sendiri merupakan pengganti MD4 yang dirancang oleh Ronald Rivest pada tahun 1991.

Kriptografi atau kriptologi berasal dari kata Kryptos dari Yunani yang berarti tersembunyi atau rahasia dan graphein

yang berarti menulis [1]. Kriptografi adalah praktek dan studi teknik untuk komunikasi yang aman dengan adanya pihak ketiga [2]. Berbagai aspek keamanan informasi seperti kerahasiaan data, integritas data, dan otentikasi adalah fokus dari kriptografi modern [3]. Kriptografi modern merupakan irisan dari berbagai disiplin ilmu seperti matematika, ilmu komputer, dan teknik listrik. Aplikasi kriptografi modern digunakan pada kartu ATM, password komputer, hingga e-commerce.

Dalam kriptografi, enkripsi adalah proses encoding pesan atau informasi dengan sedemikian rupa sehingga hanya pihak yang berwenang dapat membacanya. Dalam skema enkripsi, pesan atau informasi, disebut sebagai plaintext. Plaintext dienkripsi dengan menggunakan sebuah algoritma enkripsi, menghasilkan ciphertext yang hanya bisa dibaca jika didekripsi [4].

RSA adalah salah satu metode kriptografi yang secara luas digunakan untuk mentransmisikan data dengan aman. Dalam metode ini, kunci enkripsi bersifat publik. RSA bersifat asimetris berdasarkan pada sulitnya memfaktorkan dua bilangan prima besar. Pengguna RSA menciptakan dan kemudian menerbitkan kunci publik berdasarkan dua bilangan prima besar, bersama dengan nilai tambahan. Bilangan prima harus dirahasiakan. Siapapun dapat menggunakan kunci publik untuk mengenkripsi pesan, tetapi dengan metode ini, jika kunci publik cukup besar, hanya seseorang dengan pengetahuan tentang bilangan prima dapat mendecode pesan [5].

Error detection and correction atau error control adalah teknik yang memungkinkan pengiriman data digital secara andal melalui saluran komunikasi tidak dapat diandalkan. Error detection and correction memungkinkan mendeteksi kesalahan dan mengoreksi kesalahan. Teknik ini memungkinkan rekonstruksi data asli dalam banyak kasus [6].

Checksum atau hash sum adalah datum berukuran kecil dari blok data digital digunakan untuk mendeteksi kesalahan pada sebuah file digital. Checksum biasanya disisipkan ke file instalasi setelah diterima dari server download. Checksum sering digunakan untuk memverifikasi integritas data.

Prosedur yang menghasilkan checksum yang diberi masukan data disebut fungsi checksum atau algoritma checksum. Hal ini digunakan untuk fungsi hash kriptografi yang dapat digunakan untuk mendeteksi berbagai kerusakan data dan memverifikasi integritas data secara keseluruhan. Jika checksum dihitung untuk input data saat ini sesuai dengan nilai yang tersimpan dari checksum yang dihitung sebelumnya, ada kemungkinan sangat tinggi bahwa data tidak diubah ataupun mengalami kerusakan. Fungsi hash kriptografi sendiri adalah fungsi hash yang digunakan untuk menciptakan input data dari nilai hash-nya saja [7].

Fungsi hash kriptografi yang ideal memiliki empat sifat utama:

1. Mudah untuk menghitung nilai hash untuk setiap pesan yang diberikan
2. Tidak dapat menghasilkan pesan dari hash
3. Tidak dapat memodifikasi pesan tanpa mengubah hash

4. Tidak dapat menemukan dua pesan yang berbeda dengan hash yang sama

Algoritma MD5 digunakan sebagai salah satu fungsi hash kriptografi. MD5 menghasilkan nilai hash 128-bit (16-byte), biasanya dinyatakan dalam format teks sebagai angka hexadesimal sebanyak 32 digit. MD5 telah digunakan dalam berbagai macam aplikasi kriptografi dan juga biasa digunakan untuk memverifikasi integritas data. MD5 dirancang oleh Ronald Rivest pada tahun 1991 untuk menggantikan fungsi hash sebelumnya, MD4 [8].

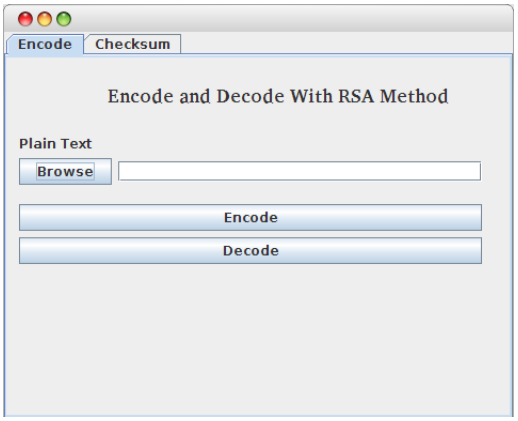
MD5 telah banyak digunakan di dunia perangkat lunak untuk menyediakan jaminan bahwa file yang ditransfer telah tiba dengan utuh. Sebagai contoh, file server sering memberikan pra-dihitung MD5 checksum untuk file, sehingga pengguna dapat membandingkan checksum dari file yang didownload. Sebagian besar sistem operasi berbasis unix menyertakan modul MD5 sum utility dalam paket instalasinya. Sementara untuk Windows, pengguna dapat menginstall sebuah utility dari Microsoft, atau menggunakan aplikasi third-party. ROM Android juga memanfaatkan MD5 [9].

METODOLOGI

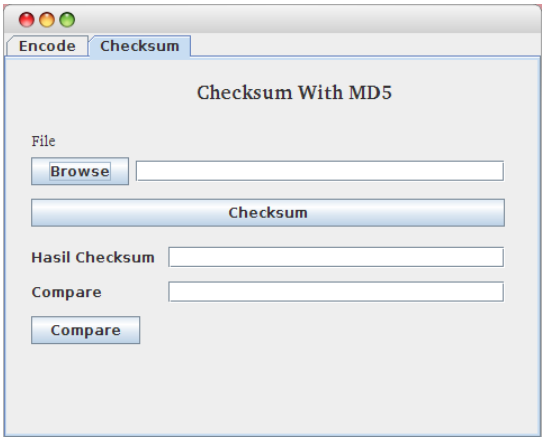
Untuk membuat program ini, penulis menggunakan sistem operasi Linux Ubuntu 15.04 serta aplikasi Netbeans versi 8.0.2 sebagai sarana untuk mendevelop program berbasis Java.

Secara keseluruhan, program ini tampak sederhana dengan dua menu utama, yakni Encode dan Checksum. Pada menu encode, terdapat tombol Browse, Encode, dan Decode. Tombol browse digunakan untuk memilih file yang ingin di encode/decode. Tombol Encode digunakan untuk mendecode file yang sudah dipilih. Sedangkan tombol Decode digunakan untuk mendecode file.

Pada menu Checksum terdapat tombol Browse, Checksum, dan Compare. Tombol Browse berfungsi untuk memilih file yang ingin dicek nilai checksumnya. Sedangkan tombol checksum berfungsi untuk menghasilkan hash value 128-bit berupa angka hexadesimal sebanyak 32 digit dari file yang sudah dipilih ke dalam sebuah textbox. Tombol Compare berfungsi untuk membandingkan antara hash value 128-bit pada textbox “Hasil Checksum” dan textbox “Compare”.



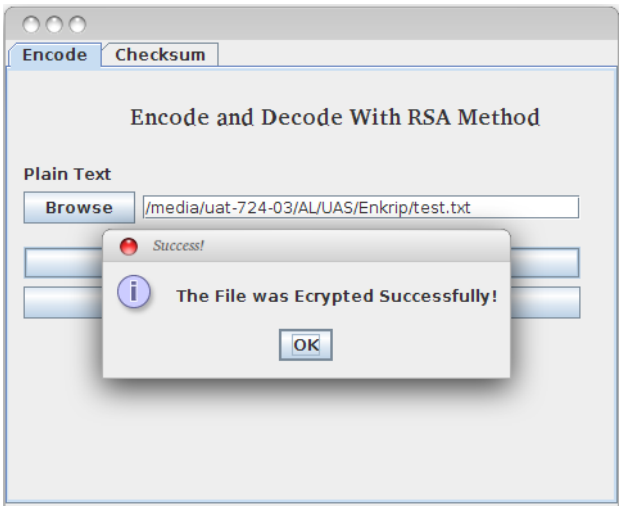
Gambar 1 Tampilan aplikasi pada sub menu “Encode”.



Gambar 2Tampilan aplikasi pada sub menu "Checksum".

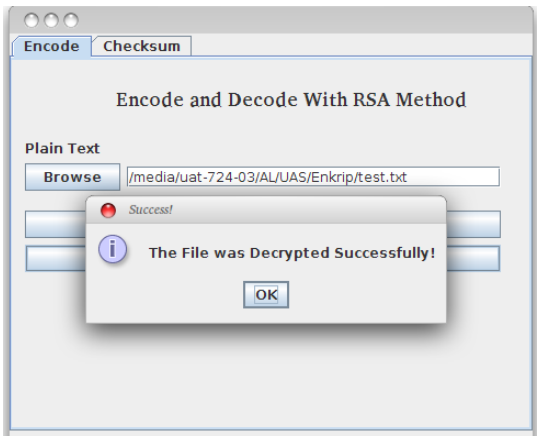
Cara Kerja Program

Sebelum dapat membaca file yang akan diencode maupun didecode, user diminta untuk menekan tombol "Browse" terlebih dahulu untuk memilih file yang akan dienkrip atau didekrip. Dengan kata lain, tombol "Browse" ini berfungsi untuk mengakses file tertentu yang ada di dalam komputer. Setelah file dipilih, user dapat menekan tombol "Encode" atau "Decode". Pada saat user menekan tombol "Encode", program akan mengenkripsi file yang sudah dipilih dengan metode RSA. Setelah melakukan enkripsi, program akan membuat file yang sudah dipilih menjadi terenkripsi tanpa membuat file baru. Ketika proses enkripsi berhasil dilakukan, program akan menampilkan MessageBox "The File was Encrypted Successfully!".



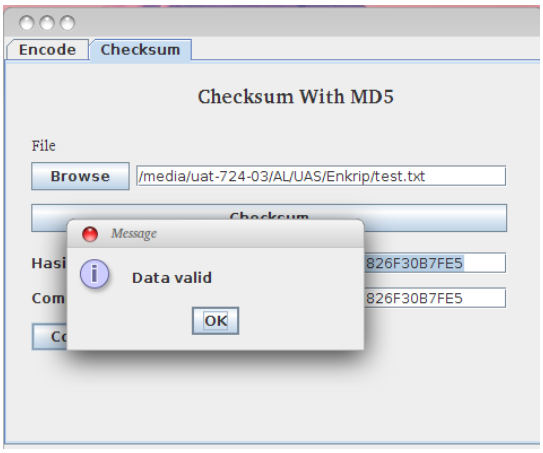
Gambar 3Tampilan aplikasi pada saat enkripsi berhasil dilakukan.

Kebalikannya, pada saat user menekan tombol "Decode", program akan mendekripsi file kembali yang sudah dienkrip sehingga pesan di dalam file tersebut dapat dibaca kembali. Dekripsi ini juga dilakukan tanpa membuat file baru. Ketika proses dekripsi berhasil dilakukan, program akan menampilkan MessageBox "The File was Decrypted Successfully!". Dengan melakukan dekripsi, file yang sudah di enkripsi pun dapat dibaca kembali.

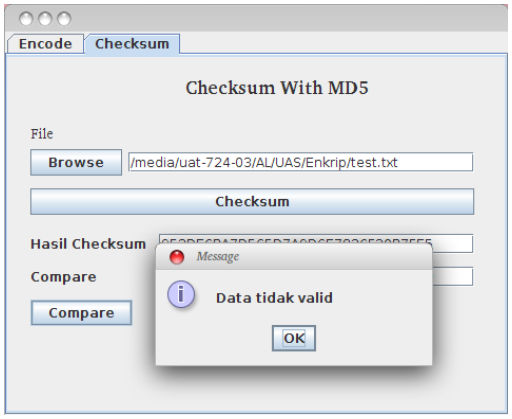


Gambar 4Tampilan aplikasi pada saat dekripsi berhasil dilakukan.

Tombol “Browse” pada menu checksum pun memiliki fungsi yang sama, yakni untuk mengakses file tertentu yang ada di dalam komputer. Melalui tombol Browse tersebut, user dapat memilih file yang sudah terenkripsi maupun terdekripsi sebelumnya. Sedangkan Tombol “Checksum” akan membaca file yang sudah dibrowse sebelumnya dan menghasilkan hash value sebanyak 32 digit angka hexadesimal dengan metode MD5. Setelah itu, hash value tersebut pun ditampilkan pada TextBox “Hasil Checksum”. Sementara tombol “Compare” akan mengecek apakah hash value yang terdapat pada TextBox “Hasil Checksum” cocok (sama persis) dengan TextBox “Compare”. Jika cocok, program akan menampilkan MessageBox yang berisi pesan “Data valid”. Jika tidak cocok, program akan menampilkan MessageBox yang berisi pesan “Data tidak valid”. Textbox “Compare” sendiri diisi secara manual oleh user sebagai pengguna program.



Gambar 5Tampilan aplikasi pada saat hasil komparasi hash value cocok.

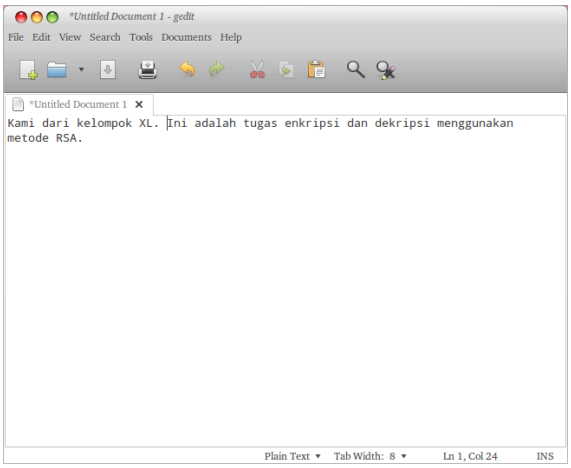


Gambar 6Tampilan aplikasi pada saat hasil komparasi hash value tidak cocok.

HASIL PENELITIAN

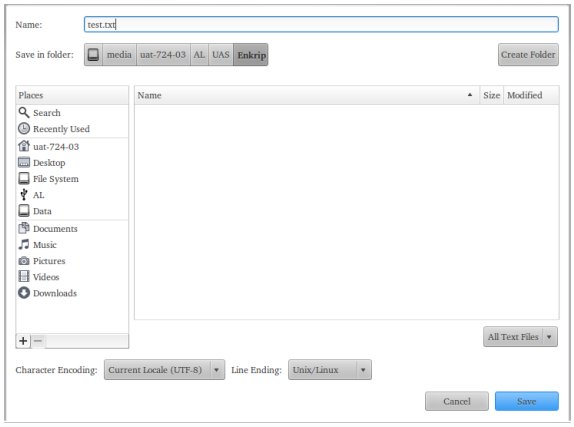
Enkripsi

Untuk menguji program ini, pertama-tama penulis membuat sebuah file dengan extension .txt yang berisi pesan “Kami dari kelompok XL. Ini adalah tugas enkripsi dan dekripsi menggunakan metode RSA.”



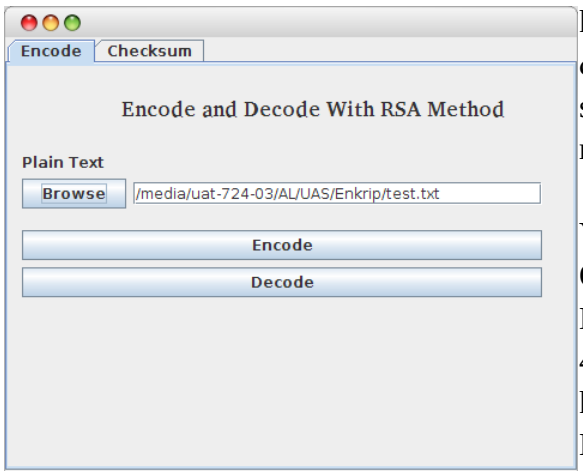
Gambar 7Sebuah file .txt untuk melakukan pengujian aplikasi.

Setelah itu, file tersebut pun disimpan ke dalam sebuah direktori yang ada di dalam harddisk dengan nama “test.txt”.



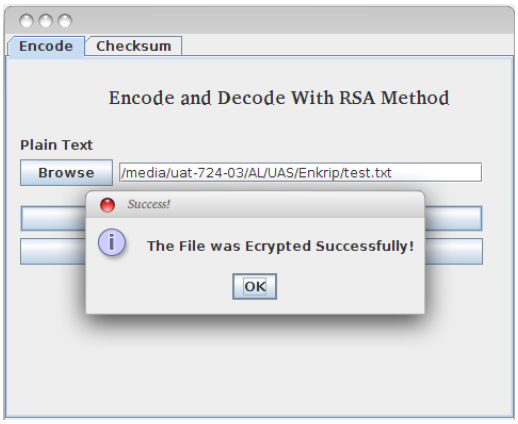
Gambar 8 Kotak dialog saat menyimpan file .txt yang sudah dibuat.

Program pun dijalankan dan file tersebut dipilih sebagai objek pengujian dengan menekan tombol “Browse”.



Gambar 9 Menekan tombol browse pada aplikasi untuk mengakses file .txt.

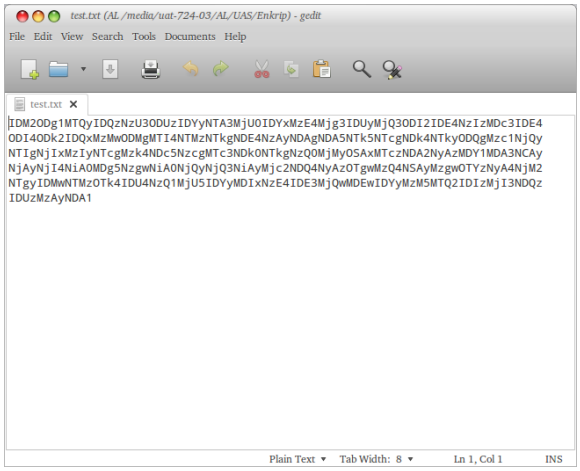
Tombol “Encode” ditekan untuk mengenkripsi file tersebut.



Gambar 10Tampilan aplikasi pada saat enkripsi berhasil dilakukan.

Setelah proses enkripsi berhasil dilakukan, file tersebut pun tetap dapat bisa dibuka. Namun isinya tak lagi sama seperti sebelumnya. Jika sebelumnya file tersebut berisi pesan “Kami dari kelompok XL. Ini adalah tugas enkripsi dan dekripsi mengguna metode RSA.”, setelah dienkripsi isi pesannya pun menjadi

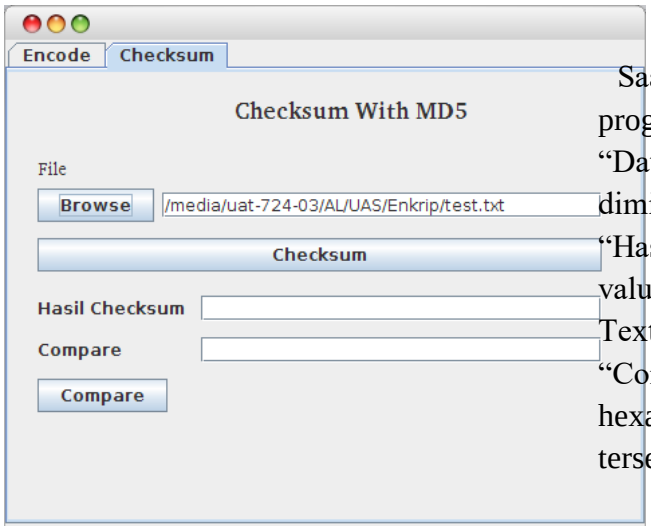
“IDM20Dg1MTQyIDQzNzU30DUzID
YyNTA3MjUOIDYxMzE4Mjg3IDUyMj
Q30DI2IDE4NzIzMDc3IDE40DI40Dk2I
DQxMzMw0DMgMTI4NTMzNTkgNDE
4NzAyNDAgNDA5NTk5NTcgNDk4NT
ky0DQgMzc1NjQyNTIgNjIxMzIyNTcg
Mzk4NDc5NzcgMTc3NDkONTkgNzQO
MjMyOSAxMTczNDA2NyAzMDY1M
DA3NCAyNjAyNjI4NiAOMDg5NzgwN
iAONjQyNjQ3NiAyMjc2NDQ4NyAzOT
gwMzQ4NSAyMzgwOTYzNyA4NjM2N
TgyIDMwNTMz0Tk4IDU4NzQ1MjU5I
DYyMDIxNzE4IDE3MjQwMDEwIDYy
MzM5MTQ2IDIzMjI3NDQzIDUzMzAy
NDAI”.



Gambar 11Isi file .txt yang sudah berhasil dienkripsi.

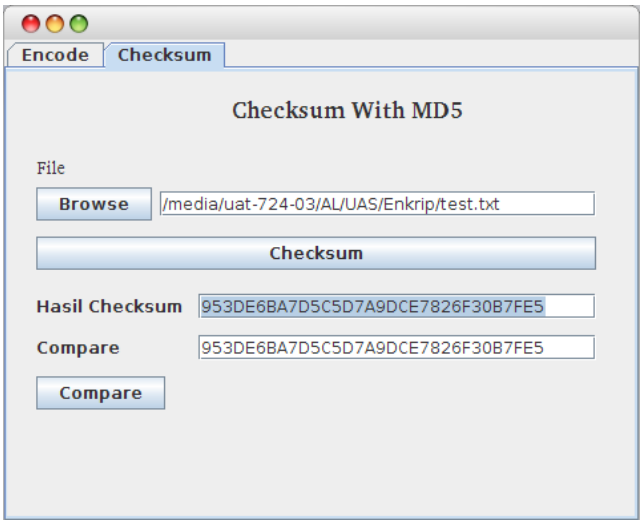
***Checksum* MD5**

Setelah berhasil dienkripsi, file yang sudah dalam keadaan terenkripsi tersebut pun kembali digunakan untuk pengujian checksum dengan menekan tombol "Browse" pada menu *Checksum*.



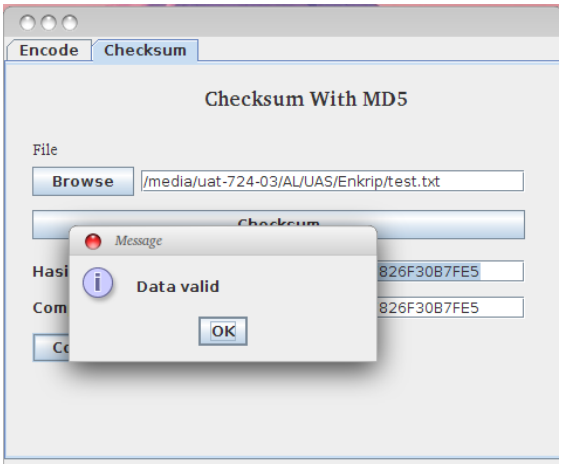
Gambar 12Menekan tombol "Browse" pada aplikasi untuk mengakses file .txt.

Hasilnya, program menampilkan sebuah angka hexadesimal pada TextBox "Hasil Checksum". Angka hexadesimal untuk file tersebut adalah "953DE6BA7D5C5D7A9DCE7826F30B7FE5". Angka hexadesimal tersebut pun dapat dicopy lalu dipaste ke TextBox "Compare" untuk menguji apakah program yang dibuat sudah berjalan dengan semestinya.



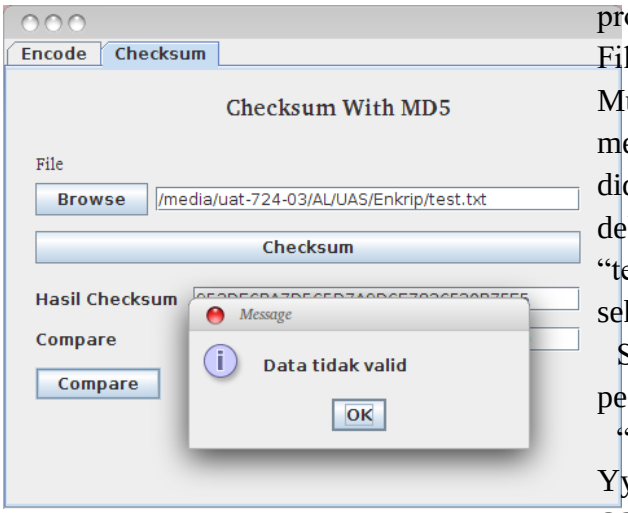
Gambar 13Menekan tombol "Checksum" pada aplikasi untuk menghasilkan hash value.

Saat tombol "Compare" ditekan, program pun menampilkan MessageBox "Data valid" karena hash value yang dimiliki file "test.txt" pada TextBox "Hasil Checksum" cocok dengan hash value pada TextBox "Compare". Jika TextBox pada "Hasil Checksum" dan "Compare" menunjukkan 32 digit angka hexadecimal yang sama, itu berarti file tersebut tidak mengalami perubahan.



Gambar 14Tampilan aplikasi pada saat hasil komparasi hash value cocok.

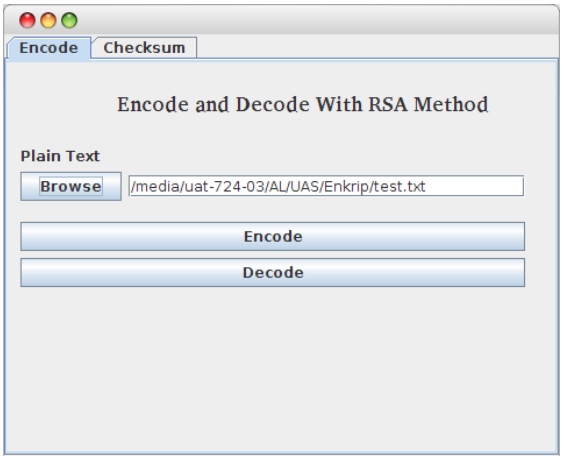
Ketika hash value yang ada pada Textbox "Compare" atau "Hasil Checksum" diubah, program akan menampilkan MessageBox "Data tidak valid". Hal ini menandakan bahwa hash value yang dimiliki oleh file yang diuji tidak cocok dengan hash value pada Textbox "Compare".



Gambar 15Tampilan aplikasi pada saat hasil komparasi hash value tidak cocok.

Dekripsi

Setelah melakukan pengujian enkripsi dan checksum MD5, file test.txt yang masih dalam keadaan terenkripsi pun kembali digunakan untuk menguji fungsi dekripsi dari program yang dibuat dengan menekan tombol "Browse" pada menu Encode.



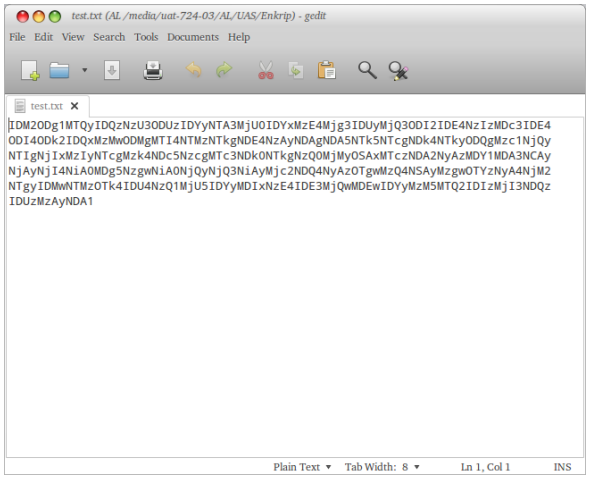
Gambar 16Menekan tombol "Browse" pada aplikasi untuk mengakses file .txt.

Ketika tombol "Decode" ditekan, program menampilkan MessageBox "The File was Decrypted Successfully!". Munculnya MessageBox tersebut menandakan bahwa file sudah berhasil didekripsi. Setelah melewati proses dekripsi, pesan yang ada di dalam file "test.txt" pun kembali seperti semula sehingga dapat dibaca kembali.

Sebelum didekripsi, file "test.txt" berisi pesan:

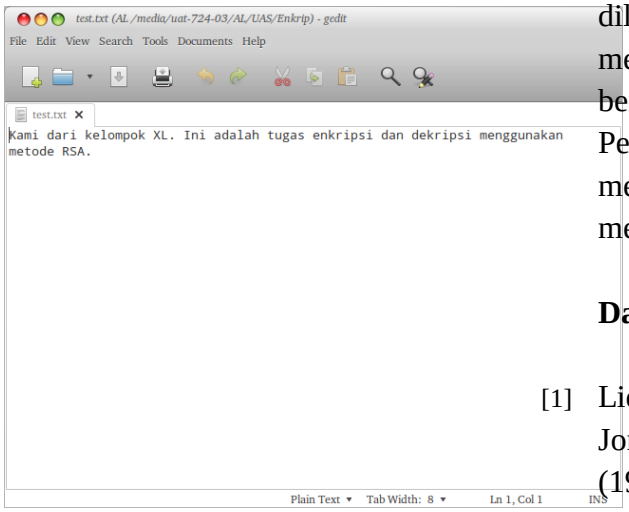
"IDM20Dg1MTQyIDQzNzU30DUzID
YyNTA3MjUOIDYxMzE4Mjg3IDUyMj
Q30DI2IDE4NzIzMDc3IDE40DI40Dk2I
DQxMzMw0DMgMTI4NTMzNTkgNDE
4NzAyNDAgNDA5NTk5NTcgNDk4NT
ky0DQgMzc1NjQyNTIgNjIxMzIyNTcg
Mzk4NDc5NzcgMTc3NDkONTkgNzQO
MjMyOSAxMTczNDA2NyAzMDY1M

DA3NCAyNjAyNjI4NiAOMDg5NzgwNiAONjQyNjQ3NiAyMjc2NDQ4NyAzOTgwMzQ4NSAyMzgwOTYzNyA4NjM2NTgyIDMwNTMz0Tk4IDU4NzQ1MjU5IDYyMDIxNzE4IDE3MjQwMDEwIDYyMzM5MTQ2IDIzMjI3NDQzIDUzMzAyNDAI".



Gambar 17Isi file .txt yang sebelumnya sudah berhasil dienkripsi.

Setelah didekripsi, pesan di dalam file "test.txt" kembali normal, "Kami dari kelompok XL. Ini adalah tugas enkripsi dan dekripsi mengguna metode RSA."



Gambar 18Isi file .txt yang sudah berhasil didekripsi.

KESIMPULAN

Dalam kehidupan nyata, program ini dapat digunakan untuk mengamankan isi pesan yang dikirim serta memastikan pesan yang dikirim tersebut merupakan pesan yang valid. Dengan fitur encode, decode, dan checksum, program ini dapat digunakan oleh pengirim maupun penerima pesan.

Agar kemananan pesan dapat terjaga, user dapat melakukan enkripsi terlebih dahulu sebelum mengirim pesan. Dengan begitu, kalaupun pesan tersebut disabotase ditengah perjalanan, isi pesan tidak akan dapat dibaca.

Sementara untuk memastikan isi pesan yang dikirim tidak terjadi perubahan, pengirim dapat memberikan hash value dari file yang dikirim kepada penerima pesan. Pengirim dapat melakukan checksum sebelum maupun sesudah file dienkrip. Itu artinya, pengirim bisa memberikan dua hash value kepada penerima, yakni hash value sebelum dienkrip dan sesudah dienkrip. Dengan begitu, pencocokan hash value pun dapat dilakukan dua kali oleh si penerima untuk memastikan bahwa isi pesannya benar-benar tidak mengalami perubahan. Pengecekan tersebut juga dilakukan untuk memastikan bahwa file yang dikirim tidak mengalami kerusakan.

Daftar Pustaka

[1] Liddell, Henry George; Scott, Robert; Jones, Henry Stuart; McKenzie, Roderick (1984). *A Greek-English Lexicon*. Oxford University Press.

[2] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. *Handbook of Theoretical Computer Science* 1. Elsevier.
[3] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A. *Handbook of Applied Cryptography*. ISBN 0-8493-8523-7.
[4] Goldreich, Oded. Foundations of Cryptography: Volume 2, Basic Applications. Vol. 2. Cambridge university press, 2004.
[5] Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). *Communications of the ACM* 21 (2): 120–126.
[6] W. William Cary Huffman; Vera S. Pless (2003). *Fundamentals of Error-Correcting Codes*. ISBN 978-0-521-78280-7.
[7] Schneier, Bruce. "Cryptanalysis of MD5 and SHA: Time for a New Standard". *Computerworld*.
[8] Ciampa, Mark (2009). *CompTIA Security+ 2008 in depth*. Australia ; United States: Course Technology/Cengage Learning.
[9] "FreeBSD Handbook, Security – DES, Blowfish, MD5, and Crypt". 2014-10-19.