PEMANFAATAN DAN APLIKASI TEKNIK OTENTIKASI DENGAN ALGORITMA MD5 UNTUK MEMERIKSA KEASLIAN TEKS AYAT AL QURAN

Abu Bakar Gadi – NIM : 13506040

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16040@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang penerapan salah satu teknik yang ada dalam kriptografi, yaitu fungsi hashing. Aplikasi fungsi hashing yang penulis implementasikan adalah dalam bidang autentikasi teks. Lebih spesifik lagi, yaitu dalam autentikasi teks Al Quran. Dalam makalah ini penulis juga mengusulkan suatu konsep sistem server yang menyimpan data nilai hash ayat-ayat Al Quran, sehingga dapat dimanfaatkan oleh banyak orang dari seluruh dunia. Sebagai alat pembantu, penulis telah membuat suatu aplikasi desktop simulasi sistem autentikasi ayat Al-Quran ini. Aplikasi ini dapat diunduh di http://s.itb.ac.id/~abu_gadi/quran_verifier.zip.

***Kata kunci**:* fungsi hash, otentikasi teks, Al Quran, MD5, server.

1. Pendahuluan

Sejak akhir tahun ‘80-an kita telah memasuki era digitalisasi. Sejak awal era digitalisasi, banyak hal mulai dapat dikonversi menjadi versi digitalnya. Sebagai contoh, foto yang tadinya hanya dapat disimpan berupa hasil cetak di atas kertas, sejak beberapa tahun yang lalu sudah dapat disimpan dalam bentuk digital (file komputer dengan format tertentu). Disamping itu masih banyak lagi contoh digitalisasi yang lainnya, seperti musik, film, buku teks, bahkan Al Quran. Dengan semakin majunya teknologi informasi, dalam hal ini bidang ilmu komputer, maka proses digitalisasi menjadi sangat mudah. Karena kemudahan tersebut, dengan ditunjang sarana internet yang sangat membantu dalam pendistribusian hasil-hasilnya, maka kini kita seringkali mendapati suatu hasil digitalisasi (untuk selanjutnya disebut *file*) yang dipalsukan dari sumber aslinya. Tentu saja pemalsuan ini akan sangat merugikan baik bagi produsen maupun pihak konsumen. Terlebih lagi jika yang dipalsukan adalah ayat Al Quran, yang merupakan firman Tuhan.

Sesuai dengan judul makalah ini, penulis akan membahas lebih jauh tentang teknik otentikasi (pengecekan keaslian) dari ayat Al Quran. Mengingat sifat dari Al Quran yang telah ditetapkan untuk tidak berubah hingga akhir zaman, tanpa ada batasan waktu atau tempat, maka dapat dikatakan bahwa Al Quran yang asli di dunia ini hanya ada satu hingga akhir zaman. Disamping itu, Al Quran diturunkan dalam bahasa arab, yang notabene sangat sensitif terhadap perubahan huruf atau *harakat* (tanda bunyi huruf). Sehingga apabila ada huruf atau *harakat* yang diubah, maka makna dari kata yang mengandung huruf atau *harakat* yang diubah tersebut akan berubah juga, sehingga tentu saja akan mengubah makna dari ayat Al Quran yang sesungguhnya. Atas dasar inilah, penulis memiliki sebuah gagasan untuk membuat suatu sistem otentikasi ayat Al Quran dengan memanfaatkan teknik hashing dengan algoritma MD5. Secara garis besar, sistem yang akan penulis implementasikan adalah berbasis web. Nilai *hash* masing-masing ayat disimpan pada server otentikasi untuk dijadikan acuan otentikasi ayat yang dimiliki oleh pengguna. Konsep otentikasinya adalah pencocokan nilai hash dari ayat pada sisi pengguna dengan nilai hash yang tersimpan di server. Untuk penjelasan lebih jauh mengenai sistem ini, akan dibahas lebih lanjut pada bagian setelah ini.

2. Dasar Teori

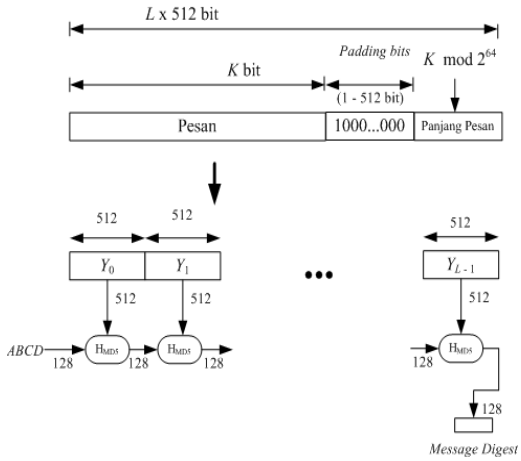
2.1 Sensitifitas Penulisan dalam Bahasa Arab

Bahasa arab adalah bahasa yang kompleks. Menurut fakta, kata-kata dalam bahasa arab banyak diadopsi ke bahasa lain. Ini menunjukkan bahwa bahasa arab kaya akan kosakata. Disamping itu, bahasa arab juga sangat sensitif terhadap tata cara penulisan (susunan huruf dan *harakat*/tanda bunyi). Oleh sebab itu, perubahan sedikit pada penulisan suatu kata akan menyebabkan makna dari kata tersebut berubah sangat signifikan. Karena Al Quran diturunkan dalam bahasa arab, maka hal yang serupa juga berlaku. Dari zaman disaat Al Quran diturunkan, hingga saat ini, Al Quran tidak pernah mengalami perubahan redaksi. Sehingga apabila ada sumber teks Al Quran yang redaksinya berubah, walaupun satu huruf atau harakat saja, berarti makna dari ayatnya akan berubah. Untuk memberikan gambaran tentang pentingnya penulisan pada bahasa arab, sebagai contoh adalah kata *Kalam* (كلم) dan *Qalam* (قلم). Walaupun hanya berbeda satu huruf saja yaitu ق dan ك , namun artinya sudah jauh berbeda. *Kalam* berarti perkataan, sedangkan *Qalam* berarti pena.

2.2 Algoritma *Hashing* MD5

Fungsi *hash* adalah fungsi yang menerima masukan string dengan panjang sembarang lalu mentransformasikannya menjadi string keluaran yang panjangnya tetap (*fixed*). Fungsi *hashing* yang sering digunakan dalam kriptografi adalah fungsi *hashing* yang bersifat satu arah (*one-way function*). Maksud dari satu arah disini adalah bahwa pesan (string) yang dihasilkan dari fungsi (dikenal sebagai *message digest*), tidak dapat dikembalikan lagi menjadi pesan semula (*irreversible*). Manfaat dari fungsi *hashing* yang salah satu contohnya adalah aplikasi yang diusulkan oleh penulis yaitu penjagaan integritas data. Apabila suatu data dimodifikasi, walaupun satu bit saja perubahannya, maka akan mengakibatkan nilai *hash* (*message digest*) dari data tersebut berubah pula, sehingga modifikasi dapat terdeteksi dengan jelas. Dengan demikian integritas data dapat dijaga dengan baik.

Salah satu algoritma fungsi *hashing* yang umum digunakan adalah algoritma MD5. Algoritma ini dibuat oleh Ron Rivest, sebagai perbaikan dari generasi sebelumnya (MD4), setelah MD4 berhasil diserang oleh kriptanalis. Algoritma MD5 menerima masukan string dengan panjang berapapun dan menghasilkan message digest yang panjangnya 128 bit. Berikut ini adalah gambar proses MD5 yang menghasilkan *message digest* dengan panjang 128 bit:



2.3 Pemanfaatan Teknologi Internet

Pada era sekarang ini, disaat teknologi internet telah menjadi sesuatu yang wajar disemua kalangan, akses terhadap internet pun menjadi semakin mudah dan murah. Semua orang dari berbagai kalangan kini dapat memanfaatkan internet untuk kebutuhan masing-masing, mulai dari kepentingan bisnis hingga kepentingan sosialisasi. Disamping banyaknya manfaat yang dapat diperoleh dari kemudahan akses internet ini, banyak pula kerugian yang dihasilkan. Salah satunya adalah banyaknya tindakan penipuan ataupun pemalsuan. Contoh tindakan pemalsuan yang kini sedang marak adalah tindakan *phishing*, yaitu duplikasi website dengan alamat server yang berbeda. Salah satu kasus *phishing* di Indonesia yang cukup dikenal adalah kasus website klikbca. Pelaku *phishing* website klikbca membuat website dengan tampilan yang sama persis dengan website asli klikbca, namun dengan alamat website yang berbeda, seperti kilkbca atau clickbca. Tujuannya adalah ketika ada nasabah yang ingin mengakses situs klikbca namun tidak tahu pasti alamat situs yang sebenarnya, mereka ‘terpeleset’ menuju situs palsu yang telah dibuat dan melakukan transaksi disana. Akibatnya, segala informasi nasabah dapat dengan mudah diperoleh oleh pelaku *phishing* yang tidak bertanggungjawab tersebut.

Untuk menanggulangi masalah ini, maka di Amerika ada suatu perusahaan yang menyediakan layanan verifikasi website. Perusahaan tersebut adalah Verisign. Teknik yang digunakan oleh Verisign dalam melakukan verifikasi website sangatlah sederhana. Secara garis besar, proses yang terjadi pada Verisign adalah sebagai berikut :

- Server Verisign menyimpan data nilai hash dari website-website yang menjadi pelanggannya.
- Apabila ada seorang pengguna internet yang akan mengunjungi suatu situs yang telah terdaftar pada Verisign, maka pengguna tersebut dapat memastikan bahwa situs yang dikunjunginya itu asli dengan cara melakukan verifikasi, baik dengan cara menekan tombol verifikasi yang biasanya disediakan di situs ataupun dengan mengunjungi situs Verisign.
- Dalam waktu singkat, server Verisign akan melakukan pencarian dan pencocokan terhadap situs yang bersangkutan dengan nilai *hash*-nya pada server. Setelah proses selesai, akan ditampilkan hasil verifikasi, apakah suatu situs otentik atau tidak, sesuai dengan kecocokan nilai *hash*-nya dengan nilai *hash* yang telah tersimpan di server.

3. Implementasi

Dengan ide yang serupa dengan Verisign, penulis memiliki suatu gagasan untuk membangun suatu sistem verifikasi ayat Al Quran. Seperti telah diuraikan dalam bagian pendahuluan, saat ini banyak ditemukan potongan-potongan ayat Al Quran dalam bentuk digital (teks komputer) di internet, yang ternyata salah dalam penulisannya, atau bahkan malah dipalsukan.

Sebagai solusi dari permasalahan ini, penulis mengusulkan suatu konsep aplikasi berbasis web yang berperan sebagai pengecek (*verifier*) ayat Al Quran. Karena berbasis web, maka pengguna di seluruh dunia dapat memanfaatkan aplikasi ini. Cara kerja aplikasi ini sangatlah sederhana. Pihak server menyimpan data nilai hash seluruh ayat Al Quran dalam database. Sedangkan dalam aplikasi client, pengguna akan diminta memasukkan teks ayat Al Quran yang ingin dites keasliannya, lengkap dengan informasi surat dan ayatnya. Setelah informasi yang diberikan telah lengkap, maka data akan dikirimkan ke server untuk kemudian dilakukan pengecekan dengan cara menghitung nilai *hash* dari ayat yang diberikan oleh pengguna dan mencocokkannya dengan nilai *hash* yang tersimpan di server sesuai dengan informasi surat dan ayat yang diberikan oleh pengguna. Setelah proses pengecekan selesai, aplikasi akan memberikan pesan sesuai dengan hasil pengecekan ayat tersebut. Apabila hasilnya menyatakan berbeda, maka server akan memberikan teks ayat yang asli.

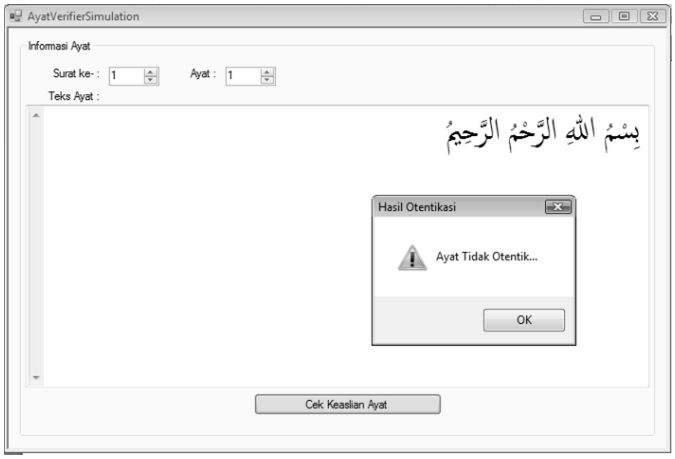
4. Pengujian dan Analisis

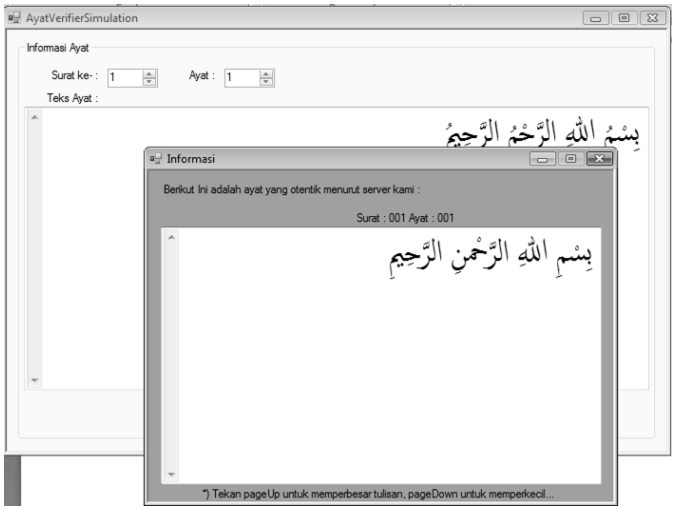
Untuk keperluan pengujian, penulis hanya mengimplementasikan aplikasi ini dalam bentuk aplikasi desktop yang berupa simulasi, belum dalam bentuk aplikasi web. Namun aplikasi simulasi yang telah penulis buat memiliki fungsionalitas yang sama dengan konsep berbasis web yang penulis usulkan. Karena keterbatasan waktu, dalam aplikasi yang penulis buat hanya dapat melakukan verifikasi terhadap surat Al Fatihah (surat pertama). Pada sub-sub bab berikut ini akan penulis jabarkan hasil pengujian dan analisis yang dilakukan.

4.1 Pengujian Pertama

Pada pengujian pertama, penulis memberikan contoh memasukkan ayat yang benar. Yaitu ayat pertama Al Fatihah. Setelah memasukkan ayat yang sesuai dan menekan tombol pengecekan keaslian ayat, maka akan muncul pesan bahwa ayat yang dimasukkan adalah otentik.

4.2 Pengujian Kedua





Pada pengujian kedua ini, penulis memasukkan ayat yang salah. Beberapa harakat diganti dan kata ketiga juga dimodifikasi. Setelah menekan tombol otentikasi ayat, maka akan muncul pesan bahwa ayat yang dimasukkan oleh pengguna adalah tidak otentik (gambar atas) dan aplikasi akan memberikan teks ayat yang otentik kepada pengguna (gambar bawah).

5. Kesimpulan dan Saran Pengembangan

Kesimpulan yang dapat diambil dari konsep ini adalah bahwa algoritma MD5 terbukti efektif. Sifat sensitifitas algoritma MD5 terhadap perubahan sangatlah cocok dengan sifat bahasa arab yang juga sensitif terhadap perubahan.

Dengan adanya suatu server yang menyimpan seluruh data nilai hash dan ayat Al Quran, maka keraguan dari seseorang atas keaslian suatu ayat dapat terjawab. Disamping itu, karena aplikasi yang penulis usulkan adalah berbasis web, maka dapat diakses dari seluruh dunia, sehingga lebih luas kegunaannya.

Karena operasi yang digunakan hanyalah pengecekan string, yaitu antara nilai hash di server dengan nilai hash ayat yang diberikan pengguna, sedangkan penghitungan nilai hash ayat masukan pengguna dilakukan sendiri oleh komputer pengguna, maka server tidak akan terbebani terlalu berat. Sehingga kinerja server dapat menjadi optimal untuk melayani permintaan banyak pengguna sekalipun.

Untuk pengembangan lebih lanjut, penulis menyarankan agar dalam percobaan digunakan ayat-ayat yang lebih bervariasi panjangnya dan percobaan kesalahannya. Sehingga hasil pengujian akan lebih terpercaya (*reliable*).

DAFTAR PUSTAKA

[1] Munir, Rinaldi. *Kriptografi*, Penerbit Informatika, 2006.