APLIKASI QUIZ PSIKOLOGIS BERBASIS WEBSITE DENGAN PENGAPLIKASIAN ALGORITMA DES

Ajie K. Wardhana[1)], Fariz D. Nurzam[2)], M. Kusnawi[3)]

[1), 2), 3)] Teknik Informatika STMIK AMIKOM Yogyakarta
Jl Ring road Utara, Condongcatur, Sleman, Yogyakarta 55281
Email : ajie0022@students.amikom.ac.id[1)], fariz0020@students.amikom.ac.id[2)], khusnawi@amikom.ac.id[3)]

Abstrak

Dalam praktik rehabilitasi psikologi, sebelum memulai praktik seorang psikolog terlebih dahulu melakukan screening kepada client guna mengetahui kondisi kesehatan mental terkini, mendiagnosa kelainan mental yang dialami, serta menjadi dasar dalam praktik rehabilitasi mental yang akan dilakukan. Screening dapat dilakukan dengan berbagai cara salah satunya adalah dengan memberikan quiz atau pertanyaan mengenai kondisi kesehatan mental maupun kebiasaan yang dialami atau dilakukan oleh client. Peranan screening dalam praktik rehabilitasi mental ini sangat penting oleh sebab itu data diri client maupun hasil dari tahap screening ini harus dirahasiakan.

Dalam paper ini termuat bagaimana quiz screening kesehatan mental berbasis elektronik dapat menjaga data-data yang adadi dalamnya meliputi data diri client, hasil jawaban, serta saran dan kesimpulan screening. Data tersebut akan dienkripsi sehingga data yang tersimpan dalam basis data merupakan data sandi. Setiap client memiliki angka kunci hasil generate yang digunakan untuk proses enkripsi dekripsi data dirinya sebagai kunci client.Dalam quiz tersebut juga dilakukan generate angka unik yang akan dikirimkan kepada psikolog untuk mengenkripsi dekripsi data sandi dari hasil quiz client sebagai kunci quiz.

Penerapan kriptografi pada kasus kali ini mengguanakan algoritma DES (Data Encryption Standard) yang merupakan algoritma kunci simetris standar. Berdasarkan pada penerapannya, algoritma DES telah berhasil melakukan enkripsi dekripsi dengan perpaduan kunci client terhadap kunci quiz yang mana untuk dapat melihat data client yang sebenarnya, harus melewati tahap dekripsi kunci client dalam bentuk data sandi menggunakan kunci quiz, kemudian mendekripsi data sandi yang ada dengan kunci client yang sebenarnya.

Kata kunci: *Screening, Rehabilitasi, Kesehatan Mental, Kriptografi, Algoritma DES*

1. Pendahuluan

Keamanan data merupakan suatu komponen yang paling utama dalam sebuah sistem aplikasi. Salah satu contoh penerapannya pada sebuah aplikasi yang berhubungan dengan dunia medis dan mengandung data-data dari pasien yang sangat riskan serta dapat disalahgunakan. Dari hal tersebut, banyak cara dalam menjaga keamanan data tersebut salah satunya adalah dengan menggunakan ilmu kriptografi. Kriptografi adalah ilmu yang mempelajari bagaimana supaya pesan atau dokumen kita aman, tidak bisa dibaca oleh pihak yang tidak berhak. Dalam pengembangannya, kriptografi juga digunakan untuk identifikasi pengirim pesan dengan tanda tangan digital (*fingerprint*)[1].

Dalam kriptografi terdapat banyak algoritma baik itu algoritma konvensional maupun modern. DES (Data Encryption Standard) merupakan salah satu metode algoritma modern yang berfungsi untuk mengenkripsi data yang dikeluarkan oleh Federal Information Processing Standard (FIPS) 46 – 1 Amerika Serikat. Metode DES ini memiliki blok kunci 64 bit tetapi yang digunakan dalam proses eksekusi adalah 56 bit. Pada awalnya dirancang untuk implementasi secara hardware[2].

Adapun penelitian sebelumnya mengenai penggunaan pengaman data dengan metode alogaritma DES (Data Encyription Standart) yang telah dilakukan oleh Rifaidi, Zainal, Dyna (2014) yang berjudul "Rancangan Bangun Multifile Locker Application Menggunakan Metode Data Encryption Standart". Proses enskripsi pada file menggunakan metode Data Encryption Standart mengubah struktur asli hexa dari file sehingga file dalam keadaan teracak dan sulit dipahami[3].

Dari hasil penelitian tersebut, kami ingin menguji kembali mengenai metode DES dengan penerapan yang berbeda yaitu membuat aplikasi quiz psikologis berbasis website dengan pengaplikasian alogritma DES. Dengan menerapkan algoritma DES ini ke dalam sistem, maka data dari *client* dapat dienkripsi dan hanya dokter yang bersangkutan yang memiliki kuncinya.

Tujuan dari penelitian ini adalah mengaplikasikan algoritma DES pada website guna tes psikologis mental dan mengoptimalkan algoritma DES agar seluruh data

terkait lebih terjaga keamanannya. Selain itu, dari keamanan yang terjamin dapat menghalau *cracker* yang ingin mencuri dan menyalahgunakan data-data user.

2. Pembahasan

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dikirim diubah sedemikian rupa sehingga tidak mudah disadap. Jadi enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plainteks*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*) (BUDI RAHARJO, 2002). Algoritma DES merupakan algoritma enkripsi yang paling banyak digunakan di dunia yang diadopsi oleh NIST (National Institue of Standards and Technology) sebagai standar pengolah informasi federal AS. Data *plaintext* dienkrip dalam blok-blok 64 bit menjadi 64 bit data ciphertext menggunakan kunci 56 bit kunci internal (*internal key*). DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk *block cipher*[4].

Skema global dari algoritma DES adalah sebagai berikut:

1. Blok Plaintext dipermutasi dengan matriks permutasi awal (initial permutation atau IP).

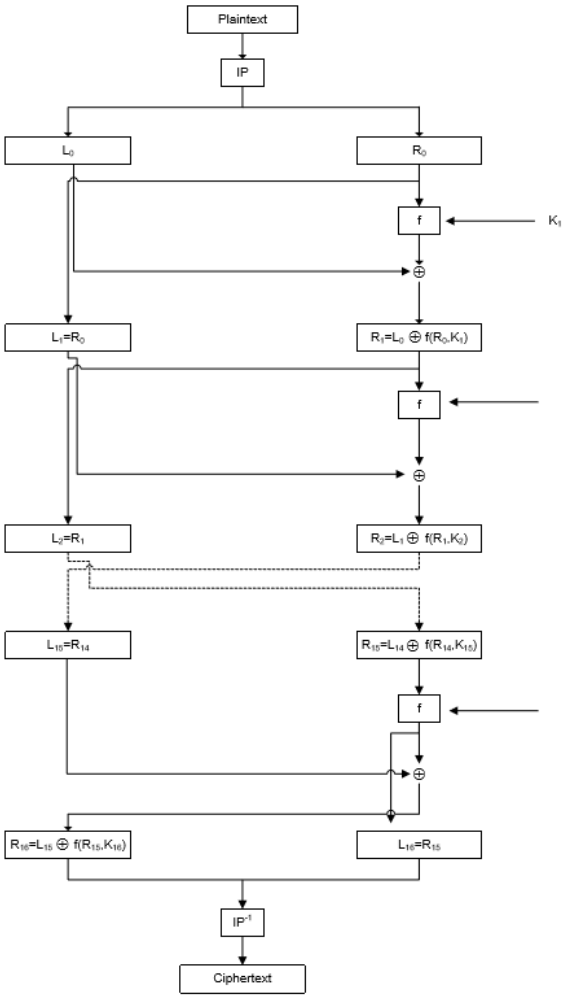
2. Hasil permutasi awal kemudian di-enciphering sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.

3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers Initial Permutation atau IP-1) menjadi blok ciphertext. Untuk lebih sederhananya dapat dilihat pada gambar 1. Skema Dasar Alogaritma DES

Dalam 16 putaran DES. Pada setiap putaran i, blok R merupakan masukan untuk fungsi transformasi yang disebut f. Pada fungsi f, blok R dikombinasikan dengan kunci internal Ki. Keluaran dari fungsi f di-XOR-kan dengan blok L untuk mendapatkan blok R sebelumnya.

Ini adalah satu putaran DES. Secara matematis, satu putaran DES dinyatakan sebagai berikut:

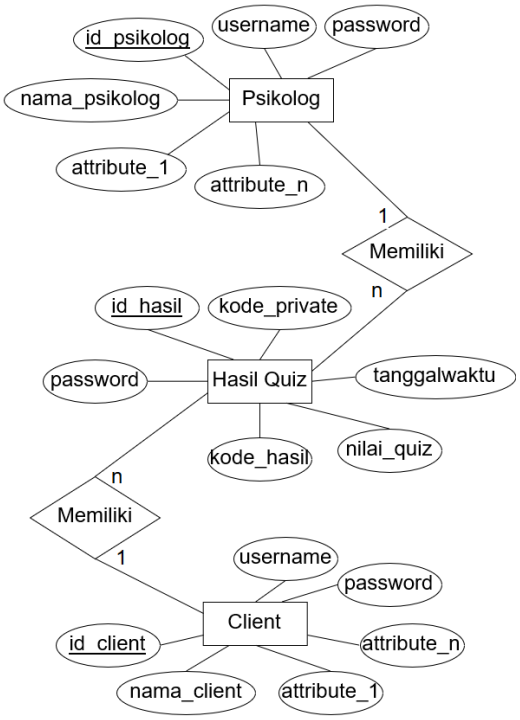
$$Li = Ri - 1$$
$$Ri = Li - 1 \oplus f(Ri - 1, Ki) \ldots..(1)$$



Gambar 1. Skema Dasar Algoritma DES

2.1. Entity Relation Diagram

Entity Relation Diagram merupakan sebuah model yang menunjukan hubungan dalam basis data. Entitas dalam ERD merupakan komponen data dalam basis data. Entity Relation Diagram dapat dilihat pada gambar-2.

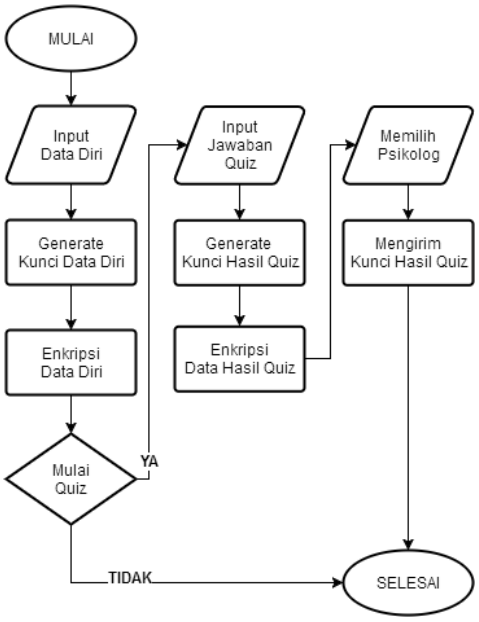


Gambar 2. Entity Relation Diagram

Dalam gambar-2 dijelaskan bahwa *client* akan mengakses quiz dengan melakukan login terlebih dahulu. Setiap *client* memiliki psikolog mereka masing-masing. Setelah login, *client* akan memulai mengerjakan soal-soal quiz yang ada. Ketika *client* sudah selesai mengerjakan quiz, maka dengan otomatis sistem akan mengenkripsi data-data baik itu data personal maupun data quiz *client.* Lalu, hasil dari psikotes tersebut akan dikirim ke psikolog yang bersangkutan. Psikolog akan mendapatkan kunci untuk melakukan dekripsi terhadap data *client*.

2.2. Flowchart Enkripsi

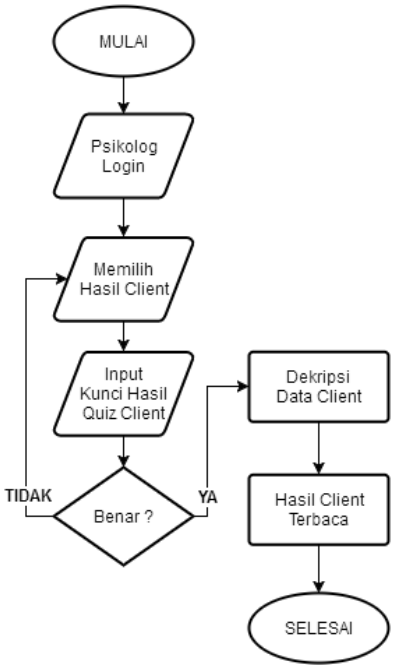
Flowchart merupakan tipe diagram yang mempresentasikan sebuah algoritma dalam suatu sistem. Dalam flowchart akan mempresentasikan langkah dalam bentuk kotak, dan anak panah yang mempresentasikan urutan dengan menghubungkan setiap langkah. Algoritma aplikasi dapat dilihat lebih jelasnya pada gambar 3.



Gambar 3. Flowchart Enkripsi

2.3. Flowchart Dekripsi

Algoritma dekripsi pada aplikasi ini dapat dilihat pada gambar 4 di bawah ini.



Gambar 4. Flowchart Dekripsi

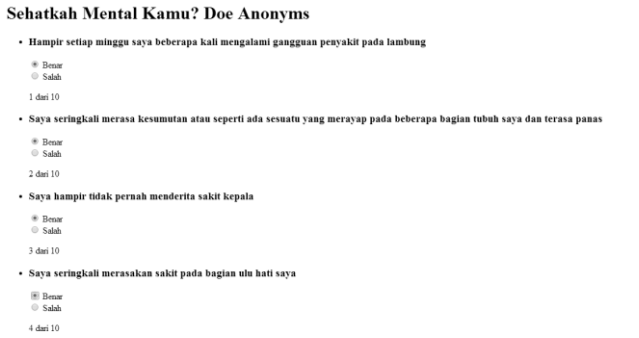
2.4. Implementasi

Pembuatan aplikasi quiz ini adalah menggunakan bahasa pemrograman PHP. PHP singkatan dari *Hypertext Preprocessor* adalah bahsa server-side scripting yang menyatu dengan HTML untuk membuat

halaman web yang dinamis. Karena php merupakan server side scripting maka sintaks dan perintah- perintah PHP akan dieksekusi di server kemudian hasilnya akan dikirim ke browser[5].

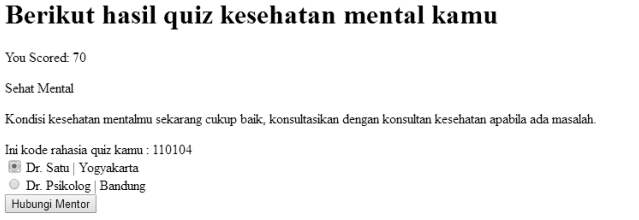
Pada gambar 5, 6, dan 7, merupakan interface ketika *client* melakukan login, mengerjakan soal, dan hasil dari test. *Client* akan melakukan login terlebih dahulu. Setelah *client* melakukan login, *client* akan memasuki interface soal yang akan mereka kerjakan. Ketika mereka sudah selesai mengerjakan soal, sistem akan menampilkan hasilnya.

Gambar 5. Gambar Halaman Daftar



Gambar 6. Gambar Halaman Quiz

interface soal dari quiz dimana *client* hanya perlu memilih 2 jawaban yang mereka alami.

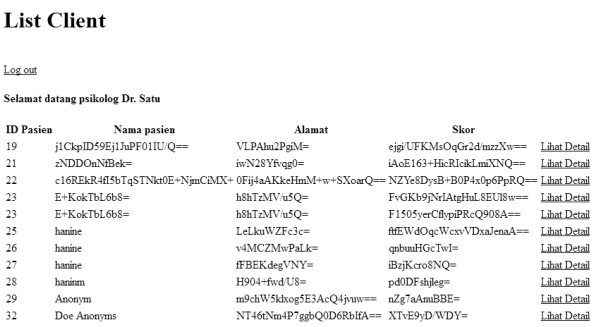


Gambar 7. Gambar Hasil Quiz

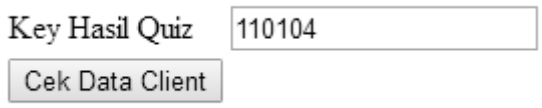
Tampilan untuk memilih psikolog. Psikolog yang terpilih akan dapat kiriman *key* dari *ciphertext* hasil enkripsi melalui *e-mail* mereka dapat dilihat pada gambar 7.

Gambar 8. Gambar Halaman Login Psikolog

Gambar 8 adalah tampilan login dari psikolog. Psikolog yang bersangkutan hanya perlu menginputkan username dan password mereka. Setelah mereka melakukan login, psikolog akan memasuki *interface list client* dimana terdapat semua data client yang mengikuti test. *Interface list client* lebih jelasnya dapat dilihat pada gambar-9 dibawah.

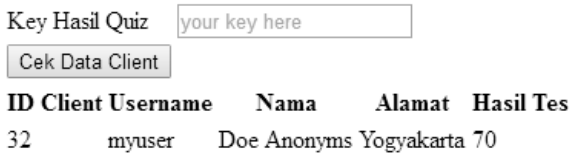


Gambar 9. Gambar Daftar Client



Gambar 10. Gambar Input Key Hasil Quiz

Ketika psikolog akan melakukan dekripsi, psikolog hanya perlu menginputkan kunci. Interface dapat dilihat pada gambar 10. Setelah menginputkan kunci, hasil akan terdekripsi. Lebih jelasnya dapat dilihat pada gambar 11.



Gambar 11. Gambar Hasil Dekripsi Data

2.5. Hasil Uji Aplikasi

Setelah melakukan pembuatan aplikasi, penulis melakukan uji aplikasi. Pada tabel 1 mengenai hasil uji aplikasi pada beberapa fungsi. *Fungsi pertama*, ialah melakukan Registrasi Client dengan cara pengujian pada *client* untuk mengisi form pendaftaran pada halaman daftar dengan harapan hasil uji data dalam form dapat tersimpan dalam basis data dan hasil yang didapat valid. *Kedua*, melakukan Quiz Online dengan cara pengujian pada *client* untuk mengerjakan quiz psikologis setelah mendaftar dengan harapan hasil uji sistem dapat menyimpan hasil jawaban client dan didapati hasil valid. *Ketiga*, menguji Hasil Quiz dengan cara pengujian client mengerjakan quiz, akan ditampilkan hasilnya langsung dengan harapan hasil ujil quiz client dapat menampilkan angka, keterangan kesehatan mental dan didapati hasil uji valid. *Keempat*, menguji Psikolog Login dengan cara pengujian psikolog menginputkan *username* dan *password* pada halaman dengan harapan hasil uji *username* dan *password* yang sesuai akan dialihkan ke halaman daftar *client* dan didapati hasil yang valid. *Kelima*, menguji Daftar Client dengan cara penguji menyesuaikan daftar nama *client* dengan daftar nama yang ada pada basis data dengan harapan hasil uji sistem dapat menampilkan daftar client yang telah dienkripsi dan didapati hasil uji yang valid. *Keenam*, menguji Detail Hasil Quiz dengan psikolog melakukan input kunci hasil quiz sesuai id quiz dengan harapan uji apabila kunci benar, sistem dapat menampilkan data hasil quiz client yang telah didekripsi dan didapati hasil uji valid.

Tabel 1. Tabel Hasil Uji Aplikasi

No.	Fungsi yang diuji	Cara pengujian	Harapan hasil uji	Hasil uji
1.	Registrasi Client	Client mengisi form pendaftaran pada halaman daftar	Data dalam form dapat tersimpan dalam basis data	Valid
2.	Quiz Online	Client mengerjakan quiz psikologis setelah mendaftar	Sistem dapat menyimpan hasil jawaban client	Valid
3.	Hasil Quiz	Setelah client mengerjakan quiz, akan ditampilkan hasilnya langsung	Hasil quiz client dapat menampilkan angka dan keterangan kesehatan mental	Valid
4.	Psikolog Login	Psikolog input username dan password pada halaman login psikolog	Username dan password yang sesuai akan dialihkan ke halaman daftar client	Valid
5.	Daftar Client	Menyesuaikan daftar nama client dengan daftar nama yang ada pada basis data	Sistem dapat menampilkan daftar client yang telah dienkripsi	Valid
6.	Detail Hasil Quiz	Psikolog melakukan input kunci hasil quiz sesuai dengan id quiz	Apabila kunci benar, dapat menampilkan data hasil quiz client yang telah didekripsi	Valid

3. Kesimpulan

Setelah penulis melakukan penelitidan dan juga berdasarkan referensi-referensi yang ada, data dan hasil analisis serta melalui fakta yang telah diuraikan pada bab-bab terdahulu, maka penilis mengangkat kesimpulan sebagai berikut:

1. Dari keseluruhan fungsi pada hasil uji aplikasi quiz psikologis berbasis website menggunakan algoritma DES menghasilkan data yang valid dan sesuai dengan harapan hasil uji aplikasi.

2. Metode DES (*Data Encryption Standard*) dapat menjadi rujukan dalam proses kriptografi (enkripsi dan dekripsi) dengan tingkat keamanan yang cukup rumit (kompleks) dan aman dalam penyimpanan data.

3. Dengan penggunaan metode DES dapat membantu dalam segi keamanan data untuk para *client*.

Daftar Pustaka

[1] Kurniawan, Yusuf. 2004. *Kriptografi (Keamanan Internet dan Jaringan Komunikasi)*. Bandung: Informatika.
[2] Sweetania, Dhian. *Implementasi Enkripsi Data Berbasis Alogaritma DES.* Sistem Informasi Jurnal Online, hal 1. http://dhian_sweetania.staff.gunadarma.ac.id/Downloads/files/35350/IMPLEMENTASI-ENKRIPSI-DATA-BERBASIS-ALGORITMA-DES.pdf. (diakses 29 november 2016 pukul 11.30 wib).
[3] Akbar Rifaidi, Arifin Zainal,dan Khairina Dyna Marisa. 2014. Rancang Bangun Multiple Locker Application Menggunakan Metode Data Encryption Standard. Jurnal Online, Vol. 9, No. 2, Juni 2014.
[4] Primartha, Rifkie. 2011. Penerapan Enkripsi dan Dekripsi File Menggunakan Alogaritma Data Encryption Standard (DES). Sistem Informasi Jurnal Online, 3 (2): 373. http://ejournal.unsri.ac.id/index.php/jsi/article/view/739. (diakses 4 desember 2016 pukul 22.00 wib).
[5] Aryanto. A, dan Tjendrowasono. Tri I. 2012. Pembangunan Sistem Penjualan Online Pada Toko Indah Jaya Furniture Surakarta. Speed Jurnal Online, 10 (6): 57. http://ijns.org/journal/index.php/speed/article/view/1099. (diakses 6 desember 2016 pukul 15.30 wib). [2] P.M. Morse and H. Feshback, *Methods of Theoretical Physic*, New York: McGraw Hill, 1953.

Biodata Penulis

Ajie Kusuma Wardhana, Mahasiswa S-1 Jurusan Teknik Informatika Program International STMIK AMIKOM Yogyakarta.

Fariz Dzulfiqar Nurzam, Mahasiswa S-1 Jurusan Teknik Informatika Program International STMIK AMIKOM Yogyakarta.

Muhammad Kusnawi, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta, lulus tahun 2006. Memperoleh gelar Magister Engineering (M.Eng) Program Pasca Sarjana Magister Teknologi Informasi Teknik Elektro Universitas Gajah Mada Yogyakarta, lulus tahun 2011.Saat ini menjadi Dosen di STMIK AMIKOM Yogyakarta.