PENERAPAN ALGORITMA GENETIKA DAN FUNGSI HASH SHA 1 PADA SISTEM KEAMANAN DOKUMEN DALAM FOLDER

Sandi Saputra[1], Susandri[2]
STMIK-Amik Riau, Teknik Informatika
Jl. Purwodadi indah Km 10 panam pekanbaru, Riau
Telp 0761 7047091, fax 0761 7047891
Email :[1]sandisaputra@stmik-amik-riau.ac.id, [2]susandri@stmik-amik-riau.ac.id

ABSTRAK

Penggunaan komputer saat ini sudah saling terkoneksi satu sama lain dengan memanfaatkan berbagai mdia transmisi. Semntara kemanan data dalam komputer sangat penting untuk mencegah kehilangan dan kerusakan data dari pihak yang tidak berkepentingan. Tujuan penelitian merancang suatu apliaksi sistem yang dapat mengamankan dokumen yang disimpan dalam folder sehingga tidak mudah hilang, terhapus atau dicuri. Penelitian ini dilakukan dengan menggunakan algortitma genetika dan fungsi Hash SHA1. Algoritma genetika digunakan untuk mengacak suatu kata dari kunci key yang akan digunakan oleh user dan fungsi Hash SHA 1 akan mengenkrip key yang telah diacak sebelumnya sehingga folder mendapatkan keamanan lebih dengan key atau password yang sulit ditebak. Penelitian ini telah menghasilkan suatu aplikasi sistem yang dapat memberikan kemanan terhadap data dalam suatu folder sehingga bisa menjadi salah satu alternatif pilihan untuk kamanan data bagi pengguna komputer.
***Kata Kunci**: Kemananan Folder, Algoritma Genetika, SHA 1*

ABSTRACT

The use of computers is now inter-connected with each other by utilizing various transmission media . While the data in the computer security is very important to prevent loss and damage of data from unauthorized parties. The research objective apliaksi design a system that can secure documents that are stored in a folder that is not easily lost, deleted or stolen . This research was conducted by using genetics algortitma and SHA1 Hash function. Genetic algorithms are used to randomize a key word from the key that will be used by the user and the SHA 1 hash function will encrypt keys that have been encrypted in advance so that the folder get more security with a key or a password that is difficult to guess . This research has resulted in an application system that can provide security of data in a folder so that it can become an alternative choice to secure data to the user 's computer
Keywords: Folder security , Genetic Algorithm , SHA 1

1. PENDAHULUAN

Keamanan merupakan suatu hal yang sangat diperlukan dalam kegiatan sehari-sehari dalam segala aspek. Hampir setiap aspek kegiatan manusia memerlukan sebuah keamanan seperti keamanan diri, keamanan dalam dunia kerja, keamanan untuk menjaga aset–aset pribadi, termasuk keamanan sebuah data. Penggunaan komputer saat ini sudah saling terkoneksi satu dengan yang lainnya melalui jaringan dengan berbagai media transmisi. Hal ini membuka peluang data-data penting yang digunakan bisa diakses oleh pengguna lainnya baik secara legal atau ilegal.

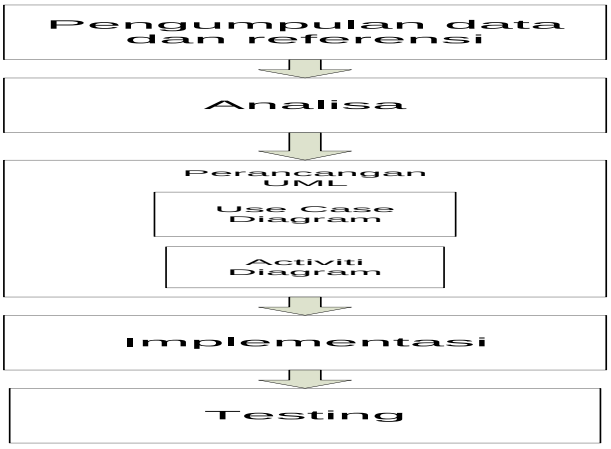
Untuk menjaga data-data penting yang tersimpan dalam komputer yang digunakan harus dikelola dengan mengelompokkan atau menghimpun data-data penting tersebut dalam suatu folder dan folder tersebut di lindungi atau diproteksi dengan suatu aplikasi yang dapat mencegah diakses oleh pengguna lain yang tidak berhak. Telah banyak penelitian untuk memproteksi data yang telah dilakukan diantaranya sri wayhuni[1] menggunakan SHA 1 untuk leglisasi Digital Signature ijazah, Candra[2] menggabungkan MD5, SHA-1 untuk meningkatkan fungsi proteksi data serta Magdalena[3] menggunakan Algoritma Genetika Pada Citra Digital utuk menjaga data citra binner yang berada dalam media penyimpanan. Bedasarkan pengamatan penulis dan literatur yang ada untuk saat ini belum ada yang menggabungkan algoritma genetika dan fungsi HASH SHA 1 yang diterapkan dalam menjaga keamanan data yang digunakan dalam folder komputer.

Penelitian ini bertujuan untuk merancang suatu aplikasi yang dapat melindungi atau menproteksi suatu folder komputer dari pengguna yang tidak diijinkan dengan menggunakan metode algoritma genetika untuk mengacak kunci yang digunakan dan metode SHA 1 untuk mengenkripsi kunci tersebut dalam suatu aplikasi

genetika untuk mengacak kunci yang digunakan dan metode SHA 1 untuk mengenkripsi kunci tersebut dalam suatu aplikasi.

2. METODE PENELITIAN

Pada penelitian ini dilakukan pengumpulan data dari referensi- referensi tentang perkembangan keamanan komputer pada masa sekarang ini dengan cara melakukan literatur review terhadap jurnal dan membaca buku serta mempelajari fungsi hash SHA 1 dan Algortima Genetika dalam membangun sebuah kemanan data. Selanjutnya dilakukan analisa kebutuhan pengguna dan perancangan dalam membangun sistem keamanan data. Selanjutnya dilakukan perancangan menggunakan alat bantu UML dengan tahapan uses case diagram untuk menggambarkan fungsi dalam suatu sistem dan siapa saja yang menggunakan fungsi tersebut. selanjutnya aktiviti diagram dirancang untuk menggambarkan aliran kerja sistem. Setelah tahapan tersebut dilakukan implementasi menggunakan bahasa pemograman visual basic dan pengujian program dengan cara pengujian modul-modul dan pemggabungan modul tersebut untuk pengujian secara keseluruhan.

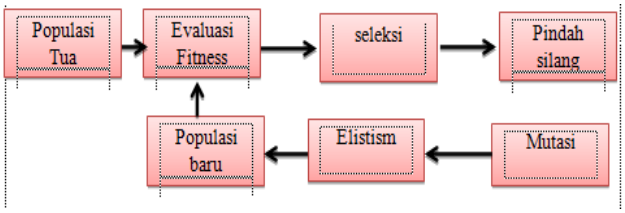


Gambar 1. Tahapan penelitian

3. PEMBAHASAN

3.1 Algoritma Genetika

Algoritma genetika dirancang untuk menyimulasikan proses-proses dalam sistem alam yang diperlukan untuk *evolusi*. Menurut Suyanto[4] algoritma adalah algoritma pencarian yang didasarkan pada mekanisme seleksi alamiah dan genetika. Algoritma digunakan sebagai algoritma pencarian parameter-paramenter optimal. Sedangkan Menurut Nita Rahmi[5] Proses-proses yang terjadi pada algoritma genetika sama dengan evolusi biologi. Proses-proses yang terjadi pada algoritma adalah



Gambar 2 Siklus algoritma genetika
(Sumber : PENS-ITS,2006)

3.1. Fungsi Hash

Fungsi hash menurut Wahana[6] adalah fungsi yang secara efisien mengubah *string input* dengan panjang berhingga menjadi string *output* dengan panjang tetap yang disebut nilai hash, sedangkan fungsi hash kriptografis adalah fungsi hash yang memiliki beberapa sifat keamanan tambahan sehingga dapat dipakai untuk tujuan keamanan data. Umumnya digunakan untuk keperluan autentifikasi dan integritas data. Sedangkan menurut menurut Rifki Sadikin[7] fungsi hash adalah sebuah fungsi yang masukannya adalah sebuah pesan dan keluaran sebuah sidik pesan

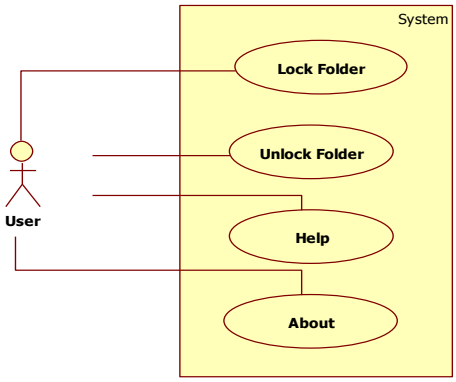
(message fingerprint). Sidik pesan juga sering disebut message digest. Fungsi hash dapat digunakan untuk mewujudkan layanan keutuhan data.

3.2. SHA 1

Menurut Komang[8] algoritma SHA-1 menerima masukan berupa *string* dengan ukuran 2^{64} bit.untuk setiap *string* akan menghasilkan keluaran sebanyak 160 bit dari *string* tersebut dan *string* tersebut disebut *message digest.* SHA-1 dikatakan aman karena proses SHA-1 dihitung seara inflesible untuk mencari *string* yang sesuai untuk menghasilkan *message digest* atau dapat mencari dua *string* yang berbeda yang akan menghasilkan *message digest* yang sama.

3.3. Use case diagram

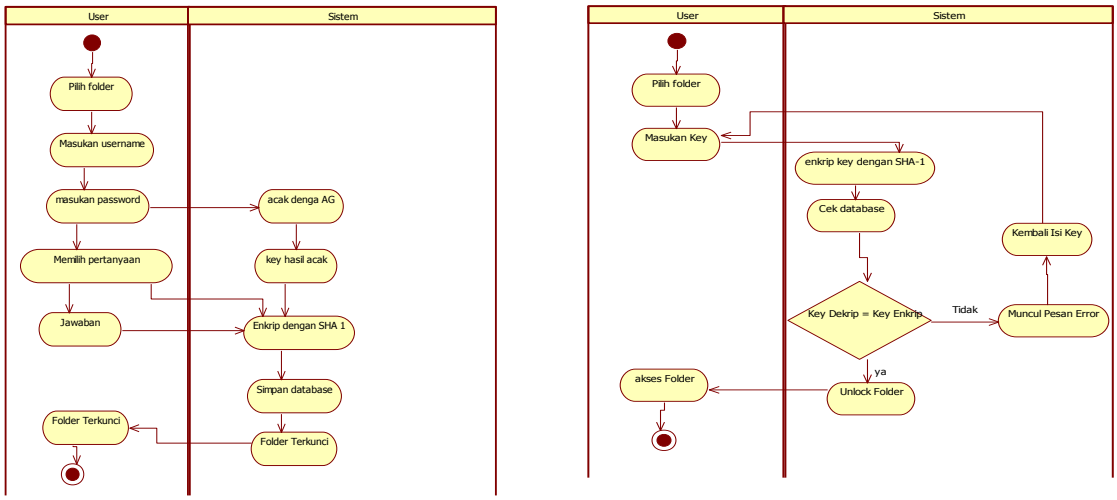
Rancangan sistem aplikasi untuk penelitian ini secara umum terdiri dari proses penguncian (lock folder) dan pembuka kunci (unlock folder) disertai proses untuk membantu user dalam menggunakan aplkasi dan pentunjuk penggunaan aplikasi. Rancangan tersebut dibuat menggunakan Use case diagram dengan bentuk racangan seperti gambar 3 berikut.



Gambar 3 Use case diagram

3.4. Activity diagram lock folder

Proses rancangan penguncian folder dibuat dalam suatu activity diagram yang menggambarkan aktivitas pengguna dan sistem ketika melakukan proses penguncian folder. Pada rancangan ini untuk mengunci sebuah folder pengguna memasukan username dan password, user name dan password diproses dengan algoritma genetika untuk menhasilkan kunci yang acak dan dienkripsi dengan SHA 1. Hasil enkripsi disimpan dalam database. Sementara pengguna juga diminta untuk memilih pertanyaan dan jawaban untuk memudahkan pengguna jika lupa password yang telah diacak dengan algoritma genetika.

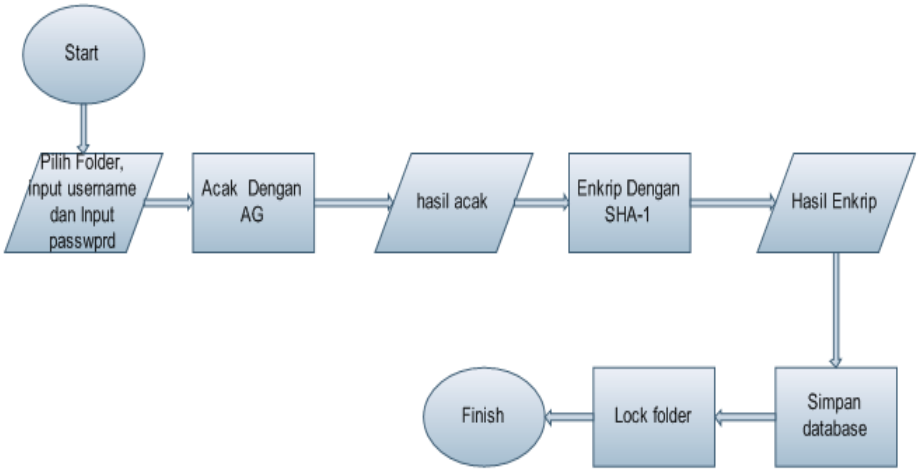


Gambar 4 Activity diagram lock dan unlock folder

sedangkan rancangan aktiviti untuk membuka kunci folder pengguna memasukan kata kunci dan sistem akan mendekrip dengan SHA 1 dan membandingkan hasil dekrip dengan data dalam database, jika sama kunci folder akan dibuka dan sebaliknya jika tidak sama akan ditampilkan pesan kesalahan dan diminta untuk memasukan kata kunci yang benar.

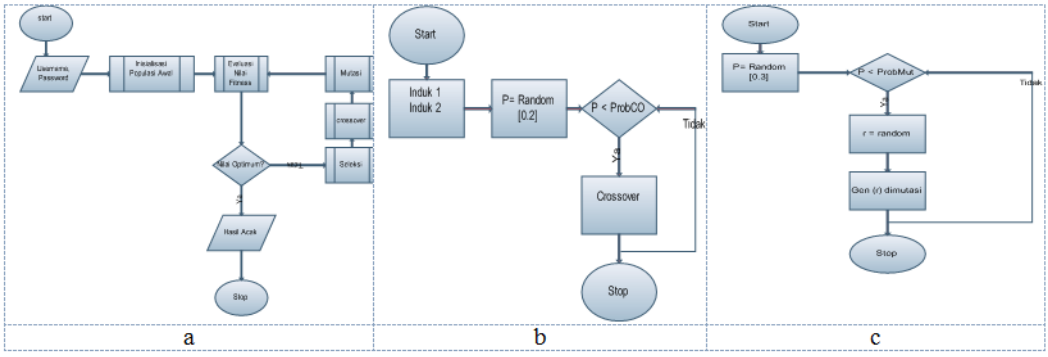
3.5. Flowchart

Rancangan flowchart dalam sistem ini terdiri dari flowchart sistem dan flowchart program. Pada flowchart sistem menggambarkan alur kerja sistem secara global dengan rancangan sebagai berikut :

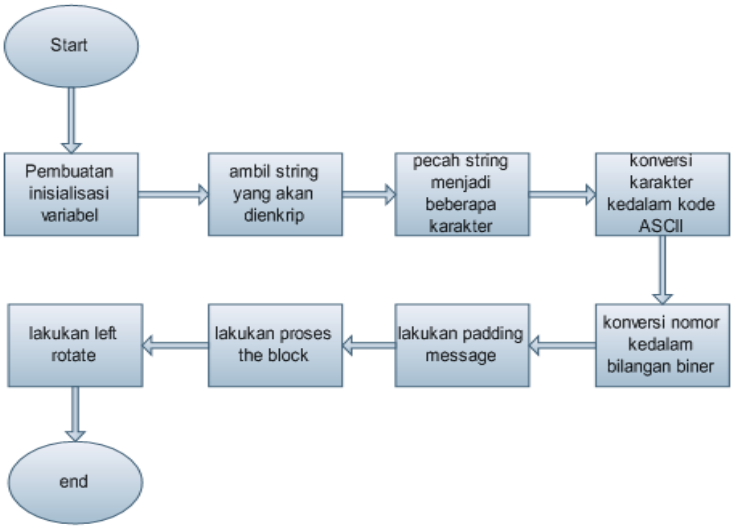


Gambar 5 Flowchart sistem

Sedangkan untuk flowchart program merupakan implementasi dari algoritma yang digunakan secara serial. Algoritma genetika digunakan untukk mengacak username dan password yang diinpukan hasil pengacakan yang merupakan output dari algoritma genetika manjadi input untuk proses selanjutnya yang merupakan proses enkripsi data dengan metode SHA1. Hasil enkripsi disimpan pada database yang aan digunakan untuk proses penguncian folder. Berikut flowchart program algoritma genetika dan fungsi SHA 1.



Gambar 6 a. Flowchart acak kata algoritma genetika, b flowchart proses crossover.
c. flowchart proses mutasi



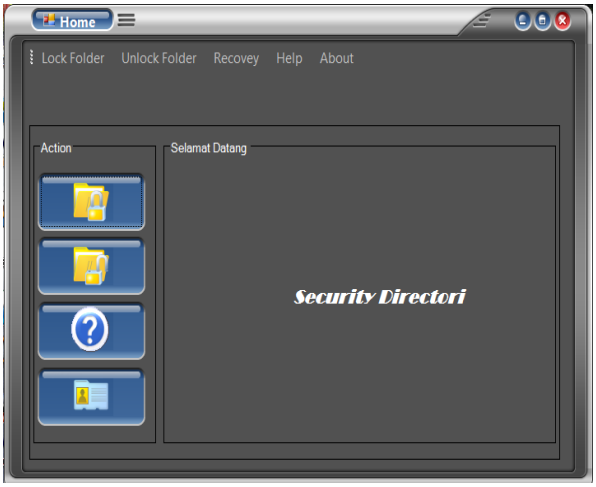
Gambar 7 Flowchart enkripsi SHA 1

3.6. Implementasi

Hasil rancangan di implemntasikan menggunakan bahasa pemograman visualbasic. Untuk memudahkan pengguna dalam memakai aplikasi ini dibuat tampilan interface yang sederhana, dan berikut tampilan-tampilan interface dari aplikasi yang dirancang.

1. Menu Utama

Pada tahap pengguna baru menjalankan sistem kemanan folder ini maka pengguna akan masuk ke tampilan menu utama seperti terlihat pada gambar 5 dibawah ini.



Gambar 8 Menu utama

Pada interface diatas terdapat menu utama dan tombol-tombol yang bisa digunakan untuk mengarahkan pengguna ke tampilan lainnya. Pengguna dapat klik menu lock folder atau tombol pertama pada pilihan action diatas untuk melakukan proses mengamankan atau mengunci folder. Tombol unlock atau menu unlock folder digunakan untuk melepas kunci folder, menu help atau tombol help digunakan untuk memberikan informasi penggunaan sistem keamanan ini dan menu about atau tombol about digunakan untuk memberikan informasi tentang aplikasi sistem keamanan ini.

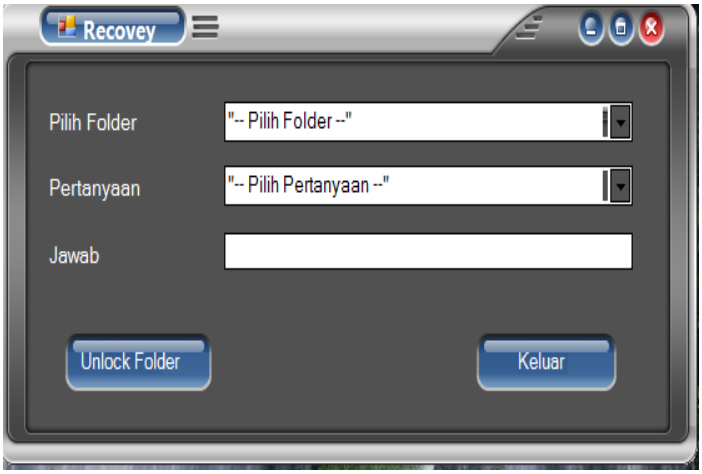
2. Lock dan unlock Folder

Gambar 9 Interface Lock dan unlock folder

Tombol *browse* digunakan untuk mencari dan memilih folder yang akan diamankan atau dikunci. Tombol acak akan melakukan proses algoritma genetika terhadap username dan password yang dinputkan oleh pengguna dan akan menghasilkan hasil optimal terbaik yang akan menjadi key dan dienkrip oleh SHA-1. Menu recovery harus diisi untuk membantu akses folder jika anda lupa password. Tombol lock folder untuk proses penguncian folder. Sedangkan untuk unlock folder pengguna akan memilih folder yang akan diunlock atau dilepas sistem keamanannya, lalu pengguna memasukan atau input kunci yang telah di acak pada porses lock folder. Tombol unlock folder digunakan untuk melepaskan kunci.

3. Recovery

Proses *recovery* digunakan jika pengguna lupa password. Pengguna tinggal memilih folder dan pertanyaan yang diinput ketika proses unlock. Pengguna juga harus benar menjawab pertanyaan tersebut. Tombol unlock folder digunakan untuk melepas kunci folder ketika semua sudah benar.



Gambar 10 interface Recovery

3.7. Pengujian Sistem

Pengujian fungsional dilakukan untuk menguji sistem yang baru adalah metode pengujian *alpha* Metode yang digunakan dalam pengujian ini adalah pengujian *black box* yang berfokus pada persyaratan fungsional dari sistem yang dibangun. Kasus dan hasil pengujian penelitian ini sebagai berikut:

1. Pengujian Menu Utama

Tabel 1
Pengujian Menu Utama

Kelas Uji	Skenario Uji	Hasil yang diharapkan	Kesimpulan
Menu Utama	Memilih Tombol *lock folder*	Menampilkan form lock folder	[√] Berhasil [ ] Tidak Berhasil
	Memilih Tombol *unlock folder*	Menampilkan form unlock folder	
	Memilih Tombol *help*	Menampilkan informasi help	
	Memilih Tombol about	Menampilan informasi tentang sistem keamanan folder	

2. Pengujian Menu Lock Folder

Tabel 2
Pengujian Menu Lock Folder

Kelas Uji	Skenario Uji	Hasil yang diharapkan	Kesimpulan
Menu *lock folder*	Ketika pengguna memilih tombol *lock folder*	Pengguna berada menu lock folder	[√] Berhasil [ ] Tidak Berhasil
	Mengisi id folder	Tersimpan pada database	
	Memilih folder	Menampilkan folder yang dipilh	
	Pengguna mengisi username dan password	Menghasilkan username dan password	
	Ketika memilih tombol acak	Menghasilkan kata acak	
	Ketika memilih dan memberikan jawaban	Tersimpan database	
	Ketika memilih tombol lock	Folder sudah terkunci	

3. Pengujian Menu Unlock Folder

Tabel 3 Pengujian
Menu Unlock Folder

Kelas Uji	Skenario Uji	Hasil yang diharapkan	Kesimpulan
Menu *unlock folder*	Ketika pengguna memilih tombol *unlock folder*	Pengguna berada menu unlock folder	[√] Berhasil [ ] Tidak Berhasil
	Memilih folder	Menampilkan folder yang dipilh	
	Pengguna mengisi password	Menghasilkan password	
	Ketika memilih tombol unlock folder	Folder sudah tidak terkunci	
	Ketika memilih tombol keluar	Keluar dari menu unlock folder	

4. Pengujian Recovery

Tabel 4
Pengujian Menu Recovery

Kelas Uji	Skenario Uji	Hasil yang diharapkan	Kesimpulan
Menu *recovey*	Ketika pengguna memilih menu *recovey*	Pengguna berada menu recovery	[√] Berhasil [ ] Tidak Berhasil
	Ketika pengguna memilih pertanyaan	Pertanyaan sama dengan yang tersimpan pada database	
	Menjawab pertanyaan	Jawaban harus sama dengan yang tersimpan pada database	
	Ketika memilih tombol unlock folder	Folder sudah tidak terkunci	
	Ketika memilih tombol keluar	Keluar dari menu recovery	

4. PENUTUP

Kesimpulan

Setelah melalui tahapan-tahapan Penelitian ini telah berhasil merancang suatu aplikasi untuk memproteksi data-data yang ditempatkan dalam folder komputer menggunakan algoritma genetika dan metode SHA 1 untuk mengacak dan mengenkripsi kata kunci yang digunakan. Aplikasi telah diuji melalui black box yang berfokus pada persyaratan fungsional dihasilkan dapat digunakan secara umum.

Saran

Untuk pengembangan penelitian penelitian disarankan menggunakan database yang lebih fleksibel dan fungsi has SHA yang lebih tinggi serta bisa digunakan dalam berbagai tipe sistem operasi.

DAFTAR PUSTAKA

[1]. Sri Wahyuni (2014). Penerapan Digital Signature DenganAlgoritma Sha-1 PadaSuratLegalisasiIjazah Dan TranskripNilai Mahasiswa, *Jurnal: pelita informatika budi darma, VII (2,) 31-38*

[2]. Candra Alim Sutanto (2010). Algoritma Fungsi Hash Baru dengan Menggabungkan MD5, SHA-1 dan Penyertaan Panjang Pesan Asli. *Makalah: IF3058 Kriptografi – Sem.IITahun 2010/2011 (ITB)*

[3]. Magdalena ariance Ineke Pakerang (2009). Kriptosistem Menggunakan Algoritma Genetika. *Jurnal : teknologi informasi-Aiti, 6(2), 118-134*

[4]. Suyanto. (2014). *Artificial Inteligence*. Bandung. Informatika Bandung

[5]. Rahmi, Nitia. (2007). *Penerapan Algoritma Genetik Untuk Meningkatkan Kerahasian Data Pada Algoritma Knapsack*. Makalah disajikan dalam lokakarya internal Pada Program Studi Teknik Informatika, Bandung : ITB.

[6]. Komputer, Wahana. (2010). *The Best Encryption Tools*. Jakarta: Wahana Komputer

[7]. Sadikin, Rifki. (2012). *Kriptografi Untuk Keamanan Jaringan*. Yogyakarta: Andi Offeset

[8]. Aryasa, Komang, Yeyasa Tommy Paulus (2014). Implementasi Secure Hash Algorithm-1 Untuk Pengamanan Data Library Pada Pemograman Java. *Jurnal Citec Jurnal 1 (1), 57-66*

[9]. Abdullah, Dahlan, Cut Ita Erliana 2012. Bisnis Rental Mobil Melalui Internet (E-COMMERCE) Menggunakan Algoritma SHA-1 (Secure Hash Algorithm-1*). Jurnal IJCSS 10(4),38-45*

[10]. Basuki, Achmad (2003). *Algoritma Genetika Suatu Alternatif Penyelesaian Permasalahan Searching, Optimasi dan Machine Learning*. Persentase penelitian, Surabaya : Politeknik Elektronik Negeri Surabaya

[11]. Haviluddin (2011). Memahami Penggunaan UML (Unified Modelling Language). *Jurnal Informatika Mulawarman, 6(1), 1-15*