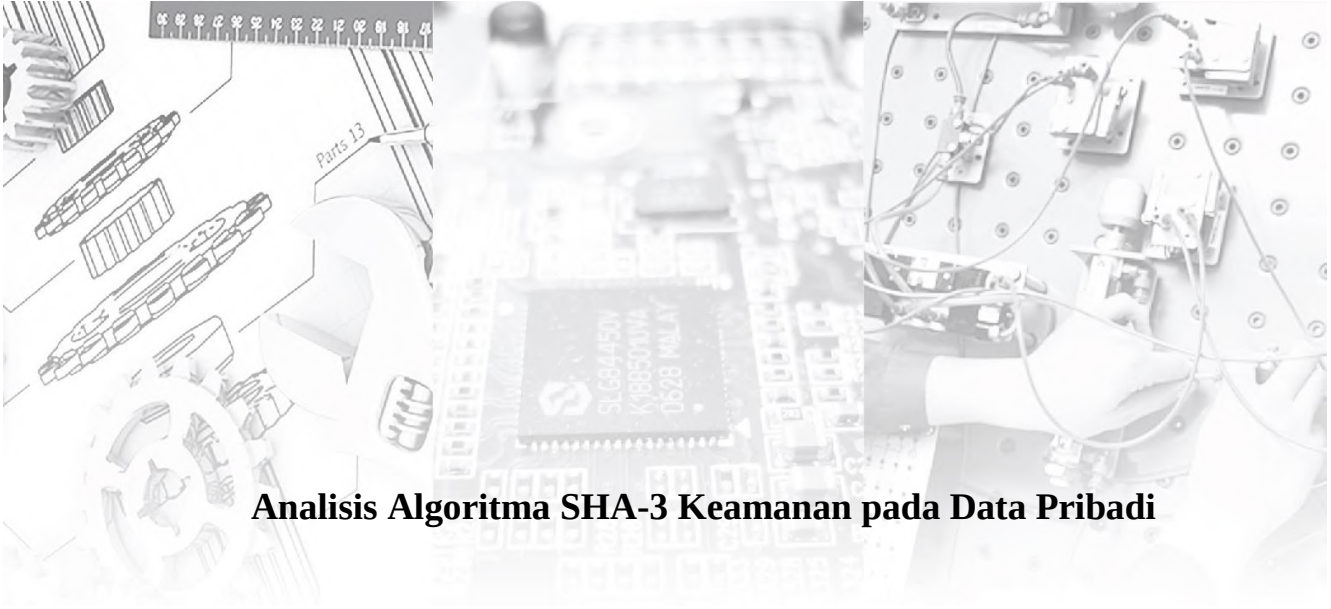


Analisis Algoritma SHA-3 Keamanan pada Data Pribadi

Morita Puspita Sari
Teknik Informatika, Universitas Amikom Yogyakarta
Email: morita.p@students.amikom.ac.id

Abstrak

Data Pribadi merupakan data yang harus dilindungi di era yang serba internet ini. Karena data tersebut berisi informasi penting yang bisa saja menjadi sasaran cyber crime.Beberapa tahun terakhir marak terjadi kasus penyerangan atau hacking yang mengambil data dan digunakan tidak semestinya oleh orang yang tidak bertanggung jawab. Dalam penelitian ini bertujuan untuk merancang sistem keamanan untuk mengamankan data tersebut.Salah satu algoritma yang dapat digunakan adalah algoritma SHA-3 untuk menjamin kerahasiaan dan keutuhan data.Pengujian yang dilakukan pada penelitian ini adalah validasi enkripsi dan dekripsi, waktu enkripsi dan dekripsi, fungsionalitas sistem dan non fungsionalitas sistem. Hasil pengujian pada penelitian ini menghasilkan, Pengujian test vector: Test Vector algoritme SHA-3, Pengujian performance Waktu, Pengujian waktu enkripsi data kosong, Pengujian waktu enkripsi data 1-char, Pengujian waktu enkripsi data fullchar, Pengujian waktu dekripsi data kosong, Pengujian waktu dekripsi data 1-char, Pengujian waktu dekripsi data fullchar, Pengujian validasi enkripsi dan dekripsi dan Pengujian Fungsional dan Nonfungsional.

Kata kunci: SHA-3, enkripsi, dekripsi

Abstract

Personal data is data that must be protected in this internet era. Because the data contains important information that could be the target of cyber crime. In the last few years, there have been cases of attacks or hacking that take data and be used inappropriately by irresponsible people. In this study, the aim of this research is to design a security system to secure the data. One of the algorithms that can be used is the SHA-3 algorithm to ensure the confidentiality and integrity of the data. The tests carried out in this study are

validation of encryption and decryption, encryption and decryption time, and system functionality. and non system functionality. The test results in this study produce, test vector test: Test Vector algorithm SHA-3, Time performance testing, Testing empty data encryption time, Testing 1-char data encryption time, Testing fullchar data encryption time, Testing time decryption. empty data, 1-char data decryption time testing, fullchar data decryption time testing, encryption and decryption validation testing and functional and non-functional testingmilliseconds for decryption.

Keywords: *SHA-3, encryption, decryption*

A. PENDAHULUAN

Di era teknologi internet ini pada akhirnya membuat semua dapat terhubung dengan sangat mudah.Namun dibalik kemudahan itu muncul permasalahan dimana kejahatan dunia maya semakin banyak, salah satu dari bentuk kejahatan dunia maya adalah seseorang dapat melakukan pengambilan data penting atau informasi rahasia yang tersimpan dalam media penyimpanan maupun yang terkirim melalui internet. Salah satu cara yang bisa dilakukan adalah dengan membuat sistem keamanan yang ketat supaya data dan informasi tersebut tidak dapat diambil oleh orang yang tidak bertanggung jawab.

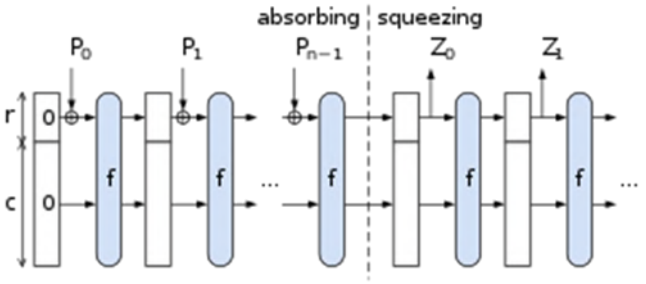
Penggunaan kriptografi dalam membangun keamanan data memang sudah lama digunakan. Kriptografi ini bertujuan agar data dan informasi yang kita miliki tidak dapat dilihat oleh orang lain yang tidak memiliki kepentingan. Salah satu algoritma kriptografi yang dapat diterapkan dalam studi kasus penelitian ini adalah Secure Hash Algorithm (SHA). Hash adalah fungsi yang menerima masukan *string* yang panjangnya sembarang dan menkonversinya menjadi *string* keluaran yang panjangnya tetap (*fixed*) (Agani, Hardjianto, & Virgian, 2016), sedangkan SHA adalah fungsi hash satu-arah yang dibuat oleh *NIST* (Abdullah & Erliana, 2012)). Berdasarkan penelitian yang dilakukan oleh Santoso

implementasi algoritma Hash SHA memiliki hasil yang sulit ditebak oleh hacker karena data yang dihasilkan tidak mungkin sama (Santoso, 2013).

Perbandingan metode antara Enkripsi RC4, SHA, dan MD5 bahwa algoritma SHA memiliki tingkat kekuatan yang lebih baik daripada metode RCA dan MD5, sehingga algoritma SHA direkomendasikan untuk digunakan dalam sistem keamanan data (Prasetyo & Hikmawan, 2016).

Terdapat varian Algoritma SHA yaitu SHA-0, SHA-1,SHA-2 dan SHA-3. Berdasarkan penelitian sebelumnya yang berjudul Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost dijelaskan bahwa penggunaan algoritma SHA-1 ditemukan kelemahan dalam mengamankan password pengguna yang tersimpan di database, sehingga penulis menggantikan algoritma SHA-1 tersebut dengan algoritma SHA-3. Dari pengujian *brute-force*, *avalanche effect,* dan pengujian waktu pemrosesan menunjukkan bahwa algoritma SHA-3 memiliki kinerja dan ketahanan yang lebih baik daripada algoritma SHA-1 (Kurniawan, Kusyanti, & Nurwarsito, 2017). Sehingga dari tinjauan pustaka tersebut batasan penelitian ini adalah menggunakan algoritma SHA-3 karena merupakan algoritma SHA yang paling baru dan kinerja yang lebih baik diantara varian lainnya.

Rancangan SHA-3 adalah menggunakan kontruksi spons yaitu data diserap ke dalam spons dimana dalam fase ini blok pesan XOR menjadi bagian dari status yang kemudian diubah keseluruhan menggunakan fungsi permutasi f kemudian hasilnya diperas dimana dalam fase ini blok keluaran dibaca dari subset yang sama dari keadaan dengan fungsi transformasi keadaan f.



Gambar 1. Kontruksi Algoritma SHA-3

Konstruksi spons untuk fungsi hash. P_i adalah masukan, Z_i adalah keluaran hash. "Kapasitas" *c yang* tidak digunakan harus dua kali lipat dari resistansi yang diinginkan terhadap benturan atau serangan preimage. Secara umum, dalam konstruksi spon terdapat dua fase, yaitu :

1. Fase absorbing, adalah fase pada proses dilakukan kepada semua pecahan di XOR-kan dan dari input masukan kemudian dilewatkan kedalam fungsi f dengan bagian bitrate dari state.
2. Fase squeezing, ada;ah fase pada proses untuk mendapatkan hasil keluaran yang dilakukan konkatenasi tkepada sejumlah bit tertentu dari hasil fungsi f sehingga jumlah bit konkatenasi tersebut sama dengan jumlah bit konkatenasi yang diinginkan.

Perhitungan logika hash SHA-3 menggunakan state : c = 25W-r state bit yang tidak tersentuh oleh input atau output atau tanpa stack pada logika prosesnya. Hal ini dapat disesuaikan berdasarkan persyaratan keamanan, tetapi SHA-3 usulan menetapkan c = 2n konservatif, di mana n adalah ukuran dari hash output. Dengan demikian r, jumlah bit pesan yang diproses per blok permutasi, tergantung pada ukuran hash output. R rate 1152, 1088, 832, atau 576 (144, 136, 104 dan 72 byte) untuk 224,, 256 384 dan ukuran hash 512-bit, masing-masing, ketika w adalah 64.

Untuk memastikan pesan dapat merata dibagi menjadi r-bit blok, itu diisi dengan pola bit 10 * 1: 1 bit, nol atau lebih bit 0 (maksimum r-1), dan sedikit 1 akhir. Bit 1 akhir diperlukan karena bukti konstruksi spons keamanan mensyaratkan bahwa blok pesan akhir ini tidak semua-nol. Untuk menghitung hash, menginisialisasi negara untuk 0, pad input, dan memecahnya menjadi r-bit potongan. Menyerap masukan ke negara, yaitu, untuk masing-masing bagian, XOR ke bagian dan kemudian menerapkan blok permutasi.

Setelah blok akhir permutasi, n bit bagian terdepan adalah hash yang diinginkan. Karena r selalu lebih besar dari n, sebenarnya ada pernah ada kebutuhan untuk permutasi blok tambahan dalam fase squeezing (Supriyanto, 2007). Namun, panjang *output* dapat berbeda-beda mungkin berguna dalam aplikasi seperti bantalan enkripsi asimetris yang optimal. Dalam kasus ini, n adalah parameter keamanan daripada ukuran output.

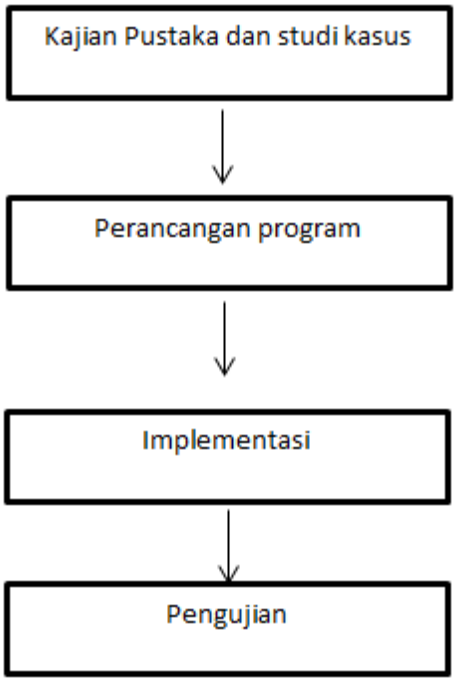
Meskipun bukan bagian dari persyaratan pemetaan memory SHA-3, varian yang lebih kecil dari blok permutasi dapat digunakan, untuk ukuran output hash sampai setengah ukuran masing-masing bagian, jika r terdapat pada tingkatan terbatas. Sebagai contoh, hash 256-bit dapat dihitung dengan menggunakan 25 32-bit kata-kata jika r = 800-2 × 256 = 288 (36 byte per iterasi).

Berikut adalah langkah-langkah contoh pembuatan message menggunakan hash SHA-3 digest secara garis besar adalah sebagai berikut.

1. Penambahan Bit-bit Pengganjal
2. Penambahan Nilai Panjang Pesan Semula
3. Inisialisai Penyangga MD
4. Mengolah Pesan dalam Blok dengan ukuran 512 bit

B. METODE

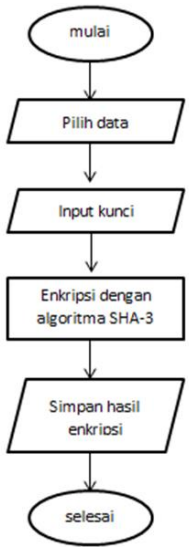
National Institute of Standars and Technology (NIST) bertujuan untuk memberikan algoritme alternatif yang bernama SHA-3, dikarenakan kekawatiran terhadap algoritme sebelumnya yang berhasil ditembus seperti MD5, SHA-0, SHA-1. Langkah – langkah yang dilakukan dalam menyelesaikan perancangan aplikasi enkripsi dan dekripsi pada data menggunakan algoritma Secure Hash Algorithm (SHA)-3 adalah sebagai berikut (Refialy, Sediyono, & Setiawan, 2015).



Gambar 2. Diagram Alir Metode Penelitian

Metode Enkripsi

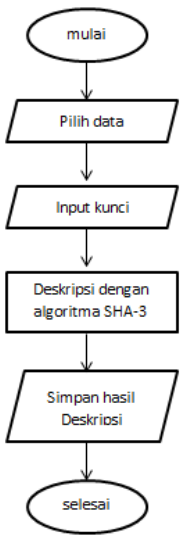
Langkah – langkah perancangan proses enkripsi adalah sebagai berikut.



Gambar 3. Flowchart Enkripsi

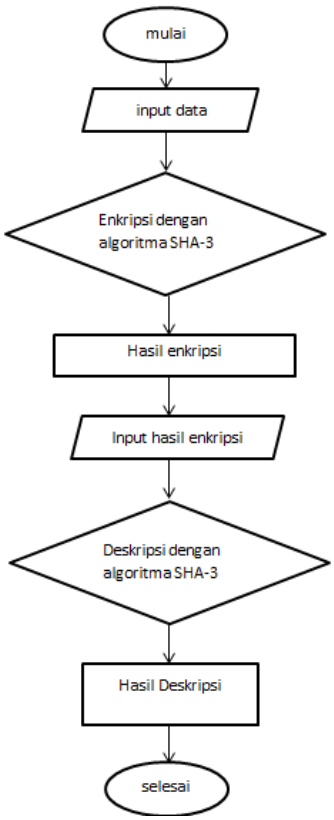
Metode Deskripsi

Langkah – langkah perancangan proses Deskripsi adalah sebagai berikut.



Gambar 4. Flowchart Dekripsi

Gambaran umum flowchart sistem



Gambar 5. Flowchart Sistem

C. HASIL DAN PEMBAHASAN

Pengujian yang dilakukan pada penelitian ini yaitu pengujian test vector, performance waktu, validasi enkripsi dan dekripsi, keamanan, fungsional, dan non fungsional.

1. Pengujian Test Vector

   Test vector algoritme SHA-3

   Pesan: “abcd”

SHA-3: f641824d3f8ef24a a09034de7d4c868f b5c3c5666d0d45ad 66c45rfr

2. Pengujian Performance Waktu

Pengujian performance waktu yang dibutuhkan oleh sistem dalam melakukan proses enkripsi dan dekripsi pada data berbentuk txt, doc, rtf. Pengujian performance waktu dilakukan sebanyak 15 kali untuk mendapatkan waktu tempuh,. Pengujian seluruh hasil waktu kemudian diambil rata-ratanya dalam waktu milisecond.

Tabel 1. Pengujian Performance Waktu

No	Nama	Tipe	Ukuran asli	Ukuran enkripsi *(bytes)*	Waktu *(second)*	Rerata Waktu
1	Testxt1	txt	34415	34415	25.012	104588,2
2	Testxt2	txt	18855	18855	16.177	
3	Testxt3	txt	170988	170988	76.409	
4	Testxt4	txt	306555	306555	189.678	
5	Testxt5	txt	408766	408766	215.665	
6	Tesdoc1	doc	16545	16545	17.766	94896,6
7	Tesdoc2	doc	20868	20868	28.220	
8	Tesdoc3	doc	30777	30777	39.765	
9	Tesdoc4	doc	308677	308677	187.966	
10	Tesdoc5	doc	407876	407876	200.766	
11	Tesrtf1	rtf	20655	20655	18.989	96172,8
12	Tesrtf2	rtf	30143	30143	30.898	
13	Tesrtf3	rtf	31878	31878	41.645	
14	Tesrtf4	rtf	308780	308780	187.656	
15	Tesrtf5	rtf	404333	404333	201.676	

3. Pengujian validasi enkripsi dan dekripsi

Pada Tabel 2 merupakan uji validasi untuk memastikan bahwa data sesudah di dekripsi memiliki hasil yang sama dengan data sebelum di enkripsi.

Tabel 2. Hasil Pengujian Validasi Enkripsi dan Dekripsi

Key	Data sebelum di Enkripsi	Data sesudah di Dekripsi
Test1	abc	abc
Test1	Hallo world	Hallo world
Test1	Ini adalah percobaan validasi enkripsi dan dekripsi	Ini adalah percobaan validasi enkripsi dan dekripsi
Test1	56njnk6565njk656i56h5i6o5o65i65oh6	56njnk6565njk656i56h5i6o5o65i65oh6

D. PENUTUP

Simpulan dan Saran

1) Program Enkripsi Dekripsi Berkas Dokumen menggunakan Algoritma SHA-3 dapat berjalan dengan baik untuk mengenkripsi dan mendekripsi berkas dokumen (.txt,.doc,.rtf).
2) Semakin besar ukuran berkas maka semakin lama waktu proses yang dibutuhkan untuk proses enkripsi maupun dekripsi.
3) Tidak ada perubahan ukuran berkas pada berkas asli baik setelah dikenai proses enkripsi maupun proses dekripsi.

DAFTAR PUSTAKA

Abdullah, D., & Erliana, C. I. (2012). Bisnis Rental Mobil Melalui Internet (E-Commerce) Menggunakan Algoritma Sha-1 (Sequre Hash Algorithm-1). *Speed-Sentra Penelitian Engineering dan Edukasi*, 4(2).

Agani, N., Hardjianto, M., & Virgian, D. (2016). Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator (PRNG) Linear Congruential Generator (LCG) di Perangkat Berbasis Android. *Budi Luhur Information Technology*, 13(1).

Kurniawan, F., Kusyanti, A., & Nurwarsito, H. (2017). Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem

Autentikasi Garuda Training Cost. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*. e-ISSN, 2548, 964X

Prasetyo, T. F., & Hikmawan, A. (2016). Analisis Perbandingan Dan Implementasi Sistem Keamanan Data Menggunakan Metode Enkripsi RC4 SHA Dan MD5. *INFOTECH journal*, 2(1).

Santoso, K. I. (2013). Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan Hash SHA. *Semantik*, 3(1).

Supriyanto, A. (2007). Otentikasi Dokumen XML menggunakan Algoritma RSA dan Hash SHA-1 (Doctoral dissertation, Universitas Gadjah Mada).

Refialy, L., Sediyono, E., & Setiawan, A. (2015). Pengamanan Sertifikat Tanah Digital menggunakan Digital Signature SHA-512 dan RSA. *Jurnal Teknik Informatika dan Sistem Informasi*, 1(3).