PENERAPAN ENKRIPSI DATA MENGGUNAKAN METODE KOLABORASI MESSAGE DIGEST ALGORITHM 5 (MD5) DAN SHA3 DENGAN *SALT FUNCTION* PADA SISTEM INFORMASI PENJUALAN DAN PEMBELIAN

SKRIPSI

diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Pendidikan Program Studi S-1 Pendidikan Teknik Informatika dan Komputer

Oleh

Khanif Nasrudin

NIM.5302414081

PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER JURUSAN TEKNIK ELEKTRO FAKULTAS TEKNIK UNIVERSITAS NEGERI SEMARANG

2018

PERSETUJUAN PEMBIMBING

Nama	: Khanif Nasrudin
NIM	: 5302414081
Program Studi	: S-1 Pendidikan Teknik Informatika dan Komputer
Judul Skripsi	: Penerapan enkripsi data menggunakan metode kolaborasi message digest algorithm 5 (MD5) dan SHA3 dengan *Salt Function* pada sistem informasi penjualan dan pembelian

Skripsi/TA ini telah disetujui oleh pembimbing untuk diajukan ke sidang panitia ujian skripsi Program Studi S-1 Pendidikan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Semarang.

Semarang, 10 Desember 2018
Pembimbing,

Dr.-Ing. Dhidik Prastiyanto, S.T., M.T.
NIP. 197805312005011002

PENGESAHAN

Skripsi dengan judul Penerapan Enkripsi Data menggunakan Metode Kolaborasi Message Digest Algorithm 5 (MD5) dan SHA3 dengan *Salt Function* pada Sistem Informasi Penjualan dan Pembelian telah dipertahankan di depan sidang Panitia Ujian Skripsi Fakultas Teknik UNNES pada tanggal 26 bulan Oktober tahun 2018.

Oleh

Nama : Khanif Nasrudin
NIM : 5302414081

Panitia Sidang Skripsi :

Ketua

Dr. –Ing. Dhidik Prastiyanto, S.T., M.T.
NIP. 197805312005011002

Sekretaris

Ir. Ulfah Mediaty Arief, M.T.
NIP. 196605051998022001

Penguji I

Dr. Ir. Subiyanto, S.T., M.T.
NIP. 197411232005011001

Penguji II

Budi Sunarko, S.T., M.T., Ph.D.
NIP. 197101042006041001

Penguji III

Dr. –Ing. Dhidik Prastiyanto, S.T., M.T.
NIP. 197805312005011002

Mengetahui,
Dekan Fakultas Teknik

Dr. Nur Qudus, M.T.
NIP. 196911301994031001

MOTO

- " Keberhasilan adalah kemampuan untuk melewati dan mengatasi dari satu kegagalan ke kegagalan berikutnya tanpa kehilangan semangat. (Winston Chochill) "

- " Lebih baik bertempur dan kalah dari pada tidak pernah bertempur sama sekali (Arthur Hugh Clough) "

ABSTRAK

Khanif Nasrudin. 2018. Penerapan Enkripsi Data Menggunakan Metode Kolaborasi Massage Digest Algorithm 5 (MD5) dan SHA3 dengan *salt function* Pada Sistem Informasi Penjualan dan Pembelian. Dr.-Ing. Dhidik Prastiyanto, S.T., M.T.
Pendidikan Teknik Informatika dan Komputer.

Tindakan pencurian data sering terjadi dengan memanfaatkan teknologi informasi khususnya pada informasi berupa teks yang merupakan bentuk penting dari informasi digital. Penerapan prosedur keamanan dapat membantu dalam memberikan keamanan pada data berupa teks salah satunya menggunakan teknik kriptografi dengan metode enkripsi.

Berbagai macam model enkripsi yang dapat digunakan untuk pengamanan data, seperti model MD5 dan SHA. Namun, model MD5 dan SHA memiliki kelemahan pada hasil enkripsi yang berpeluang diprediksi memanfaatkan metode Babbage-Kasiski. Sehingga metode enkripsi MD5 dan SHA kurang aman apabila digunakan untuk menyandikan informasi teks. Penelitian ini bertujuan untuk mengembangkan metode kolaborasi MD5 dan SHA3 dengan *salt function*, dengan melakukan modifikasi terhadap kunci enkripsi yang digunakan. Kunci enkripsi dibentuk melalui empat tahap pembentukan dengan memanfaatkan metode *salt function*. Hasil simulasi menunjukkan bahwa algoritma modifikasi kolaborasi MD5 dan SHA3 tidak dapat diprediksi dengan metode Babbage-Kasiski. Akan tetapi pada algoritma model MD5 dan SHA3 terlihat bahwa terdapat perulangan kata pada hasil enkripsi dengan rata-rata terbesar informasi dapat diprediksi sebesar 30 kata.

Kelebihan algoritma modifikasi kolaborasi MD5 dan SHA3 dengan salt function dalam penelitian ini adalah hasil enkripsi tidak memiliki pola rangkaian perulangan kata sehingga tidak dapat diprediksi menggunakan metode Babbage-Kasiski. Oleh karena itu, algoritma modifikasi MD5 dan SHA3 dengan salt function lebih aman dari pada algoritma MD5 dan SHA3 yang telah ada.

Kata Kunci: Enkripsi, MD5, SHA3, salt function, pembentukan kunci, data teks, Babbage-Kasiski.

PRAKATA

Segala puji dan syukur penulis ucapkan kehadirat Allah SWT yang telah melimpahkan rahmat-Nya sehingga penulis dapat menyelesaikan Skripsi yang berjudul Penerapan Enkripsi Data Menggunakan Metode Kolaborasi Message Digest Algorithm 5 (MD5) dan SHA3 dengan *Salt Function* pada Sistem Informasi Penjualan dan Pembelian. Skripsi ini disusun sebagai salah satu persyaratan meraih gelar Sarjana Pendidikan pada Program Studi S1 Pendidikan Teknik Informatika dan Komputer Universitas Negeri Semarang. Shalawat dan salam disampaikan kepada Nabi Muhammad SAW, semoga kita semua mendapatkan syafaatnya di yaumil akhir nanti, Amin.

Penyelesaian skripsi ini tidak lepas dari bantuan berbagai pihak, oleh karena itu pada kesempatan ini penulis menyampaikan ucapan terima kasih serta penghargaan kepada:

1. Bpk. Susdarto dan Ibu Suwarti, yang tidak henti-hentinya memberikan doa dan jerih payahnya untuk sang buah hati.
2. Prof. Dr. Fathur Rokhman, M.Hum, Rektor Universitas Negeri Semarang atas kesempatan yang diberikan kepada penulis untuk menempuh studi di Universitas Negeri Semarang.
3. Dr. Nur Qudus, M.T., Dekan Fakultas Teknik, Dr. –Ing Dhidik Prastiyanto, S.T., M.T., Ketua Jurusan Teknik Elektro serta Koordinator Program Studi Pendidikan Teknik Informatika dan Komputer, atas fasilitas yang disediakan bagi mahasiswa.
4. Dr. –Ing Dhidik Prastiyanto, S.T., M.T. Pembimbing yang dengan antusias dan sabar dalam memberikan motivasi arahan serta bimbingan yang luar biasa hebatnya.
5. Dr. Ir. Subiyanto, S.T., M.T. dan Budi Sunarko, S.T., M.T., Ph.D. selaku penguji yang telah memberikan penilaian kritik dan saran demi tercapainya hasil yang maksimal dalam karya tulis ini.
6. Semua dosen dan teman-teman Jurusan Teknik Elektro FT UNNES yang telah memberi bekal pengetahuan yang berharga.
7. Berbagai pihak yang telah memberi bantuan untuk karya tulis ini yang tidak dapat disebutkan satu persatu.

Penulis berharap semoga Skripsi ini dapat bermanfaat untuk lembaga pendidikan, pengembang serta masyarakat pada umumnya.

Semarang, 10 Desember 2018

Penulis

DAFTAR ISI

SAMPUL i

LEMBAR PERSETUJUAN PEMBIMBING ii

LEMBAR PENGESAHAN iii

LEMBAR PERNYATAAN KEASLIAN KARYA ILMIAH iv

MOTO v

ABSTRAK vi

PRAKATA vii

DAFTAR ISI viii

DAFTAR TABEL x

DAFTAR GAMBAR xi

DAFTAR GRAFIK xiii

DAFTAR LAMPIRAN xiv

BAB I. PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Batasan Masalah 6

1.3 Rumusan Masalah 7

1.4 Tujuan Penelitian 7

1.5 Manfaat Penelitian 7

1.5.1 Manfaat Teoritis 8

1.5.2 Manfaat Praktis Bagi Peneliti 8

BAB II. KAJIAN PUSTAKA DAN LANDASAN TEORI 9

2.1 Kajian Pustaka 9

2.2 Landasan Teori 12

2.2.1 Komponen Sistem Informasi 12

2.3 Kriptografi 14
2.3.1 Komponen Sistem Informasi 15
2.3.2 Tipe-Tipe Enkripsi 16
2.4 *Hash Function* 17
2.5 *Salt Function* 18
2.6 Message Digest Algorithm 5 (MD5) 19
2.7 SHA3 26
BAB III. METODE PENELITAN 31
3.1 Objek Penelitian 32
3.2 Penentuan Model Enkripsi 33
3.3 Perancangan Simulasi 34
3.4 Uji Simulasi 45
3.5 Metode Analisa 47
BAB IV. HASIL PENELITIAN DAN PEMBAHASAN 48
4.1 Hasil Uji Sistem 48
4.2 Simulasi Enkripsi Kombinasi MD5 dan SHA3 52
4.3 Hasil Uji Penyandian 54
4.4 Prediksi Informasi Pesan dengan Metode Babbage-Kasiski 57
BAB V. SIMPULAN DAN SARAN 62
5.1 Simpulan 62
5.2 Saran 62
DAFTAR PUSTAKA 64
LAMPIRAN 70

DAFTAR TABEL

Tabel 4.1 Hasil Enkripsi..... 48

Tabel 4.2 Database Hasil Enkripsi MD5 dan SHA3 dengan *salt function* ... 55

Tabel 4.3 Perbandingan Nilai Perulangan Prediksi Informasi Pesan Antara MD5 dan SHA dengan Modifikasi MD5 dan SHA3 dengan *salt function*..... 59

DAFTAR GAMBAR

Gambar 2.1 Siklus Pengolahan Data 12

Gambar 2.2 Komponen Dari Sistem Informasi 13

Gambar 2.3 Analogi dalam Fungsi *Hash* 17

Gambar 2.4 Algoritma MD5 (Kumar, 2018) 20

Gambar 2.5 *Flowchart* Algoritma MD5 (Bhandari, 2017) 21

Gambar 2.6 Simpul Utama MD5 (Sofyan, dkk. 2006) 23

Gambar 2.7 Satu Buah Operasi MD5 24

Gambar 2.8 *Flowchart* Algoritma SHA3 (Luo,2017)..... 27

Gambar 2.9 Analogi dalam komputasi pada SHA3 (Huda, 2009)..... 28

Gambar 3.1 Diagram Alir Penelitian Kolaborasi MD5 dan SHA3..... 32

Gambar 3.2 Alur Arsitektur Sistem 34

Gambar 3.3 *Flowchart* kolaborasi Enkripsi MD5 dan SHA3 dengan *salt function* 36

Gambar 3.4 Deklarasi Isi Variabel dan *function* yang digunakan 40

Gambar 3.5 Deklarasi Variabel 40

Gambar 3.6 Pemanggilan *hash function* dan *salt function*..... 41

Gambar 3.7 *Sourcode* Pembuatan Logika dari algoritma *hash function* dan *salt function* 42

Gambar 3.8 Deklarasi dan Implementasi Metode Enkripsi yang Digunakan 43

Gambar 3.9 Deklarasi Alamat dari Database yang akan Dituju pada Halaman Setelah Login Berhasil 44

Gambar 4.1 Login Database phpMyadmin 52

Gambar 4.2 Hasil Enkripsi MD5 dan SHA3 dengan *salt function* 53

Gambar 4.3 Hasil Enkripsi MD5 dan SHA3 Tanpa *salt function*..... 53

Gambar 4.4 Hasil Uji Dengan Software CrackStation..... 55

Gambar 4.5 Spesifikasi Rainbow Table..... 56

Gambar 4.6 Hasil Uji Dengan Rainbow Table 57

DAFTAR GRAFIK

Gambar 2.1 Grafik Kontrol Nilai Peluang Prediksi Informasi Pesan Kolaborasi MD5 dan SHA3 dengan *salt function* 59

DAFTAR LAMPIRAN

Lampiran 1 *Sourcode* Program Algoritma Enkripsi Kolaborasi..... 70

Lampiran 2 *Sourcode* Algoritma Enkripsi MD5 (Manual)..... 71

Lampiran 3 *Sourcode Plugin* SHA3 74

Lampiran 3 Tampilan Antarmuka Simulasi Sistem Login 75

Lampiran 4 Tampilan Antarmuka Simulasi Sistem Informasi 76

Lampiran 5 Hasil Pengujian *Ciphertext* dengan Software CrackStation..... 77

Lampiran 6 Hasil Pengujian *Ciphertext* dengan Software Rainbow Table . 78

Lampiran 7 Kode ASCII 79

Lampiran 8 Usulan Pembimbing 80

Lampiran 9 Permohonan Izin Observasi..... 81

Lampiran 10 Izin Penelitian..... 82

Lampiran 11 Surat Penetapan Dosen Pembimbing Skripsi 83

Lampiran 12 Surat Tugas Ujian SKRIPSI 84

Lampiran 13 Surat Tugas..... 85

Lampiran 14 Berita Acara Ujian SKRIPSI 86

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi khususnya pada era globalisasi komputer seperti saat ini banyak dari sistem penjualan dan pembelian yang memanfaatkan sistem informasi untuk menunjang dan membantu suatu pertokoan dalam proses penjualan barang dan proses pembelian. Di setiap perusahaan memiliki sistem yang berbeda-beda, oleh sebabnya sistem berpengaruh pada kinerja suatu perusahaan. Mulyadi (2008) menjelaskan mengenai sistem, menurutnya sistem adalah sekelompok unsur yang erat berhubungan satu dengan lainnya, yang berfungsi bersama-sama untuk mencapai tujuan tertentu. Dengan adanya kebutuhan informasi yang semakin lama semakin meningkat maka diperlukannya suatu sistem yang baik dan cepat. Suatu sistem dikatakan baik apabila akan memudahkan semua prosesnya, salah satunya dengan jalan komputerisasi. " informasi adalah data yang diolah sehingga dapat dijadikan dasar untuk mengambil keputusan yang tepat. Pendapat dari Bodnar (2006) " (Dikutip oleh Cahyono, The Creating Application of The Cash Sales Sistem by Komputerize Basis in Toko cat Anugrah Abadi).

Nurrohmah (2018) menjelaskan dalam jurnal penelitiannya yang berjudul *instrumendesign diagnostic test three-tier multiple choice redox material with redox diagnostic software (RDT)* bahwa pemanfaatan teknologi dalam lingkup komputerisasi seperti sistem informasi untuk proses pembelajaran akan membantu

mempercepat proses pembelajaran terhadap siswa dibandingkan dengan cara manual.

Didalam suatu sistem informasi penjualan dan pembelian dalam suatu pertokoan dapat menyimpan data barang yang tersedia, dapat mengedit data tersimpan, dan dapat mengamankan data tersebut. Sistem informasi telah banyak digunakan oleh berbagai organisasi atau perusahaan untuk menyimpan dan mengolah data pada organisasi atau perusahaan tersebut. Data atau informasi menjadi target serangan oleh pihak-pihak yang tidak bertanggung jawab sehingga perlu untuk menjaga keamanan dan kerahasiaan data atau informasi. Teknik pengamanan data terdiri dari dua cara yaitu pengamanan data melalui pengaturan hak akses setiap pengguna oleh database administrator dan pengamanan data dari sisi kandungan yang tersimpan dalam database. (Sibyan: 2016).

Salah satu bentuk keamanan data dalam sistem informasi yaitu dengan menggunakan ilmu kriptografi data. Ilmu kriptografi merupakan ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan. Sementara kriptografi itu sendiri mempunyai dua bagian yang penting, yaitu Enkripsi dan Deskripsi. (Sofwan, Agung, dan Susanto: 2006:22).

Kriptografi (*cryptography)* berasal dari bahasa Yunani : "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan

cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. (Munir : 2006).

Hidayatullah menjelaskan dalam penelitiannya bahwa kriptografi merupakan sebuah kata yang mengarah pada ilmu dan seni dalam mengubah pesan menjadi lebih aman dan kebal terhadap penyerangan. (Forouzen, 2007) menjelaskan didalam ilmu kriptografi kita akan mengenal *Enkripsi* dan *Deskripsi* yang merupakan sebuah algoritma yang digunakan untuk mengubah pesan menjadi sandi dan sandi menjadi pesan(dikutip oleh Hidayatullah).

Munir (2006) juga menjelaskan mengenai kriptografi, menurutnya kriptografi merupakan ilmu dan seni yang mempelajari teknik-teknik metematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta autentifikasi. Bagian terpenting dari kriptografi salah satunya yaitu enkripsi, enkripsi atau penyandian sangat diperlukan untuk mengamankan data, enkripsi adalah mengubah data asli (*plain text*) menjadi data rahasia (*chipper text*). (Kashogi: Algoritma message digest 5 (MD5)).

Didalam kriptografi ada salah satu teknik enkripsi data. Ada salah satu bagian enkripsi yaitu fungsi *hash* satu arah. Fungsi *hash* satu arah adalah dimana kita dengan mudah melakukan enkripsi untuk mendapatkan *chipper*-nya tetapi sangat sulit mendapatkan *plaintext*-nya. Contoh dari bentuk enkripsi *hash* satu arah adalah Message Digest Algorithm 5 atau yang sering dikenal dengan MD 5.

Tujuan dari setiap algoritma enkripsi adalah untuk membuat kriptanalis sesulit mungkin dalam mendeskripsikan text yang telah di enkripsi (*ciphertext*)

dari *plaintext*. Jika algoritma enkripsi benar-benar baik digunakan maka serangan dengan berbagai teknik membutuhkan waktu untuk dapat mengetahui pesan asli dari *ciphertext.* (Docs Microsoft).

Message Digest Algorthim yang sering disebut dengan MD 5 secara garis besar adalah mengambil pesan yang mempunyai panjang variabel diubah menjadi "sidik jari" atau "intisari pesan". "sidik jari" ini tidak dapat dibalik untuk mendapatkan pesan, dengan kata lain tidak ada orang yang dapat melihat pesan dari "sidik jari" MD 5 (Sofyan, 2006: 22).

Inayatullah (2007) mengemukakan dalam jurnal penelitiannya dengan judul Analisis Penerapan Algoritma MD5 Untuk Pengamanan *Password* untuk menguji permasalahan dengan kasus pengguanaan metode enkripsi MD5, didalam penelitannya menjelaskan mengenai kompleksitas serangan prinsip MD5. Menurutnya kompleksitas serangan dapat diukur dengan beberapa cara, antara lain kompleksitas data, kompleksitas waktu, dan kompleksitas memori.

Pada prinsip keamanan data menggunakan enkripsi model MD5 ternyata masih memiliki kelemahan pada *ciphertext* yang dihasilkan oleh sistem. Untuk menutupi kelemahan yang ada pada enkripsi MD5 ini peneliti menggabungkan metode enkripsi berbeda yaitu enkripsi SHA3. Menurut Kurniawan (2017) menyatakan bahwa SHA3 merupakan jenis enkripsi model *hash-ing* yang di keluarkan pada tahun 2015 untuk pengembangan keamanan data jenis *password*.

Saputra (2016) menyatakan bahwa algoritma SHA menerima masukan berupa *string* dengan ukuran 2(64) bit. Untuk setiap *string* akan menghasilkan

keluaran 160 bit dari *string* tersebut dan *string* disebut *message digest*. SHA dikatakan aman karena proses SHA dihitung secara *inflesible* untuk mencari *string* yang sesuai untuk menghasilkan *message digest* atau dapat mencari dua *string* yang berbeda yang akan menghasilkan *message digest* yang sama.

Metode enkripsi yang dijelaskan diatas memiliki kekurangan maupun kelebihan tersendiri, terutama dari enkripsi MD5. Pada model enkripsi MD5 (*message digest algorithm 5*) yang sering digunakan untuk mengkodekan teks dengan cara menggunakan sidik jari dari kedua tangan diamana pada model enkripsi ini akan mudah untuk mendapatkan *ciphertext*-nya namun sulit untuk mendapatkan *plaintext* dari hasil *ciphertext* tersebut. Menurut Dhany (2014) model enkripsi MD5 rentan terhadap teks yang menghasilkan nilai yang sama (perulangan karakter teks). Input kata menggunakan MD5 atau dengan memasukkan kalimat yang panjang sekalipun, akan menghasilkan *hash* dengan panjang 32bit.

Dengan panjang *hash* yang selalu sama pada jumlah bit yang dihasilkan (dalam hasil *ciphertext*-nya) akan sangat memungkinkan berbagai serangan dari kriptanalis untuk mengetahui pesan asli yang telah dikodekan menggunakan metode enkripsi model MD5 ini. Dapat disimpulkan jika MD5 lebih rentan dengan keadaan dimana suatu masukan yang memiliki nilai hasil *hash* yang sama atau serupa dengan nilai masukan yang lain. Keadaan ini disebut dengan *collision* (tabrakan).

Model enkripsi MD5 yang digunakan dalam penelitian ini merupakan enkripsi model MD5 dengan blok bit sebesar 512 bit, dimana dalam prosesnya dari 512bit akan dibagi kedalam sub blok dengan jumlah 32bit sebanyak 16 buah. Hasil enkripsi dari MD5 berupa 4 buah blok yang masing-masing 32 bit, MD5 merupakan fungsi *hash* satu arah yang paling banyak digunakan dan biasanya menggunakan pengembangan satu putaran.

Maka dalam penelitian ini menggabungkan enkripsi model MD5 dengan model SHA 3, pada model enkripsi SHA3 akan menghasilkan hasil *hash* yang memiliki karakter hexadecimal. Jika dari kedua enkripsi tersebut digunakan bersama untuk membuat suatu kondisi data yang berbentuk *ciphertext* (sandi) maka akan menghasilkan data yang memungkinkan sulit untuk dipecahkan oleh pihak yang tidak memiliki wewenang. Oleh sebab itu penelitian ini mengangkat judul " Penerapan Enkripsi Data Menggunakan Metode Kolaborasi Message Digest Algorithm 5 (MD5) dan SHA3 dengan *salt function* Pada Sistem Informasi Penjualan dan Pembelian".

1.2. Batasan Masalah

Untuk membentuk metode kolaborasi MD5 dan SHA3 dengan *salt function* yang lebih aman, maka perlu adanya batasan masalah yang digunakan dalam melakukan penelitian antara lain :

1.2.1 Simulasi dibangun menggunakan fungsi *plugin* dari *hash* dan *salt function*.

1.2.2 Modifikasi kolaborasi MD5 dan SHA3 dengan *salt function* dilakukan untuk membentuk kunci baru yang digunakan pada enkripsi teks.

1.2.3 Pengujian modifikasi enkripsi dilakukan pada hasil enkripsi teks *password* atau hasil *ciphertext*-nya dengan *software* RainbowTable, CrackStation, dan Babbage-Kasiski Method.

1.3. Rumusan Masalah

Berdasarkan latar belakang diatas, maka permasalahan yang akan di kaji dalam penelitian ini adalah:

1.3.1. Bagaimana cara memberikan keamanan data atau informasi yang dapat digunakan pada sistem informasi penjualan dan pembelian?.

1.3.2. Bagaimana cara mengkolaborasi model enkripsi MD5 dan SHA3 dengan *salt function* agar menghasilkan model enkripsi yang sulit untuk dipecahkan oleh kriptanalis (penyerang)?.

1.4. Tujuan Penelitian

1.4.1 Memberikan kualitas keamanan data yang terjamin tingkat keamanannya pada sistem informasi penjualan dan pembelian yang ada pada penelitian ini.

1.4.2 Menghasilkan bentuk kolaborasi enkripsi MD5 dan SHA3 dengan *salt function* untuk menghasilkan model enkripsi yang sulit untuk dipecahkan oleh kriptanalis (penyerang).

1.5. Manfaat Penelitian

Hasil dari penelitian ini diharapkan berguna dan bermanfaat antara lain sebagai berikut :

1.5.1. Manfaat Teoritis

Penelitian ini diharapkan dapat menjadi bahan informasi atau bahan kajian dalam menambahkan pengetahuan dalam bidang teknologi dan informasi, khususnya mengenai perancangan model keamanan pada sistem informasi penjualan dan pembelian pada penelitian ini.

1.5.2. Manfaat Praktis Bagi Peneliti

Penelitian ini merupakan sarana untuk menerapkan ilmu pengetahuan tentang teknologi informasi yang diperoleh selama perkuliahan dengan menyesuaikan kondisi yang terjadi di lapangan.

BAB II

KAJIAN PUSTAKA DAN LANDASAN TEORI

2.1 Kajian Pustaka

Heriyanto, *Pengenalan Kriptografi* (2009) Mengemukakan dalam ebooknya bahwa kriptografi atau *cryptosystem* secara umum dapat digolongkan menjadi dua, yaitu *Symmetric Cryptosystem* dan *Assymmetric Cryptosystem*. Dimana suatu *cryptosystem* terdiri dari sebuah algoritma, seluruh kemungkinan *plaintext*, *ciphertext* dan kunci-kunci.

Munir, *Serangan (Attack) Terhadap Kriptografi* (Ebook, 2004) menjelaskan dalam penelitiannya bahwa serangan (*attack*) adalah setiap usaha (*attempt*) atau percobaan yang dilakukan oleh kriptanalis untuk menemukan *plaintext* dari *ciphertext*-nya.

Sibyan, *Implementasi Enkripsi Basis Data Dengan Algoritma MD5 (Message Digest Algorithm 5) dan SHA* (*Jurnal PPKM*, 2007) melakukan penelitian mengenai enkripsi data MD5, dari hasil penelitiannya Enkripsi database pada sebuah sistem atau program dapat membantu keamanan terhadap data dalam database dan kombinasi algoritma MD5 dengan vigenere cipher cocok diterapkan pada penerapan enkripsi basis data dikarenakan cukup kuat untuk menjaga keamanan basis data.

Sofwan, dkk. *Aplikasi kriptografi Dengan Algoritma Message Digest 5 (MD5)* (2006) menyatakan dalam hasil penelitianya bahwa *Message Digest 5* (MD5) adalah sebuah fungsi *hash* satu arah yang mengubah masukan dengan panjang variabel menjadi keluaran dengan panjang tetap yaitu 128 bit. Kecepatan rata-rata dari program MD5 yang telah dihasilkan mencapai 7,1633 Mbytes/detik dan sumber daya komputer berpengaruh terhadap kecepatan enkripsi.

Jain (2017) *Performance Evaluation of Authenticate (MD5, SHA) Routing Traffic over EIGRP and OSPF with IPV6* menyatakan bahwa authentication dalam MD5 sangat berguna bagi kemanan data yang ada dalam suatu *database.* Data yang tersimpan dalam kode MD5 tidak akan mudah untuk dipahami maknanya oleh pihak ketiga atuapun pihak yang memang tidak punya wewenang untuk mengetahuinya.

Bahri, *Jurnal Ilmiah* (2012) menyatakan dalam jurnalnya yang berjudul Studi dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5 (message-Digest Algorihm 5) bahwa metode MD5 secara komputerisasi melalui suatu program khusus yang dirancang menggunakan database mysql. Proses pengolahan keamanan data dapat dilakukan dengan cepat karena menggunakan metode enkripsi MD5.

Inayatullah (2007) menyatakan dalam jurnal penelitiannya bahwa algoritma MD5 dapat digunakan atau diterapkan untuk pengamanan *password* dari pengguna dalam suatu *database*. Semakin besar ukuran kunci, semakin lama waktu yang dibutuhkan untuk melakukan pencarian terhadap kunci.

Dalam model enkripsi *message digest algorithm 5* (MD5) memiliki kekurangan atau kelemahan yang ditemukan oleh Sibyan (2017) dalam jurnal penelitiannya yang berjudul implementasi enkripsi basis data dengan algoritma MD5 (message digest algorithm 5) dan vigenere cipher, didalam penelitiannya Sibyan menemukan cara memecahkan sandi (*ciphertext*) dari hasil enkripsi MD5 menjadi *plaintext*. Dengan adanya kelemahan dalam model MD5 maka peneliti dalam penelitian ini mencoba mengatasi kelemahan tersebut dengan menggabungkan model enkripsi lain yang menurut peneliti cocok digunakan dan diterapkan bersamaan dengan model MD5.

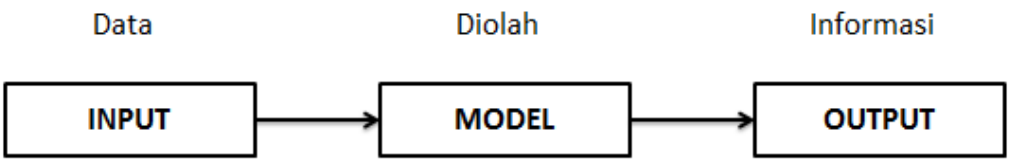
Renaldy menyatakan dalam jurnal penelitiannya bahwa enkripsi model SHA dapat dikolaborasikan dengan model enkripsi MD5, menurutnya model SHA lebih baik daripada MD5. SHA merupakan fungsi *hash* (satu arah sepertihalnya MD5) yang menerima masukan berupa pesan dengan ukuran maksimal 264 bit dan menghasilkan digest yang panjangnya 160 bit yang lebih panjang dari MD5.

Model enkripsi yang di ambil oleh peneliti dalam penelitian ini adalah model SHA, dimana dari perkembangan terbarunya SHA mengeluarkan model SHA 3 yang memiliki kriteria baik dan aman dengan jumlah bit yang dihasilkan dari hasil *ciphertext* (Kurniawan, 2017), dengan ini maka peneliti mengangkat judul Penerapan Enkripsi Data Menggunakan Metode Kolaborasi Message Digest Algorithm 5 (MD5) dan SHA3 dengan *salt function* Pada Sistem Informasi Penjualan dan Pembelian.

2.2. Landasan Teori

2.2.1. Komponen Sistem Informasi

Sistem informasi merupakan suatu komponen yang saling berhubungan yang mengumpulkan (atau mendapatkan kembali), memproses, menyimpan, dan mendistribusikan informasi untuk mendukung pengambilan keputusan dan kendali dalam suatu organisasi (Agustina, 2013). Informasi tersebut diperoleh dari hasil pengolahan data atau fakta yang dikumulkan dengan cara tertentu melalui suatu siklus. Siklus ini disebut dengan siklus pengolahan data (*data processing life cycle*) atau siklus informasi (*information life cycle*).



Gambar 2. 1 Siklus Pengolahan Data

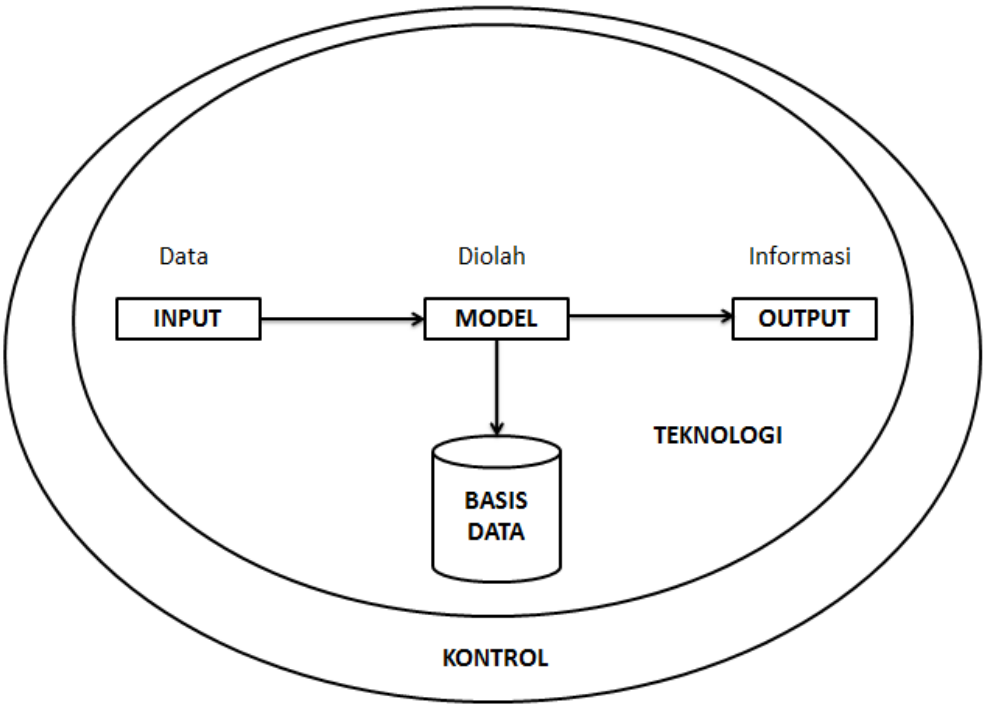
Dari Gambar 2.1 terlihat bahwa untuk melakukan pengolahan data diperlukan tiga buah komponen, yaitu komponen input, komponen model, dan komponen output. Pada umumnya, data yang diperoleh disimpan terlebih dahulu yang nantinya setiap saat dapat diambil untuk diolah menjadi informasi.

Data ini disimpan di simpanan (*storage*) dalam bentuk *database*. Tujuan dari sistem informasi yaitu menghasilkan informasi yang berguna dapat dicapai. Informasi yang relevan (*relevance*) dapat dicapai dengan komponen model.

Informasi yang tepat waktu (*timeliness*) dapat dicapai dengan komponen teknologi. Komponen teknologi sistem komputer mempercepat proses pengolahan data dan komponen telekomunikasi mempercepat proses transmisi data sehingga membuat informasi dapat disajikan tepat pada waktunya.

Informasi yang akurat dapat dicapai dengan komponen kontrol. Komponen kontrol atau pengendalian akan menjaga sistem informasi dari kesalahan-kesalahan yang disengaja atau tidak disengaja.

Dengan demikian, sistem informasi mempunyai enam buah komponen, yaitu (1) komponen input atau komponen masukan, (2) komponen model, (3) komponen output atau komponen keluaran, (4) komponen teknologi, (5) komponen basis data, dan (6) komponen kontrol atau komponen pengendalian.



Gambar 2. 2 Komponen Dari Sistem Informasi

Gambar 2.2 menjelaskan bahwa terdapat tiga aktifitas dalam sistem infromasi yaitu input, pengolahan, dan output. Aktivitas tersebut menghasilkan informasi yang diperlukan oleh organisasi untuk membuat keputusan, mengendalikan operasi, meneliti permasalahan, dan menciptakan produk baru atau jasa. Input menangkap atau mengumpulkan data mentah dari dalam organisasi atau dari lingkungan eksternalnya.

Pemrosesan mentransfer baris-baris masukan kedalam suatu format yang lebih mengandung arti. Output mengalihkan informasi yang diperoleh kepada orang-orang yang akan menggunakannya atau kepada aktivitas yang membutuhkannya dan digunakan sebagai alat bantu dalam mengambil keputusan.

2.3 Kripptografi

Menurut Munir (2006) kriptografi adalah ilmu dan seni yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta autentifikasi (Dikutip oleh Sibyan, implementasi enkripsi basis data dengan algoritma MD5 (message digest algorithm 5) dan vigenere cipher : 2017).

Kriptografi adalah ilmu sekaligus seni unntuk menjaga kerahasiaan pesan (data maupun informasi) dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna.

Kashogi menjelaskan bahwa kriptografi mempunyai tiga komponen, yaitu *plain text* (sumber berita atau pesan atau teks asli), *cipher text* (teks yang sudah

diproses (diacak, diganti), dan Algoritma atau kunci. Didalam kriptografi ada dua bagian yang sangat penting yang dinamakan dengan enkripsi dan deskripsi.

2.3.1 Definisi Enkripsi

Enkripsi merupakan salah satu proses yang terjadi dalam kriptografi, kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut ada juga pengertian ilmu yang mengajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data (Menezes, Oorschot and Vanstone Handbook of Applied Cryptography). Sedangkan menurut Kaufman (2002) menjelaskan bahwa kata kriptografi berasal dari bahasa yunani dan memiliki makna seni dalam menulis pesan rahasia (*The art of secret writing*), dimana kriptografi terdiri dari dua kata yaitu *cryptos* yang berarti tulisan. (Apriandala, 2013: 114).

Menurut Munir (2006) kriptografi adalah ilmu dan seni yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta autentifikasi.

Menurut Sibyan dalam jurnalnya yang berjudul Implementasi Enkripsi Basis Data dengan Algoritma MD 5 (Message Digest Algorithm 5) dan Vigenere Cipther (2016) mengatakan bahwa enkripsi merupakan proses mengubah suatu pesan asli (*plain text*) menjadi suatu pesan dalam bahasa sandi (*cipher text).* Enkripsi merupakan bagian dari kriptografi, dan merupakan hal yang sangat penting supaya keamanan data yang dikirimkan bisa terjaga kerahasiaannya. Enkripsi dapat diartikan sebagai *chipper* atau kode, dimana plain text diubah

menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun pihak penerima pesan.

Pengamanan data menggunakan metode enkripsi harus selalu dipantau dan dikelola oleh pengguna. Dengan adanya pengembangan aplikasi harus memperhatikan pula untuk memastikan bahwa model keamanan pada aplikasi dengan model-model yang ada terjaga dengan aman (Oracle Database).

2.3.2 Tipe-tipe Enkripsi

Menurut Sudrajat (Implementasi Enkripsi Database Menggunakan Transparent Data Encryption pada Database Engine Oracle: 2006) enkripsi data dibedakan menjadi tiga tipe sebagai berikut :

2.3.2.1. Enkripsi Manual

Enkripsi manual merupakan enkripsi yang dilakukan sepenuhnya oleh user (melalui *software* tertentu), dimana user harus secara manual memilih objek yang akan dienkripsi dan kemudian menjalankan *command* khusus untuk melakukan enkripsi atau deskripsi sebuah objek.

2.3.2.2. Enkripsi *Semi- Transparent*

Merupakan enkripsi *On the fly,*dimana operasi read atau write tidak secara permanen, sehingga dilakukan sebelum dan sesudah akses dilakukan.

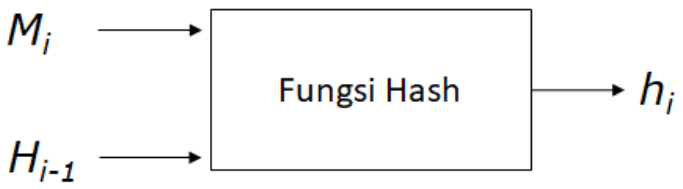
2.3.2.3. Enkripsi *Transparent*

Enkripsi *Transparent* merupakan kebalikan dari enkripsi manual, dimana enkripsi dan deskripsi dilakukan pada *level* yang rendah (*low*

level), secara permanen, saat melakukan operasi *read* atau *write* sehingga data yang dienkripsi selalu disimpan dalam bentuk enkripsi.

2.4 *Hash Function*

Bellare (2016) menyatakan bahwa fungsi *hash* merupakan fungsi yang menerima *string* dengan panjang sembarang dan mengkonfersinya menjadi *string* keluaran yang panjangnya tetap (*fixed*). Fungsi *hash* akan mengkonfersi sembarang pesan yang berukuran berapa saja menjadi *message digest* yang selalu tetap.



Gambar 2.3 Analogi dalam Fungsi *Hash*

Dilihat dari fungsinya, *hash* yang merupakan fungsi yang menerima masukan berupa *string* yang panjang mulanya sembarang dan mengkonversinya menjadi *string* keluaran yang panjangnya tetap (*fixed*). (Munir, 2004) Fungsi *hash* dapat menerima masukan *string* apa saja, jika *string* menyatakan pesan (*message*), maka sembarang pesan *M* berukuran bebas dikompresi oleh fungsi *H* melalui persamaan algoritma berikut:

$$h = H (M)$$

keluaran fungsi *hash* disebut juga nilai hash (*hash-value*) atau pesan ringkas (*message digest*). Pada persamaan h = H(M), h adalah nilai *hash* atau *message digest* dari *H* untuk masukan *M*. dengan kata lain, fungsi *hash* mengkompresi sembarang pesan yang ukurannya selalu tetap.

2.5 *Salt Function*

Salt merupakan suatu perintah pengacakan yang ditambahkan ke input dalam proses derivasi kunci. *Salt* berfungsi untuk memperkuat keamanan data yang telah diamankan yang biasanya dengan cara enkripsi, terutama dari *dictionary-attack*. (Chessin, 2013).

Slat function akan mengambil pesan asli yang digunakan untuk di acak, proses pengacakan hanya akan memindahkan karakter dari posisi awal menjadi posisi yang baru, dari posisi karakter pada teks asli, sehingga pesan yang kemungkinan memiliki pola tidak akan terdeteksi setelah di acak menggunakan fungsi *salt* ini. Dalam fungsi *salt* proses pengacakkan tidak akan meletakkan satu karakter pada tempat yang sama, hal ini dikarenakan fungsi *salt* dapat membaca setiap karakter yang digunakan dalam prosesnya, *salt function* dapat membaca jumlah bit dari masing-masing pesan yang di gunakan, sehingga dalam *salt function* tidak akan meletakkan satu karakter di tempat semula karakter tersebut berada. Hal ini sesuai dengan yang dikemukakan oleh Pietgen untuk mengkonversi nilai *random* secara kasar ke dalam distribusi Gaussian menggunakan algoritma dibawah ini (dikutip oleh Krisanty, 2010):

$$D = x = \frac{1}{A}\sqrt{\frac{12}{n}}\left(\sum_{i=1}^{n} Yi\right) - \sqrt{3n}$$

Keterangan:

D : bilangan random Gaussian

A : batas atas dari random number generator, yang mengembalikan 0,1,…..*A*

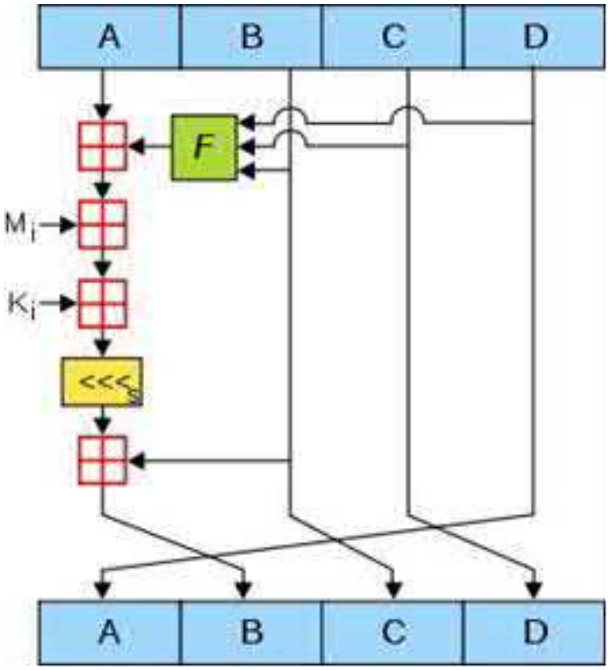
n : jumlah *event* yang independen, misal dadu

2.6 Message Digest Algorthim 5 (MD 5)

Algoritma MD5 disusun oleh Profesor Ronald L. Rivest, dari MIT. Pada RFC 1321, Prof. Ron Rivest memberikan penjelasan awal mengenai MD5, yaitu suatu algoritma yang inputnya berupa sebuah pesan yang penjangnya tidak tertentu, dan menghasilkan keluaran sebuah message digest dari pesan inputnya dengan panjang tepat 32 bit. Diperkirakan (*conjectured*) tidak mungkin untuk menghasilkan dua pesan dengan message digest yang sama. Message Digest Algorithim kepanjangan dari MD5 adalah fungsi *hash* (procedur terdefinisi atau fungsi matematika yang mengubah variabel dari suatu data yang berukuran besar menjadi lebih sederhana) teknik kriptografi yang digunakan secara luas dengan *hash* value 512-bit, (Bahri, Diana, dan Dian PS: Studi dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5(message-Digest Algorihm 5)).

2.6.1 Metode Algoritma Message Digest Algorithm 5 (MD5)

Rivest (1991) mendesain bentuk keamanan pada basis komputerisasi yang dikenal dengan metode enkripsi, Rivest membuat model enkripsi yang disebut *Message Digest (MD)* dimana dari penemuannya dengan dari awal yaitu MD1 berkembang sampai saat ini yaitu MD5. Rivest menjelaskan mengenai langkah yang digunakan untuk membentuk enkripsi model MD5 ini dalam sebuah logika algoritma MD5, terlihat pada Gambar 2.4.



Gambar 2. 4 Algoritma MD5 (Kumar, 2018)

Keterangan:

F : adalah fungsi nonlinier, satu fungsi digunakan pada tiap-tiap putaran.

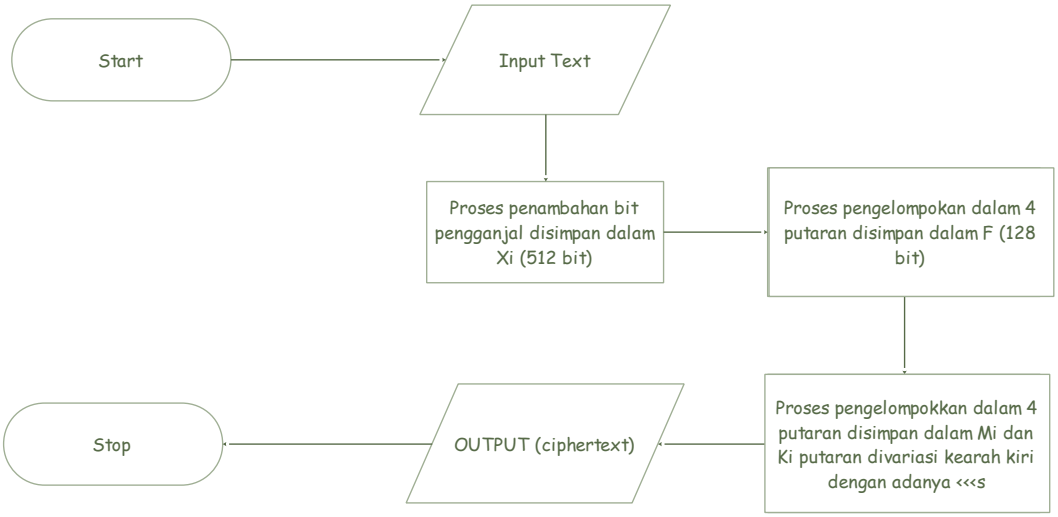
Mi : menunjukkan blok 32-bit dari masukan pesan.

Ki : menunjukkan konstanta 32-bit, berbeda untuk tiap-tiap operasi.

<<<s : menunjukkan perputaran bit kiri oleh s; s bervariasi untuk tiap-tiap operasi.

: menunjukkan tambahan modulo 2(32).

2.6.2 *Flowchart MD5*



Gambar 2. 5 *Flowchart* Algoritma MD5

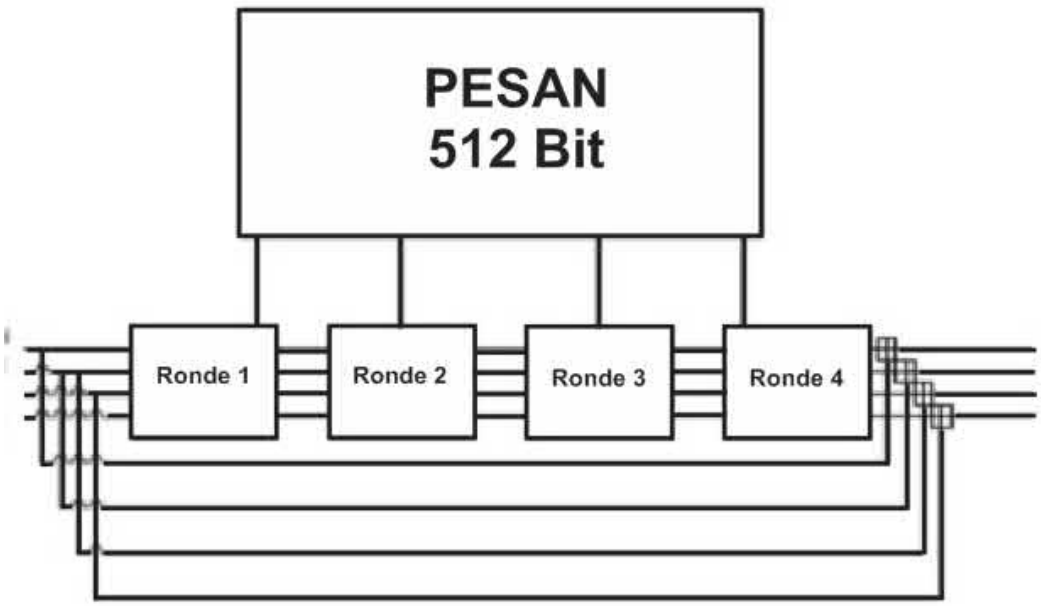
Proses yang terjadi dalam model enkripsi MD5 ditunjukkan pada *flowchart* algoritma MD5 pada Gambar 2. 5 (Bhandari, 2017) menyatakan bahwa pesan asli yang diinputkan berupa teks dalam berbagai karakter yang ada pada keyboard. Hal pertama yang dilakukan setelah pengin putan teks asli yaitu penambahan bit pengganjal, pada model enkripsi *message digest* bit yang dihasilkan paling tinggi higga saat ini sebesar 512 bit. dari pesan asli yang digunakan akan di tambahkan dengan beberapa karakter baru sehingga data

karakter dari pesan asli akan tercampur dengan karakter-karakter dari bit pengganjal sampai mencapai titik maksimal 512 bit. dari karate dengan jumlah 512 bit akan di lanjut proseskan kedalam pengelompokkan pertama yaitu dalam 4 putaran yang akan disimpan dalam “F” (fungsi nonlinier) dengan jumlah bit yang lebih sedikit, yaitu 128 bit.

Hal yang akan dilakukan dalam proses selanjutnya adalah membagi untuk kedua kalinya agar teks yang dihasilkan menciptakan karakter deng 32 bit. dalam pembagian kedua ini karakter akan dipecah kembali kedalam 4 putaran dan akan disimpan dalam Mid dan Ki dengan jumlah bit 32. Pada pemecahan kedua ini, akan divariasi bentuk putarannya agar berbeda dengan pemecahan pertama tadi dan disimpan dala <<<s. setelah dihasilakan karakter yang berbeda dari pesan asli yang memiliki jumlah bit sebanyak 32 bit, hal ini sesuai dengan pernyataan yang diutarakan oleh Rivest (1991), (dikutip oleh Bhandari (2017)).

2.6.3 Prinsip Dasar MD5

Rivest menjelaskan bahwa *Message Digest Algorithm* 5 (MD5) adalah salah satu penggunaan fungsi *hash* satu arah yang paling banyak digunakan. MD5 merupakan fungsi *hash* kelima yang dirancang oleh Ron Rivest dan didefinisikan pada RFC 1321. MD5 merupakan perkembangan dari MD 4 dimana terjadi penambahan satu ronde. MD5 memproses teks masukan kedalam blok-blok bit sebanyak 512 bit yang di inisialisasikan dengan *Xi*, kemudian dibagi ke dalam 32 bit sub blok sebanyak 16 buah. Keluaran dari MD5 berupa empat buah blok yang masing-masing 32 bit yang bisa disebut nilai *hash*. (dikutip oleh Sofyan, dkk. 2006).



Gambar 2. 6 Simpul Utama MD5 (Sofyan, dkk. 2006)

Sofyan, dkk. 2006 menjelaskan pada Gambar 2.6 merupakan simpul utama dari MD5. Simpul utama dari MD5 mempunyai blok pesan dengan panjang 512 bit yang masuk ke dalam 4 buah ronde. Hasil keluaran dari MD5 adalah berupa 128 bit dari byte terendah A dan tertinggi D. *message digest algorithm 5(MD5)* terdapat empat buah *word* 32 bit register yang digunakan untuk menginisialisasi *message digest* pertama kali. Register-register ini di insialisasikan dengan bilangan hexadecimal.

Word A : 01 23 45 67

Word B : 89 AB CD EF

Word C :FE DC BA 98

Word D : 76 54 32 10

Register-register ini biasa disebut dengan nama *chain variable* atau rantai. Proses pesan disalah satu blok MD5 memiliki fungsi untuk tiap operasinya yaitu :

F (X, Y, Z) = (X Y) ((X) Z)

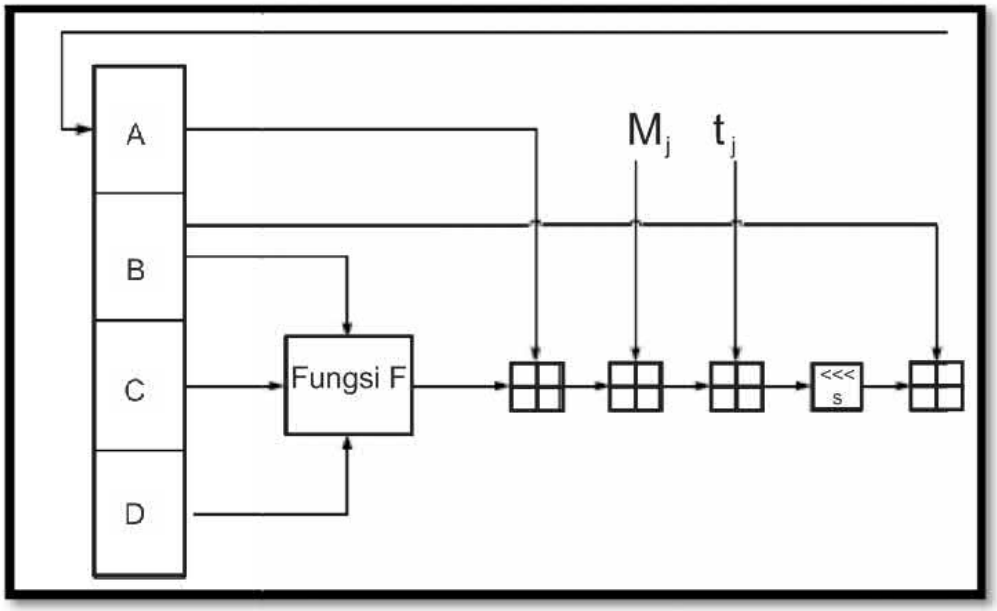
G (X, Y, Z) = (X Z) (Y (Z))

H (X, Y, Z) = X Y Z

I (X, Y, Z) = Y (X (Z))

(untuk XOR, untuk AND, untuk OR, dan NOT).

Pada Gambar 2. 7 menunjukkan satu buah blok operasi dari MD5 dengan operasi yang dipakai sebagai contoh adalah FF(a,b,c,d, M_j,s, t_i) menunjukan a = b + ((a + F (b,c,d) + M_j + t_i) <<< s).



Gambar 2. 7 Satu Buah Operasi MD5

Gambar 2.7 menggambarkan bila M_j menggambarkan pesan ke-j dari sub blok (dari 0 sampai dengan 15) dan <<<s menggambarkan bit akan bergeser ke kiri sebanyak s bit, maka keempat operasi dari masing-masing ronde adalah :

FF(a,b,c,d,M_j,s,t) menunjukan a= b + ((a + F(b,c,d) + M_j + t_j) <<<s)

GG(a,b,c,d,M_j,s,t) menunjukan a= b + ((a + G(b,c,d) + M_j + t_j) <<<s)

HH(a,b,c,d,M_j,s,t) menunjukan a= b + ((a + H(b,c,d) + M_j + t_j) <<<s)

II(a,b,c,d,M_j,s,t) menunjukan a= b + ((a + I(b,c,d) + M_j + t_j) <<<s)

Keluaran dari MD5 adalah 128 bit dari *word* terendah A dan tertinggi D masing-masing 32 bit.

2.6.4 Cara Kerja dan Alur Logika MD5

1. Penambahan bit penyangga (*padding bits*)

   Kongruen sampai 448, modulo 512. Pesan diperpanjang hanya 64 bit kemudian menjadi 512 bit. Walaupun panjang pesannya sudah kongruen sampai 448, modulo 512. Padding dilakukan sebagi berikut: bit “1” tunggal dimasukkan ke pesan, dan kemudian “0” bit ditambahkan sehingga panjang bit pesan menjadi kongruen sampai 448, modulo 512. Satu bit dan paling banyak 512 bit ditambahkan secara menyeluruh.

2. Penambahan panjang pesan semula

   Representasi 64 bit S ditambahkan ke langkah hasil sebelumnya. Tidak memungkinkan S lebih besar dari 2 pangkat 64, dan urutan

rendah 64 bit S. kemudian pesan yang dihasilkan adalah (padding dengan bit dan dengan S) memiliki panjang yang merupakan kelipatan dari 512 bit. Secara ekivalen, pesan ini memiliki panjang yang merupakan kelipatan 4 dari 16 (32bit) kata.

3. Inisialisasi penyangga (Buffer) MD

   Buffer empat kata (A,B,C,D) digunakan untuk menghitung ringkasan pesan. Disini masing-masing A,B,C,D adalah register 32-bit. Register ini adalah diinisialisasikan ke nilai dalam byte heksadesimal dan rendah pertama.

4. Pengolahan pesan dalam blok 512 bit

   Empat fungsi tambahan yang menggunakan 3 huruf untuk penginputan 32-bit dan menghasilkan sebagai satu kata 32-bit.

2.7 SHA3

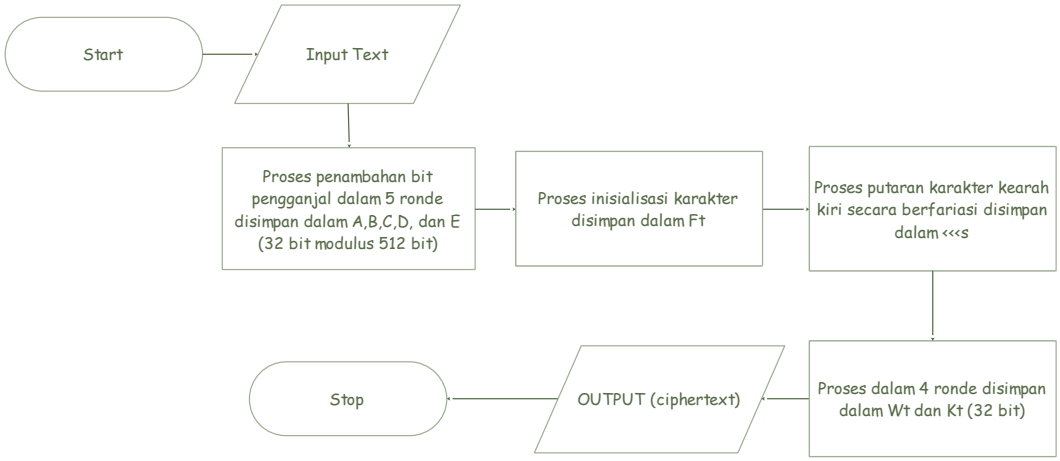
2.7.1. Tentang SHA3

NIST (2006) membuat sebuah standar *hash* baru, yaitu SHA3 yang dari perkembangannya berbagai model enkripsi SHA, NIST menemukan SHA3. SHA3 digunakan untuk menggantikan SHA2, dikarenakan belum ada serangan hebat yang terjadi pada SHA2. NIST membuat SHA3 dikarenakan kekhawatiran dikarenakan MD5, SHA0, SHA1 yang telah berhasil ditembus.

Tidak seperti model SHA sebelumnya, SHA3 memiliki ukuran keluaran yang berbeda-beda, salah satu keluarannya sama dengan model enkripsi MD5 dengan model enkripsi dan hasil enkripsi yang berbeda tentunya. SHA3 termasuk

kedalam jenis *sponge function*. Pada jurnal yang berjudul "*Cryptographic sponge function*", *sponge function* menyediakan cara tertentu agar dapat menggeneralisasikan fungsi hash dengan hasil keluaran yang beragam (Bertoni, 2011).

Langkah-langkah dalam model enkripsi SHA3 ini ditunjukkan pada Gambar 2.8 yang akan ditampilkan dalam bentuk *flowchart*.



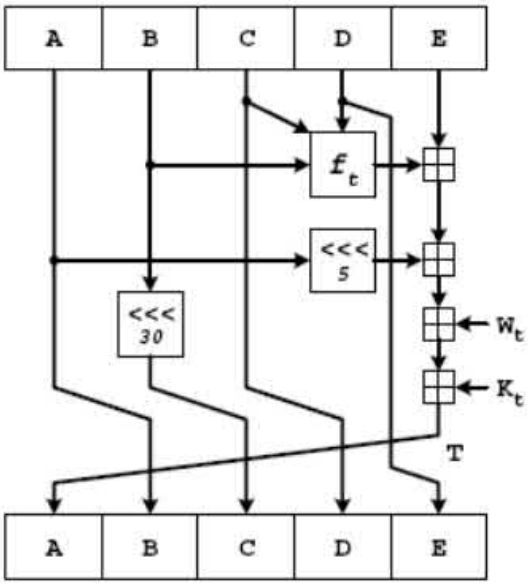
Gambar 2. 8 *Flowchart* Algoritma SHA3 (Luo, 2017)

Pada Gambar 2.8 (Luo, 2017) menyatakan bahwa tidak seperti model enkripsi MD5, pada SHA3 walupun akan menghasilkan karakter dengan 32 bit namun dalam proses penambahan bit pengganjal akan dibagi kedalam 5 ronde dengan karakter yang dihasilkan (32 bit modulus 512 bit) hal ini yang akan menjadi pembeda namun dapat di kolaborasikan. Setelah terbagi kedalam 5 ronde proses selanjutnya adalah inisialisasi karakter, untuk meminimalisir adanya perulangan karakter yang sama yang akanmembentuk suatu pola untuk diguanakan memecahkan kuncinya.

Proses selanjutnya adalah putaran karakter yaitu kearah kiri dan disimpan dalam <<<s. dari awal proses pertama hasil *ciphertext*-nya sudah memiliki 32 bit dalam karakter yang dihasilkan. Walaupun pada proses selanjutnya ini merupakan proses pembagian ronde lagi namun tidak akan mengubah jumlah karakter yang telah ada pada proses sebelumnya. Dalam pembagian terakhir akan diprose kedalam 4 ronde dan akan disimpan dalam Wt dan Kt (32 bit), baruah dihasilkan *ciphertext* dari SHA3.

2.7.2. Analogi SHA3

NIST, 2006 menyatakan bahwa enkripsi model SHA3 mempunyai kekuatan 2(80) bit, maksunya adalah, dengan melakukan *brute force*, data yang disandikan dengan algoritma ini akan menjamin menghasilkan suatu *ciphertext* yang memiliki keamanan yang baik.(dikutip oleh Huda, 2009).



Gambar 2. 9 Analogi dalam komputasi pada SHA3

Enkripsi SHA3 digunakan untuk meng-hash sebuah pesan, M, yang mempunyai panjang maksimum 2^{64} -1 bits. Algoritma ini menggunakan urutan dari 80 kali 32-bit kata, dengan menggunakan 5 variabel yang menampung 32 bits per variabel, dan hasil hashnya.

Misal urutan kata itu diberi tanda W_0, W_1,……, $W_{79.}$ 5 variabel itu diberi tanda A,B,C,D,E kata hasil hash diberi tanda H_0, H_1, H_2, H_3, H_4.

Lalu masuk ke langkah :

1. Melakukan padding terhadap pesan sehingga panjangnya adalah 448 modulus 512. Sehingga menjadi M=448+N.512. lalu membagi M menjadi $M^{(1)}$, $M^{(2)}$,….., $M^{(N)}$.
2. 64 bit sisanya adalah representasi biner dari panjang pesan.
3. Lalu masuk ke komputasi hash, dengan menggunakan iterasi $M^{(i)}$ dengan I = 1 sampai N dengan langkah :

   - Gunakan iterasi dari W, dengan symbol W_1:

$$W_t = \begin{cases} \mathrm{M}_t^{(i)} & , 0 \leq t \leq 15 \\ \mathrm{ROTL}^1(\mathrm{W}_{t-3} \emptyset \mathrm{W}_{t-8} \emptyset \mathrm{W}_{t-14} \emptyset \mathrm{W}_{t-16}, & 16 \leq t \leq 79 \end{cases}$$

   - Menginisialisasi A,B,C,D,E dengan hasil dari hash sebelumnya.

   - Lalu melakukan proses terhadap A,B,C,D,E sesuai rumus diatas :

T = $ROTL^5(A) + f_t(B, C, D) + E + K_t + W_t$

E = D

D = C

C = $ROTL^{30}(B)$

B = A

A = T

- Lalu menambahkan hasil A,B,C,D,E dengan hash sebelumnya sesuai urutan, lalu memasukkannya ke hasil hash yang sekarang juga sesuai urutan.

SHA digunakan untuk meng-*hash* subuah pesan, algoritma ini menggunakan urutan dari 80 kali 32-bit kata, dengan menggunakan 5 variabel yang menampung 32 bit per variabel, dan hasil hasnya.

BAB V

PENUTUP

5.1. Kesimpulan

Bardasarkan simulasi enkripsi modifikasi kolaborasi MD5 dan SHA3 dengan *salt function* dapat disimpulkan bahwa metode tersebut lebih aman dibandingkan dengan metode MD5 dan SHA yang telah ada sebelumnya. Keadaan tersebut dikarenakan metode modifikasi kolaborasi MD5 dan SHA3 dengan *salt function* tidak memiliki hasil *ciphertext* yang membentuk suatu pola yang dihasilkan. Disisi lain, perulangan kata pada sandi merupakan hal yang dibutuhkan dalam metode Babbage-Kasiski untuk dapat memprediksi informasi-informasi yang terdapat dalam sandi. Sehingga metode Babbage-Kasiski yang berpeluang mempredikasi sandi metode kolaborasi MD5 dan SHA3 dengan *salt function* tidak dapat memprediksi sandi yang dihasilkan oleh metode kolaborasi MD5 dan SHA3 dengan *salt function* tersebut, dikarenakan tidak adanya pola perulangan kata yang dapat diprediksi oleh metode Babbage-Kasiski.

5.2. Saran

Kekurangan dari penelitian ini adalah belum diketahui tingkat keamanan sandi yang dihasilkan apabila pesan yang dikodekan berkarakter sama dalam semua digit. Kekurangan lainnya berhubungan dengan efektifitas penggunaan sumber daya memori dan kecepatan pada proses enkripsi. Oleh karena itu, disarankan penelitian selanjutnya dapat meneliti tentang tingkat keamanan sandi

pada pesan yang memiliki karakter sama dan efektifitas penggunaan memori dan tingkat kecepatan enkripsi. Hal ini yang dilakukan pada penelitian selanjutnya adalah pengembangan metode kolaborasi MD5 dan SHA3 dengan *salt function* untuk menyandikan gambar, suara ataupun video.

DAFTAR PUSTAKA

Widiyanto, Ibnu, dkk. 2015. "Perilaku Pembelian Melalui Internet". Dalam JMK, Volume 17 No. 2. Hal 109-112.

Nore, Viktor Nikolas. 2013. Perancangan Sistem Informasi Penjualan dan Pemesanan Produk Berbasis WEB.

Purwanti, Endang. 2011. "Analisis Faktor-faktor Pengambilan Keputusan Pembelian Konsumen Pada Departemen Store/Supermarket Di Salatiga". Dalam *Among Makarti*, Volume 4. No. 7.

Ristania, Novia, dkk. "Analisa Pengaruh Harga, Promosi dan Viral Marketing Terhadap Keputusan Pembelian Pada "Online Shop" S-Nexian Melalui Facebook". Dalam *Jurnal of Business Strategy and Execution.* Hal 131-162.

Oetomo, Budi Sutedjo dharma, S.Kom., MM. 2006. *Perencanaan dan Pembangunan Sistem Informasi.* Yogyakarta : Penerbit Andi.

Nurrohmah, Enur Siti, dkk. 2018. *Instrument Design Diagnostic Test Three-Tier Multiple Choice Redox Material With Redox Diagnostic Tes Software (RDT).* Hal 190-199.

Anthony, Anthony, dkk. 2017. Analisis dan Perancangan Sistem Informasi Penjualan Berdasarkan Stok Gudang Berbasis *Client Server* (Studi Kasus Toko Grosir "Restu Anda"). Vol. 4. No. 2. Hal. 136-147.

Hariyanti, Dwi. 2008. Pengaruh Modal dan Volume Penjualan Terhadap Kemampulabaan Usaha Bakul Ikan Waita di Pasar Tulehu Kecamatan Salahutu Kabupaten Maluku Tengah. Vol. 4. No. 2.

Pangestu, Danu Wira. 2008. *Teknologi Dasar Sistem Informasi Manajemen.* Ilmu Komputer.Com.

Docs,Oracle."https://translate.google.com/translate?hl=id&sl=en&u=https://docs.oracle.com/cd/E24693_01/appdev.11203/e23448/d_crypto.htm&prev=search" (diakses tanggal 12 juni 2018)

Utomo, Shierly Lydiawati. 2012. Perancangan Sistem Penjualan Dalam Rangka Meningkatkan Ketertagihan Piutang Pada Usaha Percetakan di Surabaya. Vol. 1. No. 1.

Docs, Microsoft. https://docs.microsoft.com/enus/windows/desktop/seccrypto/data-encryption-and-decryption (diakses tanggal 17 juli 2018).

Bruen, A.A. dan M.A. Forcinito. 2005. *Cryptography, Infoormation Theory, and Error-Correction: A Handbook for the 21st Century.* A Jhon Wiley & Sons Inc. New Jersey.

Wurijanto, Tutut, dkk. 2013. Rancang Bangun Sistem Informasi Penjualan Berbasis *Cloud* Bagi Usaha Kecil dan Menengah di Indonesia. Hal. 52-59.

Inayatullah. 2007. Analisis Penerapan Algoritma MD5 Untuk Pengamanan *Password*. Vol. 3. No. 3.

Nuryana, Yana, dkk. 2017. Pengembangan Aplikasi Pengendalian Skripsi Berbasis Android Untuk Mahasiswa dan Dosen. Vol. 14. No. 2.

Luo, Pie, dkk. 2017. *Algebraic Fault Analysis of SHA-3 under Relaxed Fault Models*.

Aprida, Candra Dwi, dkk. 2013. Pembuatan Sistem Informasi Beasiswa Internal Direktorat Jendral Perbendaharaan Menggunakan PHP dan MySql. *Jurnal Teknik POMITS*. Vol. 2. No. 2.

Huda, Muharram W. 2009. *Perkembangan Enkripsi Fungsi Hash Pada SHA (Secure Hash Algorithm)*.

Krisanty, Tania. 2010. *Studi Mengenai Salt : Laboratorium Ilmu Rekayasa dan Komputasi*.

Bertoni, Guido, dkk. 2011. *Cryptographic Sponge Function.* (Version 0.1, January 14, 2011).

Tyagi, N. dan Anita G. 2014. Comparative Analysis of Symmetric Key Encryption Algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering* Vol. 4(8): 348-354.

Nishika dan R.K. Yadav. 2013. A Lookup Table Based Secure Cryptographic SMS Communication on Android Environment. *International Journal of Computer Science and Mobile Computing* Vol. 2(6): 53-56.

Dody, Andreanus, dkk. 2011. SIstem Pengamanan Data Menggunakan Metode MD5 dan *Private Key* pada Aplikasi Berbasis *Client Server* (Studi Kasus : KSP Buah Hati Bawen). *Jurnal Teknologi Informasi-Aiti, Vol.8. No.2.* Hal 101-200

Batubara, Febrin Aulia. 2012. "Perancangan Website Pada PT. RATU ENIM PALEMBANG.

Setiawan, Permadi, dkk. 2015. Rancang Bangun Aplikasi Pengolah Data Evaluasi Proses Belajar Mengajar Berbasis WEB pada Stikes Yayasan RS.Dr. SOETOMO Surabaya. Vol. 4. No. 2.

Sibyan, Hidayatus. 2017. "Implementasi Enkripsi Basis Data Dengan Algoritma MD5 (Message Digest Algorithm 5) dan Vigenere Cipher". Dalam *Jurnal PPKM I*, Hal 114-121.

Sofwan, Agus, dkk. 2006. "Aplikasi Kriptografi Dengan Algoritma Message Digest 5 (MD5)". Volume 11. No. 1. Hal 22-27.

Das, Saikat, dkk. 2016. "Implementation and Coparative Analysis of RSA and MD5 Algorithm". Volume 141. No. 9.

Jain, Garima, dkk. 2017. "*Performance Evaluation of Authenticate (MD5, SHA) Routing Traffic over EIGRP and OSPF with IPV6*". Volume 176. No. 8.

Scholar, Research, dkk. 2018. "*A STUDY ON FINGERPRINT HASH CODE GENERATION BASED ON MD5 ALGORITHM AND FREEMAN CHAIN CODE*". Volume 3. No. 1.

Lin, Jing, dkk. 2017. "*Approach of Tamper Detection for Sensitive Data Based on Negotiable Hash Algorithm*". Volume 13. No. 5.

Chauhan, Adviti, dkk. 2016. "*Review on Encrypt the text by MD5 and RSA in Client Cloud Approach*". Volume 2. No. 5.

Kumar, Senthil, K. dkk. 2016. "*Personalized Web Search Based On Client Side Ontology*". Volume 8. No. 2.

Patil, Ankita, dkk. 2015. "*Secure File Access Using MD5 for One Time Password Generation on Cloud*". Volume 2. No. 1.

Mahyudin, Rezza. 2006. "*Algoritma Message Digest 5 (MD5) dalam Aplikasi Kriptografi* ".

Munir, Rinaldi. 2004. "*Serangan (Attack) Terhadap Kriptografi* ".

Bhandari, Asmin, dkk. 2017. "*Enhancement of MD5 Algorithm for Secured Web Development*". Volume 12. No. 4.

Sharma, Deepika, dkk. 2015. "*Implementation of MD5- 640 Bits Algorithm*". Volume 3. No. 5.

Heriyanto, Tedi. 2009. "*Pengenalan Kriptografi*".

Walia, Priyanka, dkk. 201. "*Implementation of New Modified MD5-512 bit Algorithm for Cryptography*". Volume 1. No. 6.

Khairil, dkk. 2014. "Aplikasi Enkripsi dan Deskripsi Data Menggunakan Algoritma RC4 Dengan Menggunakan Bahasa Pemrograman PHP". Dalam *Jurnal Media Informasi*, Volume 10. No. 1. Bengkulu : Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.

Sudrajat, Antonius Wahyu. 2006. "Implementasi Enkripsi Database Menggunakan *Transparent Data Ecryption* Pada *Database Engine* Oracle". Volume 2. No. 3.

Bahri, Saipul, dkk. 2012. "Studi dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5 (Message-Digest Algorithm 5)".

Hidayat, Akik, dkk. 2013. Enkripsi dan Deskripsi Teks Menggunakan Algoritma *Hill Cipher* Dengan Kunci Matriks Persegi Panjang. Vol. 9. No. 1. Hal. 39-51.

Kashogi, E.Z. Adnan. 2008. *Algoritma Message Digest 5 (MD5).* Bandung.

Suryawan, Sayekti Harits, dkk. 2013. "Pengamanan Data Dengan Menggunakan Algoritma Enkripsi Rivest Code 5". Dalam *Jurnal Informatika Mulawarman.* Volume 8. No. 2.