IMPLEMENTASI ENKRIPSI DATA MESSAGE DIGEST ALGORITHM 5 (MD5) DAN SECURE HASH ALGORITHM (SHA-256) PADA SISTEM PENJADWALAN KARYAWAN AGROWISATA SETYA AJI FLOWER FARM BANDUNGAN

Skripsi

diajukan sebagai salah satu persyaratan untuk memperolah gelar Sarjana Pendidikan Program Studi Pendidikan Teknik Informatika dan Komputer

Oleh

Santi Sulastri

NIM. 5302414027

PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS NEGERI SEMARANG

2019

PERSETUJUAN PEMBIMBING

Nama	: Santi Sulastri
NIM	: 5302414027
Program Studi	: Pendidikan Teknik Informatika dan Komputer
Judul	:Implementasi Enkripsi Data Message Digest Algorithm 5 (MD5) dan Secure Hash Algorithm 256 (SHA-256) Pada Sistem Penjadwalan Karyawan Agrowisata Setya Aji Flower Farm Bandungan

Skripsi ini telah disetujui oleh pembimbing untuk diajukan siding panitia ujian skripsi Program Studi Pendidikan Teknik Informatika dan Komputer, Fakultas teknik Universitas Negeri Semarang.

Semarang, Maret 2019

Pembimbing

Riana Defi Mahadji Putri, S.T., M.T.

NIP. 197609182005012001

HALAMAN PENGESAHAN

Skripsi dengan judul "Implementasi Enkripsi Message Digest Algorithm 5 (MD5) dan Secure Hash Algorithm 256 (SHA-256) Pada Sistem Penjadwalan Karyawan Setya Aji Flower Farm Bandungan" telah di pertahankan didepan sidang Panitia Ujian Skripsi Fakultas teknik UNNES pada Maret tahun 2019.

Oleh

Nama : Santi Sulastri

NIM : 5302414027

Program Studi : Pendidikan Teknik Informatika dan Komputer

Panitia :

Ketua Panitia

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

Sekretaris Panitia

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

Penguji 1

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

Penguji 2

Drs. Ir. Henry Ananta, M.Pd., IPM
NIP. 195907051986011002

Penguji 3/Pembimbing

Riana Defi MP, S.T., M.T.
NIP.197609182005012001

Mengetahui:
Dekan Fakultas Teknik

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

PERNYATAAN KEASLIAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini, adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, magister, dan doktor) baik di Universitas negeri Semarang (UNNES) maupun perguruan tinggi lain.
2. Karya tulis ini adalah murni gagasan, rumusan, dan penelitian saya sendriri, tanpa bantuan pihak lain, kecuali arahan Pembimbing dan masukan Tim Penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat denga sesungguhnya dan apabila dikemudian hari ditemukan terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya ini, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini.

Semarang, Maret 2019
Yang membuat pernyataan

Santi Sulastri
NIM. 5302414027

MOTTO DAN PERSEMBAHAN

Motto

- “Allah tidak membebani seseorang itu melainkan sesuai dengan kesanggupannya” (QS. Al-Baqarah: 286).
- You can do it if you want it

Persembahan

Skripsi ini penulis persembahkan kepada:

- Allah SWT yang tak henti hentinya memberikan kemudahan dan kelancaran dalam penyusunan skripsi ini.
- Kedua orang tua saya, Ibu Maftukhah dan Bapak Sanuri, yang selalu memberikan doa, dukungan serta semangat.
- Kakak dan adik saya yang selalu memberi doa, dukungan, dan semangat.
- Seluruh teman-teman PTIK UNNES angkatan 2014.

SARI

Sulastri, Santi. 2019. “Implementasi Enkripsi Message Digest Algorithm 5 (MD5) dan Secure Hash Algorithm 256 (SHA-256) pada Sistem Penjadwalan Karyawan Setya Aji Flower Farm”. Pembimbing : Riana Defi Mahadji Putri, S.T., M.T. Pendidikan Teknik Informatika dan Komputer.

Perkembangan teknologi dan informasi yang sangat pesat membawa dampak positif yaitu kemudahan dalam berbagi informasi melalui jaringan komputer. Namun pada saat yang bersamaan juga menimbulkan dampak negatif yaitu informasi yang dibagi dapat diketahui atau diakses oleh pihak yang tidak bertanggung jawab. Maka dibutuhkan suatu mekanisme pengamanan informasi / data.

Penelitian ini mengusulkan sebuah mekanisme pengamanan informasi / data dengan menggunakan teknik kriptografi yaitu dengan menambahkan metode enkripsi pada suatu sistem berbasis web. Terdapat berbagai macam jenis enkripsi yang dapat digunakan, misalnya MD5 dan SHA-256. Namun penggunaan MD5 saja atau SHA-256 saja dinilai tidak cukup aman. Penelitian ini bertujuan untuk mengembangkan metode kolaborasi dari MD5 dan SHA-256. Enkripsi diterapkankan pada *password* pengguna pada sistem login web.

Hasil simulasi dapat diuji dengan mengukur ketahanan terhadap serangan *brute force* dan besar nilai *Avalanche effect.* Dari hasil pengujian yang dilakukan yaitu dengan menggunakan *software* penyerang CrackStation dan Rainbow Table hasil penyandian cukup aman dari serangan *brute force*. Dari pengujian *Avalanche effect* diperoleh hasil dengan nilai *AE* sebesar 71% yang artinya hasil penyandian cukup baik.

Kata Kunci : Enkripsi, MD5, SHA-256, *Brute force, Avalanche effect*

KATA PENGANTAR

Puji dan syukur penulis ucapan ke hadirat Allah SWT yang telah melimpahkan rahmat serta karunia-Nya sehingga penulis dapat mmenyelesaikan skripsi yang berjudul "Implementasi Message Digest Algorithm 5 (MD5) dan Secure hash Algorithm 256 (SHA-256) Pada Sistem Penjadwalan Karyawan Setya Aji Flower Farm Bandungan". Skripsi ini disusun sebagai salah satu persyaratan meraih gelar Sarjana Pendidikan pada program Studi S1 pendidikan Teknik Informatika dan Komputer Universitas Negeri Semarang. Penyelesaian skripsi ini tidak lepas dari bantuan berbagai pihak, oleh karena itu penulis menyampaikan ucapan terimakasih kepada:

1. Prof. Dr, Fathur Rokhman, M.Hum., Rektor Universitas Negeri Semarang atas kesempatan yang diberikan kepada penulis untuk menempuh studi di Universitas Negeri Semarang.
2. Dr. Nur Qudus, M.T., Dekan Fakultas Teknik, Dr. Ing. Dhidik Prastiyanto, S.T., M.T., Ketua jurusan Teknik Elektro, IR. Ulfah Mediaty Arief, M.T.., Ketua program studi Pendidikan Teknik Informatika dan Komputer atas fasilitas yang telah disediakan bagi mahasiswa.
3. Ibu Riana Defi Mahadji Putri, S.T., M.T., selaku dosen pembimbing yang telah memberikan bimbingan, arahan, nasehat serta motivasi dalam penulisan karya ini.

4. Seluruh dosen Jurusan Teknik Elektro Fakultas teknik Univers Semarang yangtelah banyak memberi bekal ilmu pengeta berharga.
5. Teman-teman mahasiswa PTIK Universitas Negeri Semara 2014.
6. Berbagai pihak yang telah memberi bantuan untuk penyusu yang tidak dapat penulis sebutkan satu persatu.

Penulis hanya dapat memanjatkan doa semoga semua pih membantu penulis dalam penyusunan skripsi ini mendapatkan pa SWT. Semoga skripsi ini dapat bermanfaat dan memberikan si berarti bagi pihak yang membutuhkan.

Semarang,

Penulis

DAFTAR ISI

Halaman

HALAMAN JUDUL.....i
PERSETUJUAN PEMBIMBING.....ii
HALAMAN PENGESAHAN.....iii
PERNYATAAN KEASLIAN.....iv
MOTTO DAN PERSEMBAHAN.....v
ABSTRAK.....vi
KATA PENGANTAR.....vii
DAFTAR ISI.....ix
DAFTAR TABEL.....xii
DAFTAR GAMBAR.....xiii
DAFTAR LAMPIRAN.....xv
BAB I.....1
1.1 Latar Belakang.....1
1.2 Identifikasi Masalah.....5
1.3 Batasan Masalah.....6
1.4 Rumusan Masalah.....6
1.5 Tujuan Penelitian.....7
1.6 Manfaat Penelitian.....7
BAB II.....8
2.1 Kajian Pustaka.....8

Halaman

2.2 Landasan Teori 10
2.2.1 Sistem 10
2.2.2 Kriptografi 11
2.2.3 Fungsi Hash 13
2.2.4 MD5 15
2.2.5 SHA-256 18
BAB III 22
3.1 Waktu dan Pelaksanaan 22
3.2 Desain Penelitian 23
3.2.1 Analisis Keamanan Sistem 24
3.2.2 Desain Sistem 24
3.2.3 Pengkodean 38
3.2.4 Pengujian Aplikasi 40
3.3 Alat dan Bahan Penelitian 41
3.4 Parameter Penelitian 41
3.5 Teknik Pengumpulan Data 42
3.6 Teknik Analisis Data 42
BAB IV 44
4.1 Deskripsi Data 44
4.1.1 Hasil Penyandian 44
4.1.2 Hasil Uji Rainbow Table 44
4.1.3 Hasil Uji Crack Station 45

Halaman

4.2 Analisis Data 47
4.2.1 Skenario Pengujian *Avalanche effect* 47
4.2.2 Hasil Pengujian *Avalanche effect* 48
4.3 Pembahasan 53
BAB V 56
5.1 Simpulan 56
5.2 Saran 57
DAFTAR PUSTAKA 58
LAMPIRAN 61

DAFTAR TABEL

Halaman

Tabel 4.1 Hasil Penyandian.....44

Tabel 4.2 Pengujian *Avalanche effect* 51

DAFTAR GAMBAR

Halaman

Gambar 2.1 Bentuk umum sistem 11

Gambar 2.2 Proses MD5 16

Gambar 2.3 Satu langkah proses transformasi SHA-256 19

Gambar 3.1 Model Sekuensial Linier (Pressman, 2001) 24

Gambar 3.2 Tahap Penelitian 25

Gambar 3.3 Use Case Diagram Sistem Penjadwalan 28

Gambar 3.4 Use Case Diagram Admin 29

Gambar 3.5 Use Case Diagram Karyawan 29

Gambar 3.6 Tampilan Halaman Login 30

Gambar 3.7 Tampilan Halaman Beranda 31

Gambar 3.8 Tampilan Halaman Manajemen Pekerjaan 31

Gambar 3.9 Tampilan Halaman Manajemen SDM 32

Gambar 3.10 Tampilan Halaman Manajemen Hari Kerja 33

Gambar 3.11 Tampilan Halaman Penjadwalan 34

Gambar 3.12 Tampilan Halaman Kehadiran 34

Gambar 3.13 Tampilan Halaman User 35

Gambar 3.14 Tampilan Halaman Jadwal (Karyawan) 36

Gambar 3.15 Tampilan Halaman Profil (Karyawan) 36

Gambar 3.16 *Activity Diagram* Sistem Penjadwalan 37

Gambar 3.17 Desain Arsitektur Sistem 36

Halaman

Gambar 3.18 *Flowchart* Modifikasi Enkripsi MD5 dan SHA-256 37

Gambar 3.19 Rancangan Kolaborasi Enkripsi.....38

Gambar 3.20 Hasil Pengujian RainbowTable.....45

Gambar 4.1 Hasil Pengujian 1 CrackStation 46

Gambar 4.2 Hasil Pengujian 2 CrackStation 46

DAFTAR LAMPIRAN

Halaman

Lampiran 1. Hasil Pengujian Rainbow Table 62

Lampiran 2. Hasil Pengujian CrackStation 63

Lampiran 3. *Source code* simulasi penyandian 68

Lampiran 2. Surat Usulan Topik Skripsi 69

Lampiran 3. Surat Usulan Dosen Pembimbing 70

Lampiran 4. Surat penetapan Dosen Pembimbing 71

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan informasi pada saat ini berkembang sangat pesat, perkembangan ini membawa perubahan besar dalam kehidupan manusia. Dampak positif dari perkembangan teknologi pada saat ini adalah informasi dapat dibagi melalui jaringan komputer. Namun pada saat yang bersamaan keadaaan tersebut dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan kejahatan, seperti melakukan pencurian data atau informasi. Maka dari itu dibutuhkan suatu mekanisme pengamanan untuk suatu sistem.

Ada berbagai aspek keamanan informasi yang dapat dilakukan untuk mengamankan suatu sistem, salah satunya yaitu memberikan *Access Control*. Aspek ini berhubungan dengan aspek *Authentication* dan *Privacy*. *Access Control* seringkali dilakukan dengan kombinasi user id dan password. Penggunaan password yang statis dapat memungkinkan terjadinya pencurian password oleh hacker, maka dibutuhkan suatu mekanisme pengamanan password yang dapat dilakukan dengan menerapkan ilmu kriptografi didalamnya.

Kriptografi (Cryptography) berasal dari Bahasa Yunani, *Cyptos* artinya *secret* atau rahasia sedangkan *graphein* berarti: *writing* atau tulisan. Sehingga kriptografi berarti *secret writing* atau tulisan rahasia. Menurut Mohamad Natsir (2017): Kriptografi dapat diartikan sebagai ilmu untuk menjaga kerahasiaan

informasi dengan metode dan teknik matematika yang cukup *confidentialy, integrity, authentication* dan *non-repudation.*

Kriptografi bertujuan untuk menjaga kerahasiaan suatu data sehingga informasi tersebut tidak mudah diketahui oleh pihak lain yang tidak sah. Kriptografi mentransformasikan data asli atau yang sering disebut dengan *plaintext* dengan data hasil atau data rahasia yang disebut dengan *chipertext*. Kriptografi terdiri dari dua proses yaitu proses mentransformasikan *plaintext* menjadi *chipertext* atau yang disebut dengan Enkripsi dan proses mentranformasikan kembali *chipertext* menjadi *plaintext* yang disebut dengan Dekripsi (Abdullah & Erliana, 2012).

Enkripsi data merupakan salah satu cabang dari ilmu kriptografi. Dalam enkripsi data dikenal suatu fungsi yang disebut dengan hashing. Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang dan dikonversikan menjadi string dengan keluaran yang panjangnya tetap (*fixed)* (Virgian, Yudha, Agani, & Hardjianto, 2016).

Terdapat dua macam fungsi hash yaitu satu arah dan dua arah. Menurut Huda (2009) Fungsi hash satu arah (*one-way hash function*) adalah fungsi hash yang bekerja satu arah dimana fungsi hash yang dengan mudah dapat menghitung hash value dari *pre-image*, tetapi sangat sukar untuk menghitung *pre-image* dari hash value atau biasa disebut dengan fungsi hash yang tidak bisa dikembalikan ke nilai hash awal.

Banyak fungsi hash yang dapat digunakan untuk mengamankan data, salah satunya yaitu MD5. Menurut Bahri dkk (2012) MD5 merupakan singkatan dari

Message-Digest algorithm 5, adalah fungsi matematika yang merubah variable dari suatu data yang berukuran besar menjadi lebih sederhana. Pada MD5 menghasilkan enkripsi dengan panjang 32 karakter.

Menurut Khairina (2011) Penggunaan MD5 hanya untuk menghindari pengiriman *password* secara apa adanya tanpa adanya perlindungan atau pengamanan ke webserver. Pada masa sekarang banyak tool yang dapat mendekripsi hasil dari enkripsi MD5, sehinga penggunaan MD5 dirasa kurang aman. Maka dari itu pada penelitian ini menambahkan jenis enkripsi lain yaitu SHA256.

SHA-256 adalah fungsi hash satu arah yang dirancang oleh The Nasional Institute of Standars and Technology (NIST) pada tahun 2002. Pada SHA-256 terdapat tiga penambahan fungsi baru dari jenis SHA yang sebelumnya yaitu SHA-1. Fungsi hash ini berfungsi dalam integritas suatu pesan: setiap perubahan pada pesan, dengan memiliki probabilitas yang tinggi akan menghasilkan *message digest* yang berbeda. Sehingga SHA-256 di sebut aman (Sklavos & Koufopavlou, 2005).

Selain itu, dalam penelitian perbandingan antara algoritma RC4, MD5 dan SHA yang diimplementasikan pada suatu sistem berbasis web didapat hasil bahwa, RC4 kurang cocok untuk digunakan dalam sistem keamanan data berbasis web dikarenakan RC4 merupakan metode enkripsi chipper key, sedangkan metode enkripsi MD5 kurang bagus dibandingkan dengan SHA, karena rentan terhadap *collision attack.* Jadi SHA direkomendasikan untuk digunakan dalam sistem keamanan data berbasis web (Prasetyo & Hikmawan, 2015).

Setya Aji Flower Farm merupakan agrowisata yang mengambil tema berupa taman / kebun bunga yang berlokasi di dusun Ngasem desa Jetis kecamatan Bandungan. Tidak hanya perkebunan yang menjadi daya tarik tersendiri, namun wisatawan juga dapat melihat dan mengamati aktifitas serta hiruk pikuk para petani bunga. Dengan adanya wisata ini maka perekonomian desa menjadi lebih baik dikarenakan banyaknya wisatawan yang mencapai 116.857 pada periode januari 2017 sampai januari 2018. Dengan tujuan memajukan desa dan menambah pendapatan bagi para petani bunga maka wisata ini dikelola oleh masyarakat desa setempat.

Luas perkebunan Setya Aji ini sekitar 5Ha yang terdiri dari beberapa lahan dengan pemilik yang berbeda dan jumlah pekerja yang mencapai ratusan menjadikan perkebunan ini memiliki beberapa jenis pekerjaan, diantaranya petani, tukang panggul / angkut bunga, sopir, karcis dan parkir. Petani pada agrowisata ini merupakan pemilik lahan yang ikut bergabung untuk menjadikan lahannya sebagai tempat wisata. Dimana para petani datang setiap hari untuk mengelola lahan yang dimilikinya. Tukang panggul / angkut bunga dan sopir merupakan pekerja yang dipekerjakan para petani pemilik lahan yang bekerja pada saaat panen dan penanaman bibit. Karcis dan tukang parkir merupakan warga desa setempat yang bekerja sebagai karyawan, pada bagian ini pekerja dibentuk kelompok / regu hari kerja yang menjadi kesepakatan bersama. Para karyawan bekerja berdasarkan system rolling harian. Hari kerja pada perkebunan ini yaitu setiap hari, dengan penjadwalan dan penentuan banyaknya pekerja ditentukan dengan kebutuhan harinya.

Penjadwalan yang masih menggunakan cara tradisional seringkali menimbulkan beberapa masalah, seperti kerancuan pada pembagian hari kerja, adanya kerangkapan jatah hari kerja yang menimbulkan pembagian hari kerja yang tidak merata. Masalah tersebut timbul karena belum adanya sistem penjadwalan atau pengeolaan karyawan yang terstruktur dan terdokumentasi dengan baik. Pembuatan sistem penjadwalan karyawan setya aji flower farm telah berhasil dibuat sebagai embrio awal sistem informasi penjadwalan yang akan di terapkan di agrowisata Setya aji flower farm.

Dalam penelitian ini, peneliti bermaksud untuk membuat kolaborasi dari enkripsi SHA-256 yang dikombinasikan dengan fungsi lain yang dihasilkan dari generate menggunakan MD5 dan akan diterapkan dalam sistem penjadwalan karyawan dengan judul "Implementasi Enkripsi MD5 dan SHA-256 pada Sistem Penjadwalan Karyawan Agrowisata Setya Aji Flower Farm Bandungan".

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan diatas, maka dapat dirumuskan beberapa identifikasi permasalahan yang akan dibahas, yaitu:

1. Rawannya pencurian data oleh pihak yang kurang bertanggungjawab.
2. Belum adanya sistem pengamanan data pada sistem penjadwalan karyawan agrowisata setya aji flower farm
3. Dibutuhkannya sistem penjadwalan yang dapat diakses karyawan dan admin yang aman untuk digunakan.

1.3 Pembatasan Masalah

Sebagai ruang lingkup perancangan penelitian ini, peneliti mengambil batas pembahasan agar menjaga konsistensi tujuan dari perancangan sistem itu sendiri, sehingga masalah yang dihadapi tidak meluas dan pembahasan menjadi terarah. Batasan tersebut adalah:

1. Penelitian ini dilakukan di Bandungan dan khususnya Agrowisata Setya Aji Flower Farm.
2. Simulasi enkripsi dibangun dengan menggunakan fungsi dari PHP.
3. Fungsi *hash* SHA-256 dibangun dengan memakai bawaan dari library.
4. Pengujian enkripsi dilakukan pada pesan teks *password* yang di dapatkan atau hasil enkripsi (chipertext-nya).
5. Pengembangan diakukan dengan menggunakan Metode Liniear Sequential Model.
6. Bahasa pemrograman untuk sistem yang dibangun menggunakan bahasa pemrograman PHP dan MySQL sebagai database.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas, maka dapat dirumuskan permasalahan yang akan dibahas dalam penelitian ini, yaitu Bagaimana mengkolaborasikan enkripsi MD5 dan SHA-256 dan mengimplementasikannya pada sistem penjadwalan karyawan agrowisata setya aji flower farm Bandungan agar didapatkan tingkat keamanan yang baik ?

1.5 Tujuan

Sesuai dengan permasalahan yang ada maka tujuan dilaksanakan penelitian ini adalah membuat mekanisme pengamanan data dengan mengkolaborasikan enkripsi MD5 dan SHA-256 yang akan diterapkan pada sistem penjadwalan karyawan.

1.6 Manfaat

1. Bagi agrowisata, diharapkan dengan adanya penelitian ini dapat mengembangkan agrowisata dan mengoptimalkan penjadwalan pada agrowisata Setya Aji Flower Farm
2. Bagi Penulis, diharapkan penelitian ini bermanfaat bagi penulis untuk menambah wawasan, sebagai pengembangan ilmu pengetahuan, dan sebagai dasar pengembangan bagi peneliti.

BAB II

KAJIAN PUSTAKA DAN LANDASAN TEORI

2.1 Kajian Pustaka

Dalam penelitian ini terdapat beberapa penelitian sebelumnya yang hampir sama dengan Sistem Informasi Penjadwalan Karyawan Agrowisata Setya Aji Flower Farm diantaranya sebagai berikut :

Penelitian yang pertama yaitu penelitian mengenai pentingnya keamanan pada sistem *login* yaitu pada bagian *password* . Sistem informasi yang terhubung ke jaringan public akan sangat berbahaya jika *password* yang dimasukan *user* tidak dilengkapi dengan enkripsi. Pentingnya memperhatikan pengamanan dengan mengenkripsi *password* pada sistem *login* sebelum data dikirm ke server juga dibahas dalam penelitian yang dilakukan oleh Khairina (2011) yang berjudul Analisis Keamanan Sisem Login bahwa proses enkripsi dapat dilakukan dengan menggunakan MD5 yang dikombinasikan dengan fungsi yang lain. Dalam penelitian tersebut kombinasi dilakukan dengan pengacak atau menggabungkan *password* asli dengan suatu *string* tertentu lalu dienkripsi. Sedangkan pada penelitian yang akan peneliti lakukan kombinasi akan dilakukan dengan enkrisi lain yaitu SHA-256.

Dalam pengujian Time Respone yang dilakukan oleh Abdilah, dkk (2017) Yang berjudul *Implementation of Cryptosystem using Method Algorithm ECC with Function of Hash SHA-256 in online ticketing system*

mengemukakan bahwa jumlah penginputan data yang dilakukan menggunakan kunci ECC dan SHA-256 lebih lambat dikarenakan kunci yang dihasilkan SHA-256 lebih panjang dibanding MD5, kunci yang lebih panjang maka akan lebih aman dikarenakan semakin sulit untuk melakukan pembukaan kunci.

Keamanan SHA-256 juga diuji pada penelitian yang dilakukan oleh Ichwan, dkk (2016) dengan judul Implementasi *Keyed-Hash Message Authentication Code* Pada Sistem Keamanan Rumah bahwa keamanan algoritma *hash* dibuktikan dengan *Avelanche Effect.* Dari hasil pengujian 16 *round* pertama pada *round function* algoritma SHA-256 dapat menghasilkan nilai rata-rata *Avelanche Effect* sebesar 62%, dan setelah 64 *round* menghasilkan nilai sebesar 85,9%. Ini menunjukan bahwa keluaran SHA-256 memiliki tingkat pengacakan yang bagus.

Modifikasi penggunaan SHA-256 juga pernah dilakukan oleh Roshdy, dkk (2013) dalam penelitiannya yang berjudul Design Implementation A New Security Hash Algorithm Based On MD5 and SHA-256 bahwa penggunaan SHA-256 saja tidak cukup aman karena memiliki serangan untuk 46 (dari 64) langkah. Hasil pengujian algoritma yang telah dimodifikasi tersebut menunjukan bahwa keamanannya lebih tinggi dibanding hanya menggunakan SHA-256 atau MD5 saja.

Berdasarkan penelitian-penelitian yang telah diuraikan sebelumnya, peneliti akan menerapkan enkripsi MD5 dan SHA-256 untuk mengamankan data. Kombinasi akan dilakukan dengan mengambil dua *string* dari hasil generate MD5 yang kemudian akan menjadi *padding* pada *password* dan

kemudian akan dienkripsi menggunakan SHA-256 sebelum disimpan ke database.

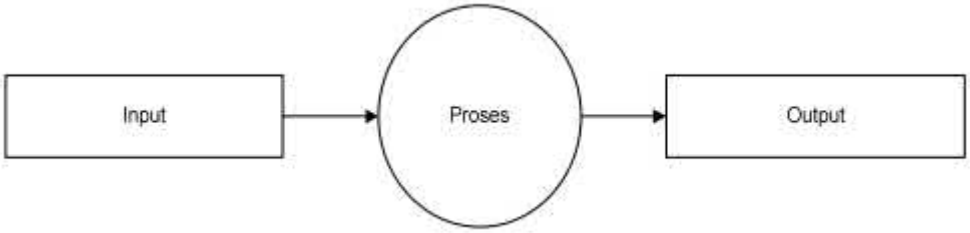
2.2 Landasan Teori

2.2.1 Sistem

Dalam mendefinisikan pengertian dari sistem ada dua kelompok pendekatan yaitu menekankan pada prosedurnya dan menekankan pada elemennya. Pendekatan sistem yang lebih menekankan pada prosedurnya mendefinisikan sistem adalah suatu jaringan kerja dari prosedur – prosedur yang saling berhubungan berkumpul bersama-sama untuk melakukan kegiaan atau untuk menyelesaikan suatu masalah (Jogiyanto : 2015).

Sistem itu adalah suatu kumpulan atau variable yang terorganisasi, saling interaksi, saling bergantung satu sama lain dan terpadu.

Bentuk umum dari suatu sistem terdiri atas masukan (*input*), proses dan keluaran (*output*), dalam bentuk umum sistem ini bias melakukan satu atau lebih masukan yang akan diproses dan menghasilkan keluaran sesuai dengan rencana yang telah direncanakan sebelumnya.



Gambar 2.1 Bentuk umum sistem.

2.2.2 Kriptografi

Sadikin (2012) dalam bukunya mengatakan bahwa kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika yang menyediakan keamanan informsai seperti kerahasiaan, keutuhan data dan otentikasi entitas. Dalam arti lain, Brenton dan Hunt (2005) dalam bukunya mengatakan Cryptography adalah sekumpulan teknik yang digunakan untuk mengubah informasi kedalam format alternative yang kemudian bisa diubah kembali ke format semula.

Kromodimoeljo (2009) dalam bukunya mengatakan Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Proses enkripsi adalah proses pengacakan "naskah asli" (*plaintext*) menjadi "naskah acak" (*chipertext*) yang "sulit untuk dibaca" oleh seseorang yang tidak mempunyai kunci dekripsi.

Munir (2004) Kriptografi memiliki beberapa aspek dalam memberikan layanan keamanan. Aspek tersebut diantaranya:

1. Kerahasiaan (*confidentiality*), layanan ii digunakan untuk menjaga kerahasian isi pesan.
2. Otentikasi (*authentication*), layanan ini berkaitan dengan keaslian pengirim, mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan

(*data authentication*). Dengan kata lain, masalah ini dapat diungkapkan sebagai pertanyaan:”Apakah pesan yang diterima benar-benar berasal dari pengirim yang sesunggguhnya ?”

3. Integritas data (*data integrity*), layanan ini berkaitan dengan keutuhan pesan. Dengan kata lain, masalah ini dapa diungkapkan sebagai pertanyaan:”Apakah pesan yang diterima tidak mengalami perubahan(modifikasi)?”
4. Anti-penyangkalan (*nonrepudiation*), layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan.

Dalam kriptografi juga terkenal beberapa istilah atau terminology yang biasa digunakan, diantaranya sebagai berikut:

1. Pengirim dan penerima pesan

   Pengirim dan penerima pesan merupakan entitas yang melakukan komunikasi dengan bertukar pesan. Entitas dapat berupa orang, mesin (komputer), kartu kredit, dan lain sebagainya.

2. Pesan, *Plaintext, Chipertext*

   Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah *plaintext* atau teks-jelas (*cleartext*). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan disandikan kebentuk lain. Bentuk dari pesan yang tersandi tersebut disebut dengan *chipertext* atau *cryptogram.*

3. Enkripsi dan Dekripsi

Proses menyandikan *plaintext* menjadi *chipertext* disebut enkripsi. Sebaliknya, mengembalikan pesan kebentuk aslinya (*plaintext*) disebut dengan dekripsi.

4. Kriptanalisis dan Kriptologi

   Kriptanalisis adalah ilmu dan seni ntuk memecahkan *chipertext* menjadi *plaintext* tanpa mengetahui kunci yang diberikan. Pelakunya disebut kritanalis. Kriptologi adalah studi mengenai kriptografi dan kriptanalisis.

2.2.3 Fungsi Hash

Sadikin (2012) Fungsi *hash* adalah fungsi yang melakukan pemetaan pesan dengan panjang sembarang ke sebuah teks khusus yang disebut *message digest* dengan panjang tetap. Fungsi *hash* yaitu fungsi yang masukannya sebuah pesan dan keluarannya sebuah sidik pesan (*message digest*). Kriteria yang menjadi standard untuk algoritma *hash* yaitu, (Kromodimoeljo, 2009):

1. *Preimage resistance.* Untuk suatu nilai *hash* yang sembarang (tidak diketahui asal-usulnya), sangat sukar untuk mencari naskah yang mempunyai nilai *hash* tersebut.
2. *Second preimage resistance.* Untuk suatu naskah $m_{1,}$ sangat sukar untuk mencari naskah lain m_2 ($m_{1\neq}\ m_2$) yang mempunyai nilai (*hash*(m_1) = *hash*(m_2). Ini sering disebut juga *weak collision resistance.*
3. *Collision resistance.* Sangat sukar untuk mencari dua naskah m_1 dan m_2 yang berbeda ($m_{1\neq}\ m_2$) yang mem[unyai nilah *hash* yang sama (*hash*(m_1) = *hash*(m_2). Ini sering disebut juga *strong collision resistance.*

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:

$$h = H (M)$$

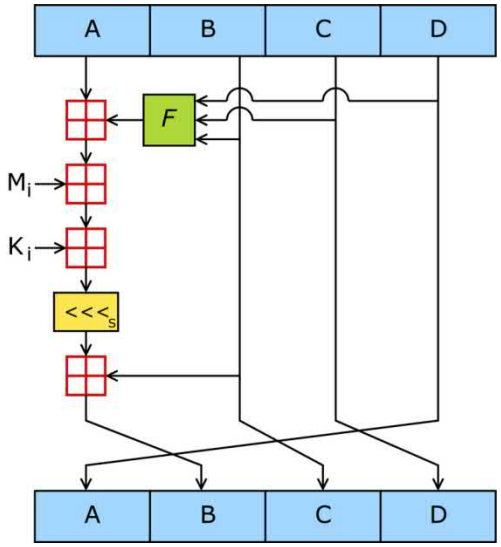
Pada persamaan diatas, h adalah nilai *hash* atas *message digest* dari *H* untuk masukan *M*. dengan kata lain fungsi *hash* mengkonfersi sembarang pesan yang ukurannya selalu tetap.

2.2.4 MD5

Algoritma MD5 (*Message Digest 5*) dirancangoleh Ron Rivest dan penggunaannya sangat popular dikalangan komunitas *open source* sebagai *checksum* untuk *file* yang dapat di *download* . MD5 juga kerap digunakan untuk menyimpan password dan juga digunakan dalam *digital signature* dan *certificate.* Besarnya blok untuk MD5 adalah 512 bit sedangkan *digest size* adalah 128 bit. Karena *word size* ditentukan sebesar 32 bit, satu blok terdiri dari 16 *word* sedangkan *digest* terdiri dari 4 *word.* MD5 adalah salah satu fungsi *hash* yang paling banyak digunakan.(Kromodimoeljo, 2009).

1. Cara Kerja MD5

   MD5 mengolah blok 512 bit, dibagi kedalam 16 sub blok berukuran 32 bit. Keluaran algoritma diset menjadi 4 blok yang masing-masing berukuran 32 bit yang setelah digabungkan akan membentuk nilai *hash* 128 bit. MD5 terdiri atas 64 operasi, dikelompokan dalam empat putaran dari 16 operasi proses tersebut dapat dilihat pada gambar 2.1.



Gambar 2.1 Satu operasi MD5

Keterangan :

F : adalah fungsi nonlinear, satu fungsi digunakan pada tiap-tiap putaran,

M_i : menunjukan blok 32 bit dari masukan pesan,

K_i : menunjukan konstanta 32 bit, berbeda untuk tiap-tiap operasi,

$<<<_I$: menunjukan perputaran bit kiri oleh $_{s;s}$ bervariasi untuk tiap-tiap operasi

: menunjukan tambahan modulo 2^{32}

2. Langkah – langkah yang dibutuhkan untuk menghitung intisari pesan adalah sebagai berikut :

1. Penambahan bit

Pesan akan ditambahkan bit-bit tambahan sehingga panjang bit akan kongruen dengan 448, mod 512. Hal ini berarti pesan akan mempunyai panjang yang hanya kurang 64 bit dari kelipatan 512 bit. Penambahan bit selalu dilakukan

walaupun panjang dari pesan kongruen dengan 448, mod 512 bit. Penambahan bit dilakukan dengan menambahkan “1” diawal dan diikuti “0” sebanyak yang diperlukan sehingga panjang kongruen dengan 448, mod 512.

2. Penambahan Panjang Pesan

   Setelah penambahan bit, pesan masih membutuhkan 64 bit agar kongruen dengan kelipatan 512 bit. 64 bit tersebut merupakan perwakilan dari b (panjang pesan sebelum penambahan bit dilakukan). Bit-bit ini ditambahkan ke dalam dua word (32 bit) dan ditambahkan dengan *low-order* terlebih dahulu. Penambahan pesan ini biasa disebut juga *MD Strengthening* atau Penguatan MD.

3. Inisialisai MD5

   Pada MD5 terdapat empat buah *word* 32 but register yang berguna untuk menginisialisasi *message digest* pertama kali. Register-register ini diinisialisasikan 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 variable rantai.

4. Proses Pesan di dalam Blok 16

   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))

5. Keluaran MD5

2.2.5 SHA-256

Fungsi *hash* SHA-256 merupakan versi SHA dengan ukuran *digest* 256 pada versi SHA2. SHA merupakan singkatan dari *Secure Hash Algorithm* adalah fungsi *hash* satu arah yang dibuat oleh NIST (*National Institute of Standard and Technology*), (NIST, 1995a). oleh NSA, SHA dinyatakan sebagai standard fungsi *hash* satu arah. SHA didasarkan pada MD4 yang dibuat oleh Ronald L. Rivest dari MIT. SHA disebut aman karena ia rancang sedemikian sehingga secara komputasi tidak mungkin menemukan pesan yang berkoresponden dengan *message digest* yang diberikan.

SHA-256 menggunakan enam logika, dimana setiap fungsi beroperasi pada 32-bit, yang direpresentasikan sebagai x, y, dan z. Fungsi logikatersebut merupakan kombinasi dasar seperti AND, OR, XOR, pergeseran bit ke kanan (*shift right*), dan rotasi bit ke kanan (*rotate right*).

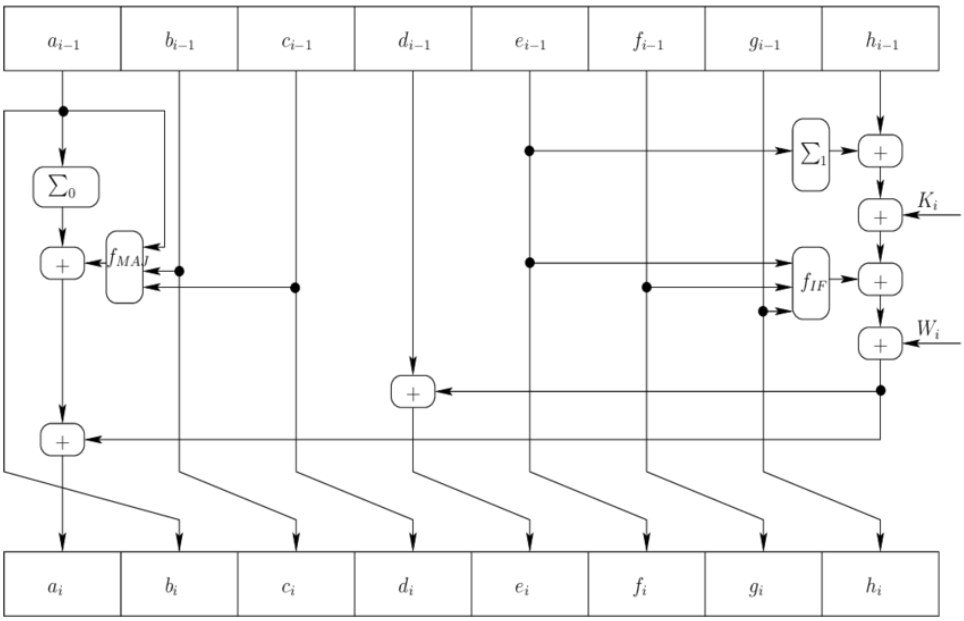
A. Dasar Prinsip SHA-256

Algoritma SHA-256 dapat digunakan untuk menghitung nilai *message digest* dari sebuah pesan, dimana pesan tersebut memiliki panjang maksismum 2^{64} bit. Algoritma ini menggunakan sebuah *message schedule* yang terdiri dari

64 element 32-bit *word*, delapan buah variable 32-bit, dan variable penyimpan nilai *hash* 8 buah *word* 32-bit. Hasil akhir dari algoritma SHA-256 adalah sebuah *message digest* sepanjang 256-bit.

B. Cara Kerja

SHA-256 mengubah pesan masukan ke dalam *message digest* 256 bit. Berdasarkan Secure Hash Signature Standard, pesan masukan yang panjangnya lebih pendek dari 2^{64} bit, harus dioperasikan oleh 512 bit dalam kelompok dan menjadi sebuah *message digest* 256-bit.



Gambar 2.2 Satu langkah transformasi pembaharuan status SHA-256

C. Tahapan

Proses untuk menghasilkan *message digest* pada SHA-256 ini meliputi tahapan sebagai berikut:

1. Penambahan bit-bit pengganjal (*m=Message padding*) : Pada tahap pertama, pesan yang berupa *binary* disiapkan dengan angka 1 dan ditambahkan bit-bit pengganjal yakni angka 0 hingga panjang pesan tersebut kongruen dengan 448

modulo 512. Panjang pesan yang asli kemudian ditambahkan sebagai angka biner 64 bit. Setelah itu maka panjang pesan sekarang menjadi kelipatan 512 bit.

2. *Parsing* : Pesan yang sudah dipadding tadi kemudian dibagi menjadi N buah blok 512 bit : $M^{(1)}$, $M^{(2)}$, …, $M^{(N)}$.

3. *Message Expansion* : Masing-masing blok 512-bit tadi lalu dipecah menjadi 16 buat *word* 32-bit : $M_0^{(i)}$, $M_1^{(i)}$, …, $M_{15}^{(i)}$ yang manantinya diperluas menjadi 64 *word* yang diberi label W0, W1, …, W63 dengan aturan tertentu yang sudah ditentukan sebelumnya oleh standar SHA-2.

$$W_t = \begin{cases} M_t^{(i)} & 0 \leq t \leq 15 \\ \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16} & 16 \leq t \leq 63 \end{cases}$$

Dengan fungsi σ_0 dan $\sigma_0$dirumuskan sebagai berikut

$$\sigma_0(x) = ROTR^7(X) \oplus ROTR^{18}(X) \theta SHR^3(X)$$

$$\sigma_1(x) = ROTR^{17}(X) \oplus ROTR^{19}(X) \theta SHR^{10}(X)$$

$ROTR^n(X)$ adalah operasi geser kanan putar melingkar, dengan x adalah sebuah sebuah penjadwalan pesan (w) dan n adalah bilangan bulat ($0 \leq n < w$), yang dapat didefinisikan $ROTR^n(X)$ = ((x >> n) v (x << w – n)) = $ROTL^{w-n}(X)$. Dalam hal ini $SHR^n(X)$ adalah operasi menggeser x sebanyak n posisi ke kanan.

Message Compression : Masing-masing dari 64 *word* yang diberi label W0, W1, …, W63 tadi kemudian diproses dengan algoritma fungsi *hash* SHA-256.

Dalam proses tersebut, inti utama dari algoritma SHA-256 adalah membuat 8 variabel yang diberikan nilai untuk nilai awal dari $H_0^{(0)}$-$H_7^{(0)}$ di awal masing-masing fungsi *hash*. Nilai-nilai awal tersebut adalah sebagai berikut:

Initial Hash Value of SHA-256

$A=H_0^{(0)}$	6a09e667
$B= H_1^{(0)}$	bb67ae85
$C= H_2^{(0)}$	3c6ef372
$D= H_3^{(0)}$	a54ff53a
$E= H_4^{(0)}$	510e527f
$F= H_5^{(0)}$	9b05688c
$G= H_6^{(0)}$	1f83d9ab
$H= H_7^{(0)}$	5be0cd19

4. Algoritma ini melakukan perhitungan sebanyak 64 kali putaran untuk setiap perhitungan blok. Delapan variable yang diberi label A, B, C, …, H tadi nilainya terus berganti selama perputaran sebanyak 64 kali putaran sebagai berikut:

   $T_1 = H + \sum_1(E) + Ch\ (E,F,G)[1] + K_t + W_t$ (1)

   $T_2 = \sum_0(A) = Maj(A,B,C)[1]$ (2)

   $H = G$ (3)

   $G = F$ (4)

   $F = E$ (5)

   $E = D + T_1$ (6)

   $D = C$ (7)

   $C = B$ (8)

   $B = A$ (9)

   $A = T_1 + T_2$ (10)

   Dengan fungsi $\sum_0$, $\sum_1$, Ch, Maj dirumuskan sebagai berikut

$$\text{Ch}\ (X, Y, Z) = (X \,\&\, Y) \oplus (\bar{X} \,\&\, Z)$$

$$\text{Maj}(X,Y,Z) = (X \,\&\, Y) \oplus (X \,\&\, Z) \oplus (\text{Y} \,\&\, \text{Z})$$

$$\sum_0(x) = ROTR^2(X) \oplus ROTR^{13}(X) \oplus ROTR^{22}(X)$$

$$\sum_1(x) = ROTR^6(X) \oplus ROTR^{11}(X) \oplus ROTR^{25}(X)$$

5. Setelah perputaran sebanyak 64 kali tadi, nilai *hash* $H^{(i)}$ kemudian dihitung sebagai berikut:

   $H_0^{(i)} = a + H_0^{(i-1)}$

   $H_1^{(i)} = b + H_1^{(i-1)}$

   $H_2^{(i)} = c + H_2^{(i-1)}$

   $H_3^{(i)} = d + H_3^{(i-1)}$

   $H_4^{(i)} = e + H_4^{(i-1)}$

   $H_5^{(i)} = f + H_5^{(i-1)}$

   $H_6^{(i)} = g + H_6^{(i-1)}$

   $H_7^{(i)} = h + H_7^{(i-1)}$

6. Selanjutnya hasil akhir SHA-256 didapat dari penggabungan delapan variable yang tadi sudah dikomputasi.

   $H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$

BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Kesimpulan yang didapatkan dari penelitian ini yaitu untuk mengkolaborasikan MD5 dan SHA-256 peneliti melakukan modifikasi. Modifikasi dilakukan sebelum *plaintext* dienkripsi menggunakan SHA-256, *plaintext* mendapatkan *padding* dua karakter dimana karakter tersebut didapatkan dari *plaintext* yang dienkripsi menggunakan MD5. Hasil enkripsi MD5 diambil dua karakter pertama dan terakhir ntuk kemudian dijadikan *padding* sebelum proses enkripsi menggunakan SHA-256. Penyandian diimplementasikan pada *password* login pengguna.

Dari hasil pengujian yang telah dilakukan, diperoleh hasil bahwa *chipertext* yang dihasilkan yang dienkripsi menggunakan kolaborasi dari MD5 dan SHA-256 cukup aman untuk digunakan. Sebagaimana dalam pengujian ketahanan terhadap serangan *brute* force menggunakan software penyerang memperoleh hasil yang cukup memuaskan. Keadaan tersebut dikarenakan *chipertext* yang dihasilkan oleh kolaborasi MD5 dan SHA-256 memiliki kombinasi karakter yang beragam, sehingga membutuhkan waktu yang sangat lama untuk dapat dipecahkan. Hasil pengujian *Avalanche effect* menghasilkan nilai *AE* sebesar 71%. Ini menunjukan enkripsi dari kolaborasi MD5 dan SHA-256 memiliki tingkat pengacakan yang bagus sehingga sulit untuk diprediksi.

5.2 Saran

Dalam penelitian ini masih banyak terdapat kekurangan, sebagaimana pada pengujian menggunakan CrackStation, *chipertext* yang berasal dari *password* dengan inputan kombinasi huruf saja dapat dipecahkan. Maka untuk penelitian selanjutnya dapat menambahkan model enkripsi lain untuk menambah kekuatan *password*.

DAFTAR PUSTAKA

Abdullah, Dahlan & Erliana, Cut ita. 2012. Program Studi Teknik Informatika, 2 Jurusan Teknik Industri Fakultas Teknik, Universitas Malikussaleh Reuleut, Aceh Utara, Aceh-Indonesia, *4*(2), 38–45.

Adilah, S. dkk. 2017. *Implementation of Cryptosystem Using Method Algorithm ECC With Function of Hash SHA-256 in Online Ticketing System*. *E-Proceduring of Engineering* 4(3): 4138-4146. ISSN : 2355-9355.

Aminudin. 2015. Cara Efektif Belajar *Framework* Laravel. Lokomedia. Yogyakarta.

Ardiansyah, Doni. 2017. Pengukuran Kualitas Sistem Informasi Event Management Menggunakan Standard ISO 9126-1.*Journal Speed* 9(1): 1-7.

Bahri, Saipul, dkk. 2012. Studi Dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5 (*Message-Digest Algorithm* 5). Jurnal Ilmiah 5(1): 1-15.

Barovih, Guntoro. 2016. Pengembangan Interface Sistem Informasi Penjadwalan Laboratorium STMIK Palcomtech. *Jurnal Eksplora Informatika* 6(1): 44-53.

Deacon, John. 2005. *Model-View-Controller (MVC) Architecture*. Jdl.co.

Divya, K & Kalaiarasi, S. 2013. *A Study On Comparison Of Algorithm For One Time Password System*. *IOSR Journal of Computer Engineering* 9(6): 28-33. e-ISSN : 2278-0661, p-ISSN : 2278-8727.

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

Ichwan, M. dkk. 2016. Implementasi *Keyed-Hash Message Authentication Code* Pada Sistem Keamanan Rumah. *MIND Journal* 1(1): 9-18. ISSN : 2528-0015.

Jogiyanto, HM. 2005. Analisis dan Design. AndiOffset: Yogyakarta.

Khairina, D. 2011. Analisis Keamanan Sistem Login. Jurnal Informatika Mulawarman 6(2): 64-67.

Kromodimoeljo, Sentot. 2009. Teori dan Aplikasi Kriptografi. SPK IT Consulting.

Kumar & Tawiri. 2012. *Effective Implementation and Avalanche Effect of AES*.

International Journal of Security, Privacy and Trust Management (IJSPTM) 1(3/4): 31-35.

Kuncoro, Rudi Banu. 2012. Pembuatan Website Tempat Pariwisata Rumah Dome New Nglepen. *Journal Speed* 4(1): 36-41.

Munir, R. 2004. Pengantar Kriptografi. *Departemen Teknik Informatika Institut Teknologi Bandung*, Issue Bahan Kuliah, p. 12.

Natsir, Mohamad. 2016. Pengembangan *Prototype* Sistem Kriptografi Untuk Enkripsi dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java. Jurnal Sistem Informasi (JSI) 6(2): 87 – 105.

Pinedo, M. L. 2012. *Scheduling Theory, Algoritms, and Systems.* Fourth Edition. London:Spinger Science.

Prasetyo, T. F., & Hikmawan, A. (2015). Analisis Perbandingan Dan Implementasi Sistem Keamanan Data Menggunakan Metode Enkripsi RC4 SHA dan MD5. *Infotech Journal*, 41–46.

Pressman, Roger S. 2001. *Rekayasa Perangkat Lunak : Pendekatan praktis (Buku Satu)*. Yogyakarta : Andi.

Rohman, Abdul. 2014. Mengenal *Framework* "Laravel" (best Frameworks for 2014). Imulti.org.

Roshdy, R. dkk. 2013. *Design And Implementation a New Security Hash Algorithm Based on MD5 and SHA-256. Intertional Journal of Engineering Sciences & Emerging Technologies* 6(1): 29-36. ISSN : 2231-6604.

Sadikin, Rifki. 2012. Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java. Andi: Yogyakarta.

Sanjaya, M. 2017. *Inisialisasi Key Generating Kriptografi AES Pada Pendekatan Protokol SMSSec*. Jurnal INFOTEL 9(1): 18-23. ISSN : 2085-3688; e-ISSN : 2460-0997.

Sklavos, N., & Koufopavlou, O. (2005). *Implementation of the SHA-2 hash family standard using FPGAs. Journal of Supercomputing*, *31*(3), 227–248. https://doi.org/10.1007/s11227-005-0086-5

Spinellis, Diomidis. 2006. *Code Quality: The Open Source perspective*. Pearson Education, Inc.

Syafriadi, M. 2006. Analisis kecepatan dan Keamanan Algoritma Secure Hash Algorithm 256 (SHA-256) Untuk Otentikasi Pesan Teks.

Sugiyono. 2015. *Metode Penelitian Pendidikan (Pendekatan Kuantitatif, Kualitatif, dan R&D).* Cetakan 21. Alfabeta : Bandung.

Susandi, Doni. dan Milana, Lia. 2016. Perancangan dan Pngembangan Aplikasi Penyusunan Jadwal Kerja Dinas Jaga perawat IGD Menggunakan Algoritma TPB. *Infotech Journal* 1(1): 49-54.

Virgian, D., Yudha, S., Agani, N., & Hardjianto, M. (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 B ... BIT VOL 13 No . 1 April 2016 ISSN : 1693-9166 Pengamanan Sistem Me, (April 2017).

Yusfrizal. 2018. Kode Autentikasi Hash Pada Pesan Teks Berbasis Android. Jurnal Eksplora Informatika 8(1): 6-14.