# IMPLEMENTASI ENKRIPSI BASIS DATA DENGAN ALGORITMA MD5 (MESSAGE DIGEST ALGORITHM 5) DAN VIGENERE CIPHER

**Hidayatus Sibyan** [a]
[a]Program Studi Teknik Informatika Universitas Sains Al Qur'an (UNSIQ) Wonosobo
[a]email: hsibyan@fastikom-unsiq.ac.id

**INFO ARTIKEL**

**Riwayat Artikel:**
Diterima : 20 Desember 2016
Disetujui : 27 Desember 2016

**Kata Kunci:**
kriptografi, enkripsi, dekripsi, md5, vigenere cipher

**ABSTRAK**

Basis data telah banyak dimanfaatkan oleh berbagai organisasi/ perusahaan untuk menyimpan dan mengolah data pada organisasi/ perusahaan tersebut. Data/ informasi menjadi target serangan oleh pihak-pihak yang tidak bertanggungjawab sehingga perlu untuk menjaga keamanan dan kerahasiaan data/ informasi. Pada penelitian ini mengimplementasikan pengamanan data dari sisi kandungan yang tersimpan dalam basis data. Teknik pengamanan data yang digunakan dalam penelitian ini adalah teknik kriptografi. Algoritma yang digunakan adalah MD5 yang merupakan algoritma fungsi hash. Algoritma MD5 saat ini banyak digunakan untuk meng-enkripsi data guna mengamankan data pada basis data. Namun saat ini banyak pula aplikasi/tool yang beredar di internet yang digunakan untuk proses men-dekripsi-kan data, sehingga keamanan algoritma MD5 pun menjadi lemah.
Perlu adanya kombinasi algoritma MD5 dengan algoritma yang lain untuk memperkuat keamanan basis data. Kombinasi algoritma MD5 dan vigenere cipher cocok diterapkan pada penerapan enkripsi basis data dikarenakan cukup kuat untuk menjaga keamanan basis data.

***ARTICLE INFO***

***Article History***
*Received : December 20, 2016*
*Accepted : December 27, 2016*

***Key Words :***
*cryptography, encryption, decryption, md5, vigenere cipher*

***ABSTRACT***

*The database has been used by various organizations / companies to store and process data in organizations / companies. Data / information become the target of attacks by parties who are not responsible so it is necessary to maintain the security and confidentiality of data / information. In this study, implement secure data from the content stored in the database. Data security techniques used in this study is a cryptographic technique. The algorithm used is the MD5 hash function is an algorithm. MD5 algorithm currently used to encrypt the data in order to secure the data in the database. But now many applications / tools that circulated on the Internet that is used for process decrypts the data, so security becomes weak MD5 algorithm. It needs a combination of the MD5 algorithm with other algorithms to strengthen the security of the database. The combination of the MD5 algorithm and vigenere cipher encryption application is compatible to the database due to be strong enough to maintain the security of the database.*

## 1. PENDAHULUAN

Basis data telah banyak dimanfaatkan oleh berbagai organisasi/ perusahaan untuk menyimpan dan mengolah data pada organisasi/ perusahaan tersebut. Data/ informasi menjadi target serangan oleh pihak-pihak yang tidak bertanggungjawab sehingga perlu untuk menjaga keamanan dan kerahasiaan data/ 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.

Pada penelitin ini akan membahas mengenai teknik pengamanan data dari sisi kandungan data yang tersimpan dalam basis data. Teknik pengamanan data tersebut dapat menggunakan teknik kriptografi. Kriptografi bisa diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. Salah satu algoritma yang bisa digunakan dalam teknik kriptografi adalah algoritam MD5 (Message-Diggest Algorithm 5), yang merupakan fungsi hash (prosedur terdefinisi atau fungsi matematika yang mengubah variabel dari suatu data yang berukuran besar menjadi lebih sederhana. Algoritma MD5 saat ini banyak digunakan meng-enkripsi data guna mengamankan data pada basis data. Namun saat ini banyak pula aplikasi/tool yang beredar di internet yang digunakan untuk proses men-dekripsi-kan data, sehingga keamanan algoritma MD5 pun menjadi lemah. Sehingga perlu adanya teknik pengamanan data yang lebih kuat sehingga keamanan dan kerahasiaan data menjadi tetap terjaga.

Untuk memperkuat enkripsi data, algoritma md5 bisa dikombinasikan dengan algoritma kriptografi yang lain seperti vigenere cipher. Vigenere cipher merupakan sebuah enkripsi dengan melakukan beberapa pergeseran yang direpresentasikan menggunakan satu kata kunci. Kombinasi algoritma MD5 dan vigenere cipher ini bisa menjadi lebih kuat jika dibandingkan hanya menggunakan MD5 saja karena kombinasi algoritma ini akan melakukan proses enkripsi dua kali.

## 2. TINJAUAN TEORI

### 2.1. Kriptografi

Kriptografi berasal dari Bahasa Yunani: “cryptós” artinya rahasia, sedangkan “gráphein” artinya tulisan. Jadi, secara morfologi kriptografi berarti tulisan rahasia. Definisi yang dipakai dalam makalah ini: Kriptografi adalah ilmu dan seni yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta autentifikasi (Munir, 2006). Kata “seni” di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan.

Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (plaintext) menjadi suatu pesan dalam bahasa sandi (ciphertext). Enkripsi merupakan bagian dari kriptografi, dan merupakan hal yang sangat penting supaya keamanan data yang dikirimkan bisa terjaga kerahasiaannya. Enkripsi bisa diartikan dengan chiper atau kode, dimana pesan asli (plaintext) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan.

C = E (M)

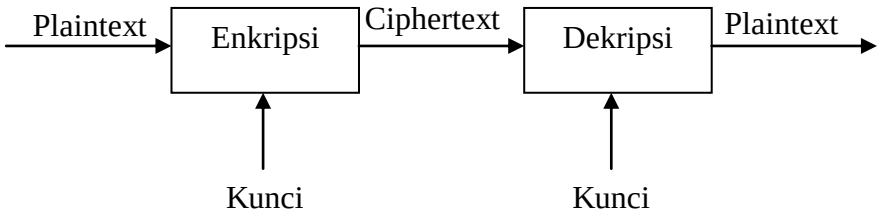
Dimana :

C = pesan dalam bahasa sandi (ciphertext),

E = proses enkripsi dan

M = pesan asli (plaintext).

Gambar 1 berikut menjelaskan baik proses enkripsi maupun proses dekripsi.




Gambar 1. Proses Enkripsi dan dekripsi

Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi (ciphertext) menjadi pesan asli (plaintext) kembali. Dekripsi merupakan proses sebaliknya dari enkripsi yaitu mengembalikan sandi-sandi atau informasi yang telah dilacak ke bentuk file aslinya dengan menggunakan kunci atau kode.

M = D (C)

Dimana :

M = pesan asli (plaintext),

D = proses dekripsi dan

C = pesan dalam bahasa sandi (ciphertext).

Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci. (Pasaribu, 2016)

## 2.2. MD5 (Message Diggest Algorithm 5)

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data serta autentikasi data.

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga.

Terminologi dalam kriptografi diantaranya enkripsi yang merupakan mekanisme untuk merubah plaintext menjadi chipertext. Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Fungsi hash merupakan fungsi yang secara efisien mengubah string masukan dengan panjang berhingga menjadi string keluararn dengan panjang tetap yang disebut nilai hash.

MD5 adalah salah satu dari serangkaian algoritma message-digest yang dirancang oleh Profesor Ronald Rivest dari Massachusetts Institute of Technology (MIT). Ketika kerja analitis menunjukkan bahwa pendahulu MD5 yaitu MD4 mulai tidak aman, maka MD5 kemudian dirancang pada tahun 1991 sebagai pengganti dari MD4. Hash MD5 sepanjang 128-bit (16-byte), yang dikenal juga sebagai intisari pesan, message digest secara tipikal ditampilkan dalam bilangan heksadesimal 32-digit. MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan dan MD5 juga umum digunakan untuk melakukan pengujian integritas data. (Khairina, 2011)

## 2.3. Vigenere Cipher

Vigenere cipher merupakan teknik kriptografi sederhana yang lebih aman. Dikembangkan dari metode caesar cipher, metode ini menggunakan karakter huruf sebagai kunci enkripsi. Vigenere cipher juga merupakan polyalphabetic substition cipher. Karakter huruf yang digunakan pada vigenere cipher yaitu A, B, C, ..., Z dan disamakan dengan angka 0, 1, 2, ..., 25. Proses enkripsi dilakukan dengan menulis kunci secara berulang. Penulisan kunci secara berulang dilakukan hingga setiap karakter pada pesan memiliki pasangan sebuah karakter dari kunci. Selanjutnya karakter pada pesan dienkripsi menggunakan metode caesar cipher dengan nilai kunci yang telah dipasangkan dengan angka.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Plaint Text* | T | H | E | S | K | Y | I | S | F | A | L | L | I | N | G |
| Kunci | E | N | C | O | D | E | E | N | C | O | D | E | E | N | C |
| *Cipher Text* | X | U | G | G | N | C | M | F | H | O | O | P | M | A | I |

Gambar 2. Contoh Enkripsi

Contoh enkripsi pada Gambar 2, karakter pesan "Y" dienkripsi dengan kunci "E" dan menghasilkan cipher text "C". Hasil enkripsi didapatkan dari karakter pesan "Y" bernilai 24 dan karakter kunci "E" yang bernilai 4. Masing- masing nilai karakter ditambahkan 24 + 4 = 28. Karena 28 lebih besar dari pada 26 yang merupakan jumlah karakter yang digunakan, maka 28 dibagi dengan 26. Sisa pembagian tersebut adalah 2 yang merupakan nilai karakter "C". Proses enkripsi dapat dihitung dengan persamaan berikut :

$E_i$= (Pi + Ki) mod 26

dimana Ei, Pi dan Ki merupakan karakter hasil enkripsi, karakter pesan dan karakter kunci. Sedangkan proses dekripsi dapat menggunakan persamaan berikut:

Di = (Ci− Ki) mod 26

dengan Di adalah karakter hasil dekripsi, Ci adalah karakter cipher text atau sandi, Ki adalah karakter kunci. (Prabowo, 2015)

Dari contoh tabel, maka dapat disimpulkan bahwa rumus dari enkripsi dan dekripsi data vigenere chiper adalah (Arjana, 2012):

Enkripsi:

$$Ci = (Pi + Ki) \bmod 26$$

Dekripsi:

$$Pi = (Ci - Ki) \bmod 26; \text{ untuk } Ci >= Ki$$

$$Pi = (Ci + 26 - Ki) \bmod 26; \text{ untuk } Ci < Ki$$

Ci = (Pi + Ki) mod 26
Pi = (Ci – Ki) mod 26; untuk Ci > = Ki
Pi = (Ci+ 26 – Ki) mod 26; untuk Ci < = Ki
Keterangan:
C = Chiphertext
P = Plaintext
K = Kunci

## 3. ANALISIS DAN HASIL

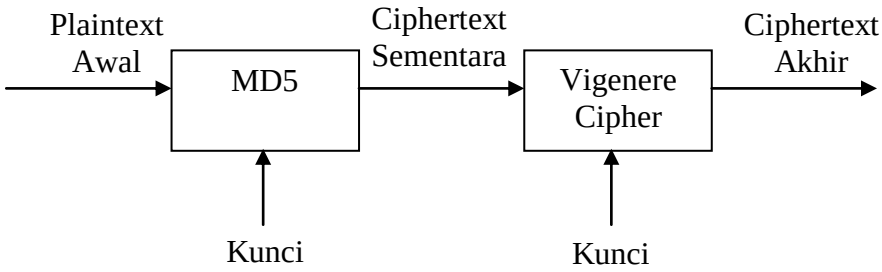
### 3.1. Analisis Sistem

MD5 yang mulai diperkenalkan oleh seorang profesor MIT yang bernama Ronald Rivest pada sekitar tahun 1991 sempat dijadikan sebagai algoritma enkripsi standar dalam berbagai keperluan proses otentikasi. Akan tetapi pada tahun 1996, kelemahan pada MD5 mulai ditemukan. Sejak saat diketahui bahwa MD5 cenderung rentan terhadap serangan collision. Serangan collision adalah suatu peristiwa dimana dua nilai yang berbeda dapat memiliki nilai hash yang sama. Bahkan setelah tahun 2008, telah ditemukan cara untuk memanfaatkan collision ini untuk memalsukan sertifikat SSL yang menjadikan MD5 divonis tidak cocok untuk dipakai sebagai fungsi enkripsi yang membutuhkan ketahanan dari serangan collision (Dewanto, 2011). MD5 juga tidak menggunakan kunci apapun untuk melakukan proses enkripsi, hal tersebut menjadikan proses dekripsinya tidak perlu menemukan kunci yang digunakan. Selain itu saat ini hasil dari enkripsi MD5 semakin mudah di dekripsi dengan banyaknya situs-situs di internet yang menyediakan fasilitas dekripsi algoritma MD5.

Dengan kelemahan yang terdapat pada MD5, maka diperlukan kombinasi antara algoritma MD5 dengan algoritma enkripsi lain, yaitu vigenere cipher. Vigenere cipher merupakan bagian dari algoritma kriptografi klasik yang menggunakan kunci simetrik yang mana kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi. Penggunaan kunci pada algoritma

Vigenere cipher ini menjadikan kriptanalisis membutuhkan waktu untuk menemukan kunci yang digunakan sebelum melakukan dekripsi pada ciphertext.

Untuk proses enkripsi menggunakan algoritma MD5 dan Vigenere cipher akan dilakukan dengan cara mengenkripsi plaintext awal menggunakan MD5 yang akan menghasilkan ciphertext sementara. Selanjutnya dari ciphertext sementara tersebut kemudian akan dienkripsi lagi menggunkan Vigenere cipher untuk menghasilkan ciphertext yang akan digunakan. Proses enkrisi menggunakan kombinasi algoritma MD5 dan Vigenere cipher dapat dilihat pada gambar berikut.




Gambar 3. Proses enkripsi menggunakan algoritma MD5 dan vigenere cipher

### 3.2. Perancangan Database

Untuk database dalam penelitian ini hanya dibuat satu tabel, yaitu tabel users yang digunakan untuk menyimpan data registrasi user dan untuk login user ke aplikasi.

Tabel 1. Struktur Tabel Users

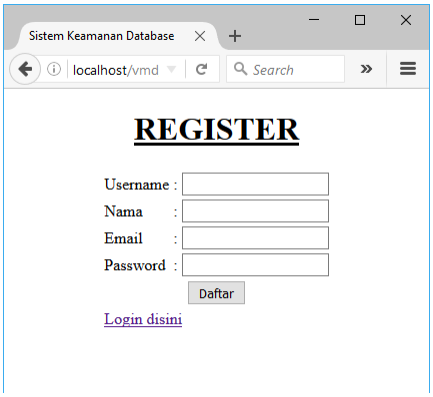
| No. | Field | Tipe Data | Panjang | Keterangan |
|---|---|---|---|---|
| 1. | Username | Varchar | 15 | PK |
| 2. | Nama | Varchar | 30 | |
| 3. | Email | Varchar | 25 | |
| 4. | Password | Varchar | 50 | |

### 3.3. Implementasi

Pada tahap implementasi ini penulis mencoba melakukan percobaan pengamanan data base login dengan menggunakan enkripsi pada data password pengguna sehingga pengguna yang berhak saja yang dapat menggunakan sistem tersebut. Namun sebelum melakukan login, pengguna harus mendaftar/ register terlebih dahulu. Selanjutnya untuk dapat masuk ke dalam halaman utama sistem setiap pengguna harus melakukan login dengan memasukkan Username dan Password yang telah terdaftar sebelumnya. Jika Username dan Password yang dimasukkan sesuai dengan yang ada di dalam database maka akan menuju ke halaman utama. Namun jika Username dan Password tidak terdaftar atau salah maka akan muncul pesan kesalahan dan tidak bisa masuk ke halaman utama sistem. Detail dari halaman register, login dan halaman utama adalah sebagai berikut:

a. Form Register

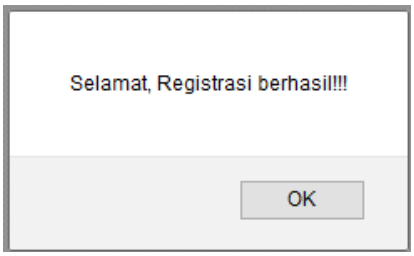
Form Register terlihat pada gambar di bawah ini




Gambar 4. Form Register

Form ini digunakan untuk melakukan pendaftaran pengguna/ user baru. Pengguna/ user tinggal mengisikan data-

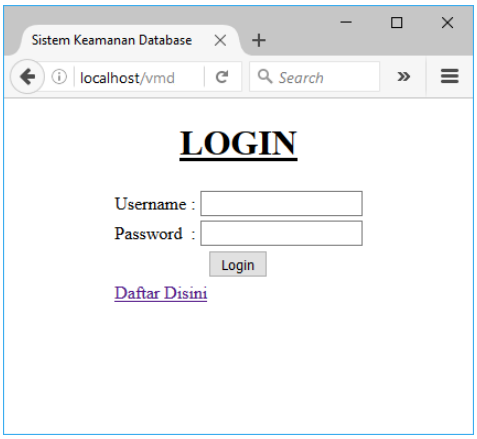
data sesuai dengan isian yang sudah tersedia kemudian klik Daftar. Data password yang diisikan oleh user akan di enkripsi dengan algoritma MD5 dan vigenere cipher kemudian akan tersimpan di dalam database. Jika registrasi berhasil akan muncul pesan pemberitahuan bahwa registrasi telah berhasil dilakukan seperti pada gambar.




Gambar 5. Konfirmasi registrasi berhasil

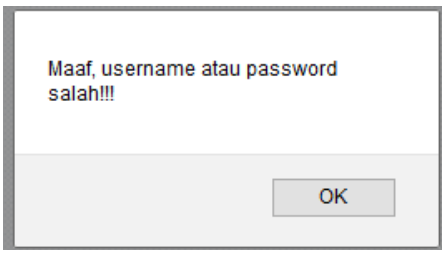
b. Form Login

Form Login terlihat pada gambar di bawah ini




Gambar 6. Form Login

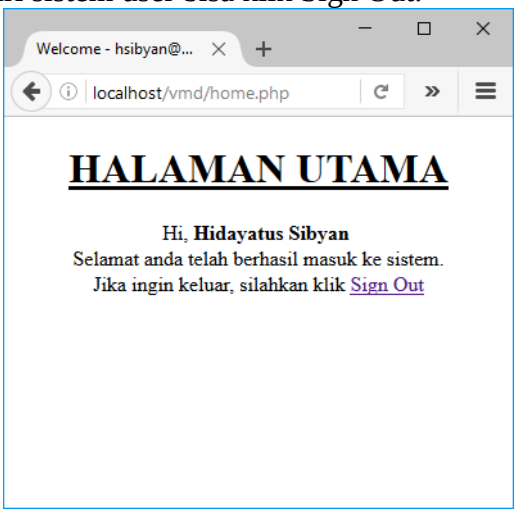
Form login digunakan oleh user untuk masuk ke dalam sistem. Pengguna/ user mengisikan username dan password sesuai dengan data yang telah diisikan pada saat registrasi, kemudian klik Login. Jika username dan password yang dimasukkan sesuai dengan yang ada dalam database, maka akan masuk ke halaman utama sistem. Namun jika username dan password tidak sesuai, akan muncul pesan peringatan seperti pada gambar berikut.




Gambar 7. Konfirmasi username/ password salah

c. Halaman Utama

Halaman utama akan terbuka jika user mengisikan username dan password secara benar sesuai dengan data yang telah dimasukkan saat registrasi. Untuk keluar dari sistem user bisa klik Sign Out.




Gambar 8. Halaman Utama

### 3.4. Pengujian

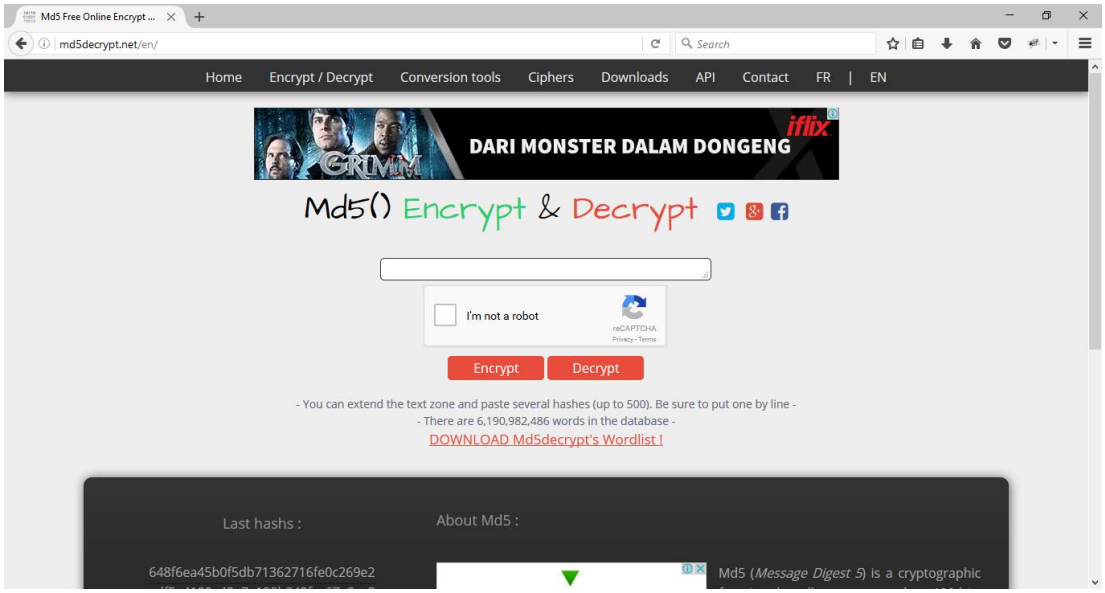
a. Pengujian Enkripsi Algoritma MD5

Pada tahapan ini akan dilakukan pengujian terhadap enkripsi algoritma MD5. Password yang telah dimasukkan oleh user saat registrasi telah tersimpan di dalam database dengan enkripsi MD5 seperti terlihat pada gambar di bawah ini.

| username | nama | email | password |
|---|---|---|---|
| hsibyan | Hidayatus Sibyan | hsibyan@gmail.com | 803d629fa0a51f04256aa561a8e6cdd9 |

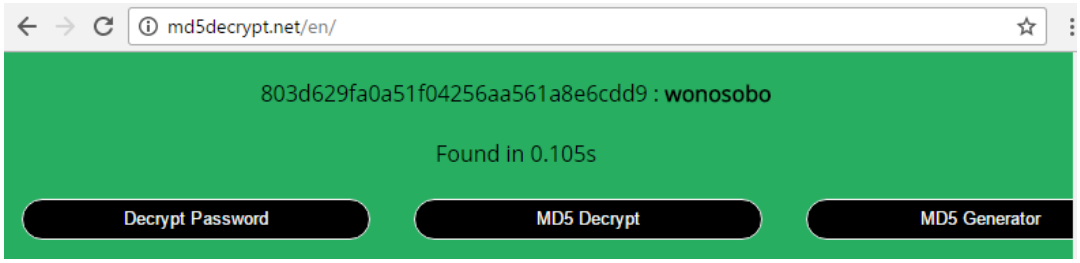
Gambar 9. Data yang tersimpan dalam database dengan algoritma MD5

Saat ini banyak tool yang beredar di internet untuk proses dekripsi algoritma MD5 ini, diantaranya sebuah website yang beralamat di http://md5decrypt.net. Selanjutnya akan dilakukan pengujian terhadap password yang telah tersimpan di dalam database dengan menggunakan algoritma MD5.




Gambar 10. Tampilan http://md5decrypt.net

Setelah mengakses alamat http://md5decrypt.net kemudian kita isikan hasil enkripsi MD5, yaitu: **803d629fa0a51f04256aa561a8e6cdd9** ke dalam form yang tersedia kemudian klik Decrypt untuk melakukan proses dekripsi algoritma MD5.




Gambar 11. Hasil proses dekripsi melalui website di internet

Setelah dilakukan proses dekripsi terhadap algoritma MD5, terlihat hasil seperti pada gambar di atas yaitu **803d629fa0a51f04256aa561a8e6cdd9: wonosobo.** Berarti proses dekripsi algoritma MD5 yang dilakukan oleh website tersebut berhasil dilakukan. Dengan demikian password telah bisa diketahui hanya dengan melakukan proses dekripsi melalui website yang banyak tersedia di internet.

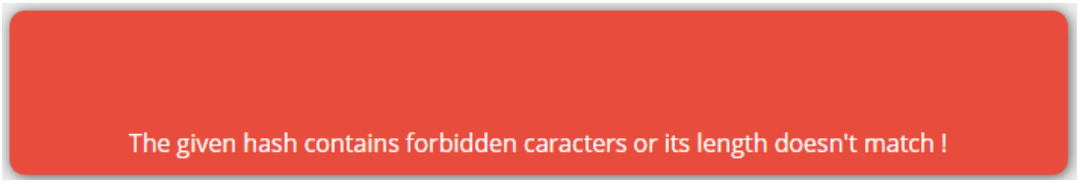
b. Pengujian Enkripsi Algoritma MD5 dan Vigenere Cipher

Untuk pengujian selanjutnya adalah pengujian terhadap sistem dengan menggunakan kombinasi algoritma enkripsi MD5 dan vigenere cipher.

| username | nama | email | password |
|---|---|---|---|
| hsibyan | Hidayatus Sibyan | hsibyan@gmail.com | O00DN09WAGAM9FQ495NIAL68APM6TDK9 |

Gambar 12. Data yang tersimpan dalam database dengan algoritma MD5 dan vigenere cipher

Password yang telah ter enkripsi kemudian dilakukan proses dekripsi di dalam website http://md5decrypt.net, hasil proses dekripsi terlihat pada gambar berikut.




Gambar 13. Hasil dekripsi algoritma MD5 dan vigenere cipher di internet

Hasil dekripsi menunjukkan terjadi error sehingga tidak bisa dilakukan proses dekripsi terhadap teks/ password yang dimasukkan.

Hal ini dapat disimpulkan bahwa kombinasi algoritma MD5 dan vigenere cipher tidak bisa dilakukan proses dekripsi menggunkan tool/ website yang ada di internet, sehingga keamanan data menjadi lebih kuat jika dibandingkan dengan hanya menggunakan algoritma MD5 saja.

## 4. PENUTUP

### 4.1. Kesimpulan

Dari hasil penelitian yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

a. Enkripsi database pada sebuat sistem/ program dapat membantu keamanan terhadap data dalam database.
b. Kombinasi algoritma MD5 dan vigenere cipher cocok diterapkan pada penerapan enkripsi basis data dikarenakan cukup kuat untuk menjaga keamanan basis data.

### 4.2. Saran

a. Penerapan algoritma MD5 dan vigenere cipher ini dapat dijadikan sebagai referensi untuk mengembangkan sebuah aplikasi/ sistem basis data.
b. Teknik enkripsi basis data dapat dikembangkan menggunakan algoritma kriptografi yang lain untuk membentuk keamanan data yang lebih baik lagi.

## 5. DAFTAR PUSTAKA

Arjana, Putu H.; dkk. 2012. Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper. Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012), Yogyakarta.

Khairina, Dyna Marisa. 2011. Analisis Keamanan Sistem Login. Jurnal Informatika Mulawarman Vol. 6 No. 2.

Munir, Rinaldi. (2006). Diktat Kuliah IF5054 Kriptografi. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, ITB.

Pasaribu, Johni S. 2016. Penerapan Algoritma Hill Chiper Dalam Pengamanan Data Dengan Teknik Enkripsi dan Dekripsi. Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016), Bandung.

Prabowo, Hendro, Eko. 2015. Enkripsi Teks Menggunakan Metode Vigenere Cipher Dengan Pembentukan Kunci Tiga Tahap. Jurusan Teknik Elektro Fakultas Teknik Universitas Negeri Semarang.

S, Dewantono, "Kelemahan Fungsi Massage Digest 5," Makalah IF2091, 2011.