SIGMA
Jurnal Teknologi Pelita Bangsa

Vol. 11 No. 3 September 2020 ISSN: 2407-3903

Diterima, 16 Juli 2020 | Direvisi, 28 Agustus 2020 | Dipublikasikan, 28 September 2020

KELEMAHAN METODE ENKRIPSI *MESSAGE DIGEST 5* TERHADAP KRIPTANALISIS MODERN

Asep Muhidin[1], Rudi Alfianto[2]

Program Studi Teknik Informatika Fakultas TeknikUniversitas Pelita Bangsa
[1]asep.muhidin@pelitabangsa.ac.id

Abstraksi

Penelitian ini mengkaji tentang teknik enkripsi dengan menggunakan metode *MD5*. Begitu populernya metode ini sehingga setelah beberapa dekade rilisnya metode ini masih sering digunakan, meski setahun sejak diumumkan rilisnya sudah dipublikasikan tentang potensi kelemahan dari metode ini. Pembahasan tentang kelemahan pada metode *MD5* dalam penelitian ini adalah merujuk pada penelitian yang dilakukan oleh Dobertin H. Tentang potensi kesalahan pada metode ini. Penelitian ini menguji kelemahan teknik enkripsi dengan menggunakan metode *MD5* yang sudah dipublikasikan oleh penelitian lain sebelumnya. Hasil dan kesimpulan pada penelitian ini untuk bisa dijadikan referensi bagi pembuat sistem informasi untuk memperhatikan segi keamanan data dan melakuan modifikasi sedemikian rupa untuk mencegah potensi kelemahan yang dibahas pada penelitian ini.

Kata kunci : Kriptografi, Keamanan data, *MD5*, Potensi kelemahan *MD5*.

Abstract

This study examines encryption techniques using the MD5 method. So popular is this method that after several decades of its release this method is still often used, even though a year since its release was announced about the potential weaknesses of this method. The discussion of weaknesses in the MD5 method in this study is referring to research conducted by Dobertin H. About the potential errors in this method. This study examines the weakness of encryption techniques using the MD5 method that has been published by other studies before. The results and conclusions in this study can be used as a reference for information system makers to pay attention to the aspect of data security and make modifications in such a way as to prevent the potential weaknesses discussed in this study.

Keywords: *Cryptography, Data security, MD5, MD5 potential weaknesses*

1. Pendahuluan

Tingkat pencurian data di Indonesia semakin mengkhawatirkan. Sebanyak dua pertiga dari bisnis menengah/besar mengalami setidaknya satu penyusupan atau serangan siber dalam 12 bulan terakhir. Ini berdasarkan laporan yang dirilis Grant Thornton bertajuk "*Cyber Security: The Board Report* 2019" yang dikutip pada Selasa (27/8/2019). Sebanyak 73 persen dari 500 perusahaan yang disurvei melaporkan kerugian hingga 25 persen dari pendapatan. [1] Salah satu data yang paling sering diretas adalah akun user, dimana dalam tabel tersebut memuat informasi hak akses yang bisa digunakan untuk masuk kedalam sistem. Dengan memiliki hak ases terhadap sistem pelaku bisa dengan mudah mengambil atau memanipulasi informasi yang ada pada akun tersebut. Oleh karena itu diperlukan enkripsi lebih dalam keamanan data tersebut. Kriprtografi adalah ilmu yang mempelajari teknik-teknik atematikayang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. [2] Dengan kriptografi, informasi-informasi penting bisa di sembunyikan dengan menggunakan kata sandi. Tanpa kata sandi pesan yang telah di enkripsi memiliki bentuk yang sulit diterjemahkan.

Salah satu untuk metode enkripsi adalah message *digest*. Ada beberapa versi dari message *digest* yaitu, *MD2, MD3, MD4* dan

MD5. Versi terakhir yaitu *MD5* memiliki tingkat keamanan lebih tinggi daripada pendahulunya. Konsep *MD5* bekerja dengan memanipulasi data *password* yang disimpan tidak sama dengan data *password* yang diisikan. Data *password* sudah dalam bentuk pesan ringkas (*message digest*) hasil pengolahan fungsi *hash* sehingga data *password* hanya diketahui oleh pembuat itu sendiri. Waktu yang dibutuhkan untuk pencarian kunci dalam *MD5* cukup lama. [3]

Sejak versi terakhirnya rilis, tepatnya 27 tahun yang lalu. Tidak banyak yang berubah dari *MD5*. Meski begitu *MD5* masih cukup populer digunakan sebagai metode enkripsi sebuah data. Serangan *cyber* sekarang tentu tidak sama lagi dengan 27 tahun yang lalu. Hal ini membuat metode enkripsi ini dilaporkan memiliki beberapa kelemahan. Perubahan setiap input yang dilakukan selalu memiliki panjang *MD5* yang sama. Hal ini memungkinkan jika banyak karakter yang dinputkan memiliki *MD5* yang sama karena keterbatasannya hanya 32 bit.

Berdasarkan uraian diatas penelitian akan membahas teknik enkripsi dengan menggunakan metode *MD5*

dan melakukan analisa dan simulasi kelemahan dari *MD5* dan melakukan solusi pencegahan.

2. Landasan Pemikiran

Pada ini akan dibahas beberapa penelitian terdahulu yang berkaitan dengan metode *MD5* yang menjadirujukan dalam penelitian ini diantaranya :

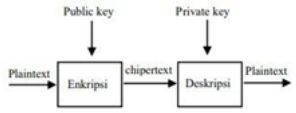
1. Penerapan Algortima *Brute Forced* Pada Penebakan *MD5*.
   Pada penelitian ini menggunakan metode *brute forced* dengan melakukan kombinasi karakter yang mungkin bisa dijadikan *password* lalu mengubahnya menjadi nilai *MD5*. Teknik ini menyediakan kamus *MD5* dari berbagai kombinasi karakter untuk bisa mendeksripsikan nilai pada *MD5*. [4]
2. *Collisions for Hash Functions MD4, MD5 Haval-128 and RIPEMD*
   Teknik ini melanjutkan penelitian dari Dobertin. H. Yang merinci potensi kesalahan pada *MD5* dengan konversi kompleks bilangan biner sehingga di dapat
   2 string yang memiliki nilai *MD5* yang sama. Pada penelitian ini wang xia yan dan timnya melakukan
   percoban merubah 2 string berbeda kedalam bentuk hexadesimal, setelah itu dikonversika menjadi biner lalu di ubah nilainya menjadi *MD5*. Pada penelitian ini menunjukan perbedaan nilai *MD5* dari karakter yang langsung diubah menjadi *MD5*, dengan karakter yang diubah menjadi heksadesimal terlebih dahulu. Dengan perbedaan ini kesalahan fatal berpotensi terjadi pada algoritma ini. Jika tanpa dilakukan modifikasi. [5].
3. Studi dan Implementasi Pengamanan Basis Data Menggunakan Metode *MD5*.
   Mengimplementasikan algoritma *MD5* pada sebuah program sistem informasi berbasis *web* dengan bahasa *PHP* dan *MySQL* sebagai basis data. Untuk menguji hasil data yang sudah di *MD5*-kan. Untuk mengetahui komplektifitas keamanan data. Hasil *checksum MD5* menunjukan nilai berbeda dengan *input*an yang dimasukan. Penggunaan bilangan *hexadesimal* dalam hasil akhir pada *MD5* membuat sulit untuk di deskripsikan. [6].
4. Sistem Bilangan (*Numbering System*)
   Suatu sistem bilangan, senantiasa mempunyai *Base* (*radix*), *absolute* digit dan *positional (place) value*.Suatu sistem komputer mengenal beberapa sistem bilangan, seperti :
   a. Sistem Bilangan Desimal (*Decimal Numbering System*).
   b. Sistem Bilangan *Biner* (*Binary Numbering System*).
   c. Sistem Bilangan *Octal* (*Octenary Numbering System)*.
   d. Sistem Bilangan *Hexadesimal* (*Hexadenary Numbering System*)
5. Kriptografi
   Kriptografi adalah seni atau ilmu untuk menyembunyikan isi pesan yang disandikan/ dienkripsi sedemikian rupa sehingga tidak diketahui apa isi pesan tersebut. [2]
   Dengan menggunakan algoritma matematika. Isi pesan atau informasi di acak menjadi bentuk yang sulit ditebak maksudnya. Namun akan sangat mudah di akses jika di ketahui kode aksesnya.
   Seni kriptografi itu sendiri berawal dari Julius Caesar sejak zaman Romawi Kuno. Teknik ini dijuluki Caesar, *cipher* untuk mengirim pesan secara rahasia meskipun teknik yang digunakannya sangat tidak memadai untuk ukuran kini. Casanova menggunakan pengetahuan mengenai kriptografi untuk mengelabui Madame d'Urfe (ia mengatakan kepada Madame d'Urfe bahwa sesosok jin memberi tahu kunci rahasia Madame d'Urfe kepadanya, padahal ia berhasil memecahkan kunci rahasia berdasarkan pengetahuannya mengenai kriptografi), sehingga ia mampu mengontrol kehidupan Madame d'Urfe secara total.[6]
   Kriptografi mempunyai 2 bagian yang penting yaitu deskripsi dan enkripsi. Enkripsi ialah proses penyadian pesan asli hingga tidak dapat di artikan maksud pesannya.Sedangkan deskripsi ialah merubah pesan yang sudah di sandi-kan menjadi pesan asli.

Gambar 1. Alur Kriptograf

Pada gambar 2.1 dapat dilihat bahwa masukan plain-text akan masuk ke dalam blok enkripsi dan keluarannya berupa chipertext kemudian chipertext akan masuk ke blok deskripsi dan keluarannya menjadi plain-text.

Ada dua model algoritma yang menggunakan kata kunci yaitu, Kunci simetrik yaitu enkripsi yang biasa menggunakan kunci yang sama untuk enkripsi dan deskripsi. Dalam menggunakan metode ini perlu persetujuan antara pembuat pesan dan tujuan pesan.

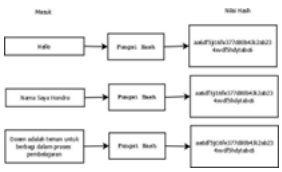
Kunci asimetrik yaitu yang menggunakan kunci yang berbeda antara enkripsi dan deskripsi. Enkripsi berbentuk publik sehingga bisa disebar-luaskan karena kunci untuk deskripsi berbeda dengan enkripsi. Seperti contohnya tanda tangan digital adalah sebuah public key untuk memverifikasi data yang bisa diketahui publik. Sedangkan untuk koneksi yang lebih privasi menggunakan password atau kode akses.



Gambar 2. Kunci Asimetrik

6. Fungsi Hash Dalam Algoritma Kriptografi Fungsi Hash adalah fungsi yang menerima masukan string yang panjangnya sembarang selanjutnya mentransformasikannya menjadi string keluaran yang panjangnya tetap (fixed) yang biasanya berukuran jauh lebih kecil daripada ukuran string semula. [7]
   1. Menyimpan Password.
   2. Sebagai Message Integrity.
   3. Sebagai Message Fingerprint.

Gambar 3. Alur Data dengan Fungsi Hash

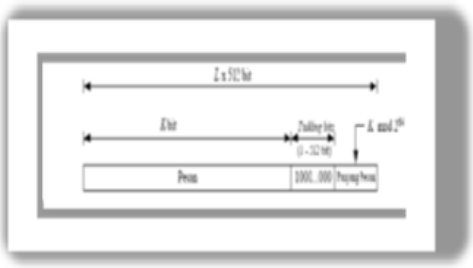


Gambar 4. Hasil Input dan Output dengan Hash

7. Message *Digest Algorithm 5*
   MD5 dikembangkan dari MD, MD2, MD3 dan MD4. MD5 pesan mencerna algoritma, yang dikembangkan oleh Ron Rivest, menerima masukan pesan berbagai panjang dan menghasilkan kode hash 128-bit. Ini telah menjadi salah satu algoritma hash yang paling banyak digunakan. Algoritma ini pada dasarnya dirancang untuk tujuan keamanan yang tinggi di mana pesan yang besar harus "kompresi" dengan cara yang aman sebelum ditandatangani dengan kunci pribadi . Algoritma MD5 digunakan untuk mengimplementasikan integritas pesan yang menghasilkan message digest dari ukuran 128 bit.

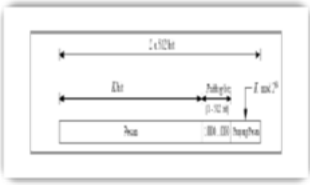
   Dalam implementasi algoritma MD5 menggunakan algoritma 128 bit sebagai unsur dasar dan membuat aplikasi untuk 640 pesan bit sehingga mencipakan kemanan yang tinggi untuk transfer data dalam jaringan mobile. Algoritma ini dapat digunakan dalam mengirim pesan untuk jaringan 3G, 4G, dapat digunakan untuk mengirim file JPG, MPEG, Docx, PDF. Ini adalah fungsi matematika yang memproses informasi untuk membuat pesan yang berbeda dan unik. Keuntungan lain adalah bahwa pesan yang dibuat jauh lebih pendek dari dokumen aslinya. Memproses pesan dan menghasilkan 128-bit message digest [8].

8. Sistem Kerja Message Digest 5 (MD5)
   Setiap pesan yang akan di enkripsi, terlebih dahulu dicari berapa banyak bit yang terdapat pada pesan. Kita anggap sebanyak b bit. Di sini b adalah bit non negatif integer, b bisa saja nol dan tidak harus selalu kelipatan delapan. Langkah kerja MD5 adalah sebagai berikut :
   1. Penambahan bit pengganjal Proses pertama yang dilakukan adalah menambahkan pesan dengan sejumlah bit pengganjal sedemikian sehinggapanjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512



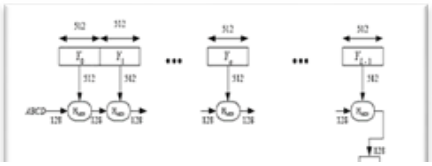
Gambar 5. Alur Kerja Bit Pengganjal

   2. Penambahan nilai panjang pesan semula proses berikutnya adalah pesan ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula. Apabila panjang pesan lebih besar dari 2 64 maka yang diambil adalah panjangnya dalam modulo 264. Dengan kata lain, jika pada awalnya panjang pesan sama dengan K bit, maka 64 bit yang ditambahkan menyatakan K modulo 264. Sehingga setelah proses kedua ini selesai dilakukan maka panjang pesan sekarang adalah 512 bit



Gambar 6. Alur Kerja Penambahan dan Pengganjalan MD5

3. Inisialisasi penyangga MD5 Pada algoritma MD5 dibutuhkan empat buah penyangga atau buffer, secara berurut keempat nama penyangga diberi nama A, B, C dan D. Masingmasing penyangga memiliki panjang 32 bit. Total panjang penyangga adalah 4 ´ 32 = 128 bit.



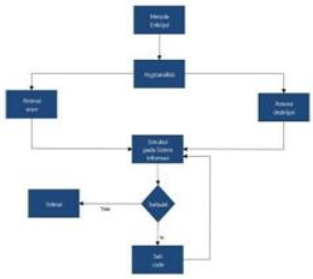
Gambar 7. Inisialisasi Penyangga *MD5*

A = 32 bitB = 32 bitC = 32 bitD = 32 bit
Total = 128 bit
Keempat penyangga ini menampung hasil antara dan hasil akhir. Setiap penyangga diinisialisasidengan nilainilai (dalam notasi Hexadesimal) sebagai berikut:
A = 01234567 B = 89ABCDEFC = FEDCBA89D = 76543210

3. Methode Penelitian

Enkripsi adalah teknik mengacak pesan agar pesan asli hanya diketahui oleh orang yang dituju. Sedangkan kryptanalisis adalah teknik yang digunakan untuk menganalisa kemampuan dari metode enkripsi yang digunakan. Tujuan dari kryptanalisis adalah :

1. Mencari kemungkinan erorr. Dengan mengetahui variabel ini memungkinkan developer untuk mempertimbangkan kelayakan dari metode enkripsi yang digunakan. Sehingga saat diterapkan dalam sistem berjalan, metode enkripsi tidak mengganggu arus data dan hasil input output.
2. Mencari kemungkinan di deskripsikan. Bagian ini memungkinkan developer proram sistem informasi untuk melakukan modifikasi terhadap sistem informasi, agar kerahasiaan data yang di enkripsi lebih terjamin. Setelah kedua variabel itu diketahui, dilanjutkan ketahap analisa hasil dengan mensimulasikan hasil kedua variable tersebut ke sistem informasi untuk diketahui dampak yang terjadi. Jika digambarkan alur tahapannya seperti berikut:



Gambar 8. Kerangka Berpikir

Adapun yang menjadi kelemahan metode ini dalam prakteknya pada sistem informasi dan serangan digital modern sebagai berikut:

1. Bukan enkripsi sesungguhnya
   MD5 bukanlah algoritma enkripsi. Enkripsi mengubah *plain-text* menjadi *ciphertext* yang ukurannya berbanding lurus dengan ukuran *file* aslinya. Semakin panjang *plain- text* maka hasil enkripsinya juga semakin panjang. Hasil enkripsi bisa dikembalikan ke *plain-text* semula dengan proses dekripsi. Jadi enkripsi adalah fungsi dua arah dan *reversible*. Selain itu dalam enkripsi dibutuhkan kunci, tanpa kunci itu namanya bukan enkripsi, melainkan hanya *encoding*/*decoding*.
   Berbeda dengan enkripsi, fungsi *hash* tidak butuh kunci dan sifatnya hanya satu arah, yaitu dari teks masukan menjadi nilai *hash* yang panjangnya selalu sama. Setelah menjadi nilai *hash*, tidak ada fungsi yang bisa mengembalikan nilai *hash* itu menjadi teks semula.
2. Tabrakan (*Collision*)
   Collision dalam bahasa Indonesia artinya tubrukan atau bisa juga disebut tabrakan. Sedangkan *MD5*
   adalah suatu fungsi *hash* kriptografik yang digunakan secara luas dengan *hash value* 128-bit.
   collision MD5 disini adalah suatu keadaan fatal yang mengakibatkan *MD5* tidak dapat membedakan integritas 2 atau lebih *file* yang berbeda. Hal ini ke berkaitan erat dengan fungsi algoritma ini yang banyak digunakan sebagai "*fingerprint*" suatu *file*. Publikasi tentang kelemahan di *MD5* ini sudah ada dari tahun 2005, ketika itu pertama kali ditulis oleh Xiaoyun Wang dan Hongbo Yu. Mereka membuat algoritma yang dapat digunakan untuk membuat *file* yang memiliki *hash MD5* yang sama, dengan perbedaan yang hanya terletak diantara 128 *byte* di *file* tersebut. [5]
3. Rainbow *Table*
   Tabel pelangi adalah daftar semua kemungkinan permutasi *plain-text* dari kata sandi terenkripsi khusus untuk algoritma *hash* yang diberikan. Setelah penyerang mendapatkan akses ke basis data kata sandi sistem, *cracker* kata sandi membandingkan daftar *hash potensial* tabel *hash* yang telah dikompilasi dengan kata sandi *hash* dalam database. Tabel pelangi

mengaitkan kemungkinan *plain- text* dengan masing-masing *hash,* yang kemudian dapat dieksploitasi oleh penyerang untuk mengakses jaringan sebagai pengguna yang diautentikasi.
Rainbow table membuat *cracking* kata sandi jauh lebih cepat daripada metode sebelumnya, seperti pemaksaan dan serangan kamus . Tergantung pada perangkat lunak tertentu, tabel pelangi dapat digunakan untuk memecahkan kata sandi alfanumerik 14 karakter dalam waktu sekitar 160 detik. Namun pendekatan ini menggunakan banyak *RAM* karena banyaknya data dalam tabel tersebut.
Rainbow table hanya menjadi layak baru-baru ini karena jumlah *RAM* yang *file alfanumerik* standar hampir 4 *gigabytes*(GB). Menambahkan simbol kedalam campuran meningkatkan jumlah memori yang diperlukan, seperti halnya setiap langkah dalam enkripsi.

4. Pembahasan

Pada hasil ini penelitian melakukan pengujian terhadap kekurang enkripsi metode *MD5* yang sudahdijelaskan.

1. Bukan Enkripsi Sesungguhnya Penggunaan MD5 terbatas untuk file yang bentuk aslinya tidak diperlukan lagi. Karena mengadopsi sistem hash sehingga sulit untuk membuat pembaliknya untuk mendapatakkan data asli. Seperti contohnya nilai gaji pokok seseorang. Jangan gunakan MD5 untuk melakukan enkripsi, karena data itu sangat mungkin dibutuhkan data aslinya jika suatu saat ada klaim dari orang itu perihal perhitungan gaji. Akan sangat merepotkan kalau harus mengkonversi MD5 ke data aslinya. Tanpa pengetahuan yang cukup. Karena data yang tersimpan bukanlah data asli yang di inputkan.

Gambar 9. Database Setelah di *MD5*

2. Tabrakan (Coliision) Pada prosesnya MD5 menggunakan konversi nilai inputan standar ke bentuk bilangan biner, lalu melakukan eksekusi berdasarkan penjelasan. Ada satu kejadian dimana nilai biner pada dua string adalah sama maka eksekusi yang dilakukan pada algoritma pada kedua string tersebut adalah sama. Ini menyebabkan jika MD5 digunakan untuk pengamanan password maka keduanya dapat digunakan untuk validasi proses login. Seperti percobaan berikut:

   File 1 :
   4dc968ff0ee35c209572d4777b721587d36f
   File 2 :
   4dc968ff0ee35c209572d4777b721587d36fa7b
   21bdc56b74a3dc0783e7b9518afbfa202a8284b
   f36e8e4b55 b35f427593d849676da
   0d1d55d8360fb5f07fea2

   Dua karakter diatas adalah contoh bilangan berbentuk hexadesimal yang memiliki nilai MD5 yang sama. Untuk pembuktiannya adalah dengan mengubahnya kedalam bentuk bilangan binner yang menjadi.
   File 1
   10011011100100101101000111111110000111011100011010111000010000010010101011100910110101
   00011101110111101101110010000101011000011111010011011011111010011110110010000110111110
   11100010101101011011101001010001111011100000000111100000111110011110111001010100011000
   10101111101111111010001000000000101010000010001010000100101111110011011011101000111001001
   01101010101101100110101111101000010011101011001001111011000010010010110011101101110110
   10000011010001010101010101110110000011011000001111101101011111000001111111111010001
   0
   File 2
   10011011100100101101000111111110000111011100011010111000010000010010101011100910110101
   00011101110111101101110010000101011000011111010011011011111010011110110010000110111110
   11100010101101011011101001010001111011100000000111100000111110011110111001010100011000
   10101111101111111010001000000000101010000010001010000100101111110011011011101000111001001
   01101010101101100110101111101000010011101011001001111011000010010010110011101101110110
   10000011010001110101010101110110000011011000001111101101011111000001111111111010001
   0

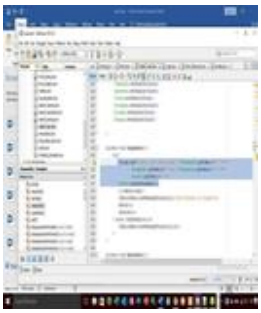
   Setelah itu ubah bentuk biner itu menjadi MD5 disini saya menggunakan konverter online crypti dengan lisensi MIT.

   File 1 93b885adfe0da089cdf634904fd59f71 File 2 93b885adfe0da089cdf634904fd59f71
   Keduanya memiliki nilai hash yang sama

3. Rainbow Table Inilah yang menjadikan MD5 perlu ditingkatkan atau mungkin ditinggalkan. Rainbow Table sejenis brute force yang disusun sedemikian rupa hingga menjadikan

a7b21bdc56b74a3dc0783e7b9518afbfa200a8284bf36e8e4b55b35

semua nilaian yang memungkinkan dijadikan password bisa di deskrip. Dan semuanya disimpan dalam sebuah database dan ditambahkan mesin pencari agar lebih mudah penggunanya. Pengguna hanya perlu memasukan nilai MD5 lalu mesin pencari akan mencari kata yang cocok untuk nilai MD5 yang dimasukkan.



Gambar 10. Sistem dengan Enkripsi *MD5*

Program ini sudah dilengkapi dengan enkripsi *MD5*. Pada bahasa program java proses input pada text
password diubah stringnya menjadi bentuk *MD5*.

1. Lalu kita *input*kan *string* atau kata yang akan di *MD5*. Dengan menjalankan simulasi program ini untuk memastikan keberhasilan dari proses deskripsi dengan *rainbow table*

Gambar 11. *Input* data yang akan di *MD5*

2. Setelah itu cek hasil *MD5* di *database*. Teks yang tersimpan biasanya kombinasi huruf dan angka acak takberaturan sepanjang 32 karakter.

Gambar 12. Database Setelah di *MD5*

3. Deskripsikan string MD5. Disini saya menggunakan situs online dari https://www.MD5online.org/

Gambar 13. Situs MD5online.org

Hasil menunjukan dengan metode *rainbow table* enkripsi *MD5* bisa diterjemahkan.

5. Penutup

Penggunaan MD5 memang cukup bisa menjaga kerahasiaan data dan mudah pemakaiannya. Namun serangan akan semakin canggih. Melalui percobaan. Kita dapati kecenderungan fatal MD5 jika dijadikan sebagai enkripsi. Perlu juga diketahui jenis data yang akan di enskrip apakah nilai aslinya masih diperlukan. Tabrakan MD5 sangat jarang terjadi, tapi bukan berarti aman. Jenis string yang digunakan dalam penelitian memang sangatlah rumit. Sangat tidak mungkin itu digunakan untuk kata sandi. Tapi teknologi saat ini sudah memungkinkan penggunaan gambar dalam melakukan verifikasi. Pada konsepnya dalam autentikasi, penggunaan gambar juga diubah bentuknya kedalam file biner. Tidak ada jaminan gambar yang digunakan bebas dari tabrakan jika di enkripsi dengan MD5. Dan Rainbow Table, sangat sulit dihindari. Kecepatan komputasi modern menyediakan miliaran gabungan kata yang mungkin dijadikan sebagai kata sandi menjadikan MD5 semakin mudah dideskripsikan.

Daftar Pustaka

[1] S. R. D. Setiawan, "Pencurian Data Hingga Bitcoin," kompas, p. all, 27 08 2019.

[2] R. Munir, Kriptografi, Bandung: Informatika, 2019.

[3] Inayatullah, "Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password," kriptografi, no. kriptografi MD5, p. 1, 2016.

[4] K. D. Wulandari, "Penerapan Algoritma Brute Force Pada Penebakan Data Yang Di Enkripsi Dengan Md5," UNniversitas Lampung, Lampung, 2019.

[5] F. D. L. X. Y. H. Wang Xianyan, "Collisions for Hash Functions MD4, MD5 Haval-128 and RIPEMD," CRYPTO, 2008.

[6] S. Kromodimoedjo, Teori dan Aplikasi Kriptografi, SPK IT Consulting, 2016.

[7] M. M. amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," Pseudocode, p. 132, 2016. Rusdianto, "Implementasi Algoritma MD5 Untuk Keamanan Dokumen," Ilmiah Ilmu Komputer, p. 2, 2016