**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

# PENERAPAN ALGORITMA MD5 SEBAGAI PENGAMAN AKUN PADA APLIKASI WEB EMUSRENBANG KOTA BINJAI

**KADRI YUSUF**

Jurusan Teknik Komputer dan Informatika, Politeknik Negeri Medan
Jl. Almamater No. 1 Kampus USU 20155, Medan
E-mail : kadriyusuf@polmed.ac.id

***ABSTRACT***

*Encryption is a technique for hiding passwords into writing that changes from their original form. Encryption aims to increase the security of passwords on an account so that it is not misused by people who are not responsible or who have an interest in seeing data on the application or the web.*

*Emusrenbang application in Binjai City is a website that aims to accommodate community proposals in Binjai so that every community in Binjai city can submit proposals without having to come to the Kelurahan office. Each community has an account to be able to submit proposals based on Local Government Work Plans (OPD). To increase security for each user account is equipped by adding a password. To prevent passwords from being read easily, passwords are encrypted using the MD5 algorithm implemented in PHP. MD5 is an algorithm. It is expected that the emusrenbang web application can cut costs in implementing the emusrenbang from villages, sub-districts, the Regional Representative Council and the Regional Parliament Council (PokD), and can increase public trust with government transparency in carrying out musrenbang in the city of Binjai..*

***Keywords: Cryptography, MD5 Algorithm***

**ABSTRAK**

Enkripsi merupakan teknik dalam menyembunyikan password menjadi tulisan yang berubah dari bentuk aslinya. Enkripsi bertujuan untuk meningkatkan keamanan password dalam sebuah akun agar tidak disalahgunakan oleh orang yang tidak bertanggung jawab atau yang mempunyai kepentingan untuk melihat data sebuah aplikasi atau web.

Aplikasi Emusrenbang Kota Binjai merupakan sebuah web yang bertujuan untuk menampung usulan masyarakat di kota Binjai sehingga setiap masyarakat di kota Binjai dapat memasukkan usulan tanpa harus datang ke kantor Kelurahan. Setiap masyarakat memiliki akun untuk dapat memasukkan usulan berdasarkan Renja OPD (Organisasi Perangkat Daerah). Untuk meningkatkan keamanan untuk masing-masing akun pengguna dilengkapi dengan menambahkan password. Agar password tersebut tidak dapat dibaca dengan mudah maka untuk password dienkripsi menggunakan algoritma MD5 yang diimplementasikan ke dalam bahasa PHP. MD5 merupakan algoritma. Diharapkan dengan adanya aplikasi web emusrenbang ini dapat memangkas biaya dalam menjalankan emusrenbang baik dari kelurahan, kecamatan, OPD dan Pokir DPRD (Dewan Perwakilan Rakyat Daerah), serta dapat meningkatkan kepercayaan masyarakat dengan transparansi pemerintah dalam menjalankan musrenbang di kota Binjai.

Kata kunci: Kriptografi, Algoritma MD5

**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

## 1. PENDAHULUAN

Emusrenbang merupakan singkatan dari Electronic dan Musrenbang. Defenisi

Aplikasi Web Emusrenbang kota Binjai merupakan sebuah aplikasi berbasis web yang bertujuan untuk memudahkan

Aplikasi kriptografi merupakan aplikasi yang paling sering digunakan untuk mengamankan informasi, informasi yang diamankan bisa berupa file video, audio, gambar dan juga teks, pengamanan bisa dilakukan dengan banyak cara dan menggunakan banyak metode dengan tingkat keamanan yang berbeda mulai dari penggunaan kriptografi klasik sampai penggunaan kriptografi modern seperi AES, DES, RSA, Cipher, Permutasi, dan lainnya.

Encryption adalah pekerjaan mengubah teks terang menjadi teks tersandi / suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi / Suatu pesan dibuat seolah tidak bermakna dengan merubahnya menurut prosedur tertentu.Enkripsi menggunakan algoritma tertentu untuk mengacak pesan. Umumnya algoritma enkripsi dapat dibagi menjadi dua kelompok : algoritma untuk private key system dan algoritma untuk public key system. Contoh untuk algoritma yang digunakan di private key system adalah DES dan IDEA, sedangkan contoh algoritma yang digunakan di public key system adalah RSA dan ECC.

Kriptografi merupakan ilmu yang mempelajari tentang pengamanan data atau informasi, dalam kriptografi banyak ditemukan metoda-metoda kriptografi. Namun dengan adanya teknik Brute Force, sebuah enkripsi dapat ditembus keamanan data nya

## 2. METODOLOGI PENELITIAN

### a. Kriptografi

Kata kriptografi berasal dari bahasa yunani yaitu krupto (*hidden* atau *secret*) dan grafh (*writing*) sehingga berarti *secret writing*. Secara istilah kriptografi didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang mempunyai pengertian, dengan cara menyamarkannya (mengacak) menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu.

Secara etimologi kata kriptografi (Cryptography) berasal dari bahasa Yunani, yaitu kryptos yang artinya yang tersembunyi dan graphein yang artinya tulisan (Prayudi, 2005). Awal mula kriptografi dipahami sebagai ilmu tentang menyembunyikan pesan (Sadikin, 2012), tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi (Diffie, 1976).

Secara umum 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.

Di dalam kriptografi memiliki beberapa tujuan, diantaranya :

1. Kerahasiaan
2. Integritas data
3. Autentifikasi
4. Non-repudiasi

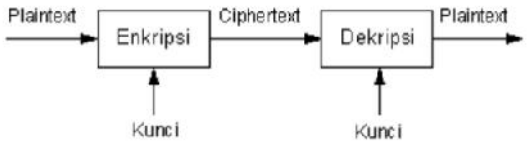
Di dalam kriptografi akan sering ditemukan berbagai istilah atau terminology. Beberapa istilah yang harus diketahui yaitu :

1. Pesan, plaintext, dan cipherteks
2. Pengirim dan penerima
3. Enkripsi dan dekripsi

**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

4. Cipher dan kunci

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah plaintext menjadi ciphertext (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti.




Gambar 1. Proses Enkripsi dan Deskripsi

Dalam kriptografi, MD5 (Message-Digest algortihm 5) ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standart Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah berkas.

Message Digest 5 (MD-5) adalah salah satu penggunaan fungsi hash satu arah yang paling banyak digunakan. MD-5 merupakan fungsi hash kelima yang dirancang oleh Ron Rivest yang didefinisikan pada RFC 1321.

MD-5 merupakan pengembangan dari MD-4 dimana terjadi penambahan satu ronde[1,3,10]. MD-5 memproses teks masukan ke dalam blok-blok bit sebanyak 512 bit, kemudian dibagi ke dalam 32 bit sub blok sebanyak 16 buah. Keluaran dari MD-5 berupa 4 buah blok yang masing-masing 32 bit yang mana akan menjadi 128 bit yang biasa disebut nilai hash[3,10].

Simpul utama MD5 mempunyai blok pesan dengan panjang 512 bit yang masuk ke dalam 4 buah ronde. Hasil keluaran dari MD-5 adalah berupa 128 bit dari byte terendah A dan tertinggi byte D.

**b. Algoritma MD5**

Setiap pesan yang akan dienkripsi, terlebih dahulu dicari berapa banyak bit yang terdapat pada pesan. Diumpamakan sebanyak b bit. Di sini b adalah bit non negatif integer, b bisa saja nol dan tidak harus selalu kelipatan
delapan.

Cara Kerja MD5

Langkah-langkah pembuatan message digest secara garis besar:

1. Penambahan bit-bit pengganjal (padding bits).
2. Penambahan nilai panjang pesan semula.
3. Inisialisasi penyangga (buffer) MD.
4. Pengolahan pesan dalam blok berukuran 512 bit.

1. Penambahan Bit-bit Pengganjal
   Pesan ditambah dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512. Jika panjang pesan 448 bit, maka pesan tersebut ditambah dengan 512 bit menjadi 960 bit. Jadi, panjang bit-bit pengganjal adalah antara 1 sampai 512. Bit-bit pengganjal terdiri dari sebuah bit 1 diikuti dengan sisanya bit 0.
2. Penambahan Nilai Panjang Pesan
   Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula. Jika panjang pesan > 264 maka yang diambil adalah panjangnya dalam modulo 264. Dengan kata lain, jika panjang pesan semula adalah K bit, maka 64 bit yang ditambahkan menyatakan K modulo 264. Setelah ditambah dengan 64 bit, panjang pesan sekarang menjadi kelipatan 512 bit.

**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

3. Inisialisai Penyangga MD
   MD5 membutuhkan 4 buah penyangga (buffer) yang masing - masing panjangnya 32 bit. Total panjang penyangga adalah 4 x 32 = 128 bit. Keempat penyangga ini menampung hasil antara dan hasil akhir. Keempat penyangga ini diberi nama A, B, C, dan D. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut:
   A = 01234567
   B = 89ABCDEF
   C = FEDCBA98
   D = 76543210
4. Pengolahan Pesan dalam Blok Berukuran 512 bit.
   Pesan dibagi menjadi L buah blok yang masing-masing panjangnya 512 bit (Y0 sampai YL – 1). Setiap blok 512-bit diproses bersama dengan penyangga MD menjadi keluaran 128-bit, dan ini disebut proses HMD5.

Inisialisasi MD5

Pada MD-5 terdapat empat buah word 32 bit register yang berguna untuk menginisialisasi message digest pertama kali. Register-register ini diinisialisasikan dengan bilangan hexadesimal.
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 variabel atau variabel rantai.

Proses Pesan di Dalam Blok 16 word

Pada MD-5 juga terdapat 4 (empat) buah fungsi nonlinear yang masing-masing digunakan pada tiap operasinya (satu fungsi untuk satu blok),
yaitu:
F(X,Y,Z) = (X Ù Y) Ú ((Ø X) Ù Z)
G(X,Y,Z) = (X Ù Z) Ú (Y Ù (Ø Z))
H(X,Y,Z) = X Å Y Å Z
I (X,Y,Z) = Y Å (X Ú (Ø Z))
(Å untuk XOR, Ù untuk AND, Ú untuk OR dan Ø untuk NOT).
Pada Gambar 3.2 dapat dilihat satu buah operasi dari MD-5 dengan
operasi yang dipakai sebagai contoh adalah FF(a,b,c,d,Mj,s,ti)
menunjukan a = b + ((a + F(b,c,d) + Mj + ti) <<<>
FF(a,b,c,d,Mj,s,ti) menunjukan a = b + ((a + F(b,c,d) + Mj + ti) <<<>
GG(a,b,c,d,Mj,s,ti) menunjukan a = b + ((a + G(b,c,d) + Mj + ti) <<<>
HH(a,b,c,d,Mj,s,ti) menunjukan a = b + ((a + H(b,c,d) + Mj + ti) <<<>
II(a,b,c,d,Mj,s,ti) menunjukan a = b + ((a + I(b,c,d) + Mj + ti) <<<>

**c. Analisa Permasalahan**

Sebuah akun sangat penting bagi seorang pengguna karena mempunyai data penting yang tidak boleh diketahui oleh orang lain. Untuk itu, perlu penguatan akun dengan melengkapi password dengan sebuah enkripsi yang nantinya password akan berubah sesuai dengan algoritma yang digunakan.
Pada web emusrenbang kota Binjai, yaitu emusrenbang.binjaikota.go.id telah memiliki username dan password untuk masuk ke system tersebut. Untuk masuk ke sistem emusrenbang.binjaikota.go.id membutuhkan username dan password. Algoritma MD5 diletakkan pada kolom password sehingga isi password dapat berubah sesuai dengan alogritma MD5
Contoh :
Seorang user memasukkan username = “pengguna” dan password = 1234. Maka, yang tersimpan password di database bukan lagi 1234, karena telah diubah dengan menggunakan algoritma MD5 menjadi 81dc9bdb52d04dc20036dbd8313ed055.

P-ISSN: 2548-9704
E-ISSN: 2686-0880

## 3. HASIL DAN PEMBAHASAN

Untuk implementasi dan pengujian digunakan sebuah komputer spesifikasi sebagai berikut:

- Processor Intel Core 2 Duo
- memori sebesar 512 MB
- Windows 10

Tampilan web dapat dibuka dengan alamat emusrenbang.binjaikota.go.id

### a. Tampilan Home

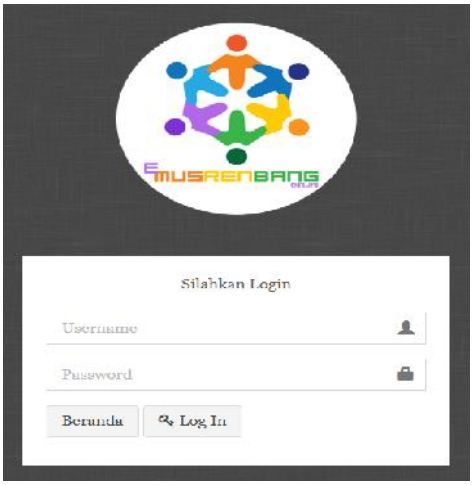
Tampilan Home merupakan tampilan yang pertama kali muncul ketika masuk ke web emusrenbang.binjaikota.go.id.


Gambar 2. Tampilan Depan website Emusrenbang kota Binjai

### b. Tampilan Login

Tampilan login berfungsi untuk memverifikasi pengguna sesuai dengan username dan password. Jika username dan password benar, maka akan masuk ke login menu.

Untuk masuk ke login, klik menu Login




**Gambar 3. Tampilan Login**

Berikut merupakan fungsi merubah tulisan password menjadi tulisan yang telah disandikan menggunakan algoritma MD5

```
function md5_16($string){
  $tmp = md5($string);
  $out='';
  for ($i=0;$i<=30;$i=$i+2){
    $out.=chr(hexdec(substr($tmp,$i,2)));
  }
  return $out;
}
```

### c. Tampilan Administrator

Form ini digunakan untuk menampilkan menu Administrator. Berikut ini tampilan Administrator emusrenbang.binjaikota.go.id


**Gambar 4. Tampilan Administrator**

**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

## 4. KESIMPULAN

Algoritma MD5 dengan fungsi hashnya sangat peka terhadap perubahan pesan, maka algoritma MD5 cocok untuk aplikasi yang menjaga integritas suatu data. Aplikasi algoritma dapat digunakan untuk menjaga keintegritasan data. Dengan aplikasi fungsi hash yang menjadi asas algoritma MD5, perubahan kecil pada data sekalipun dapat terdeteksi. Langkah yang harus ditempuh adalah bangkitkan message digest dari isi arsip menggunakan algoritma MD5. kemudian gabung message digest ke dalam arsip. Verifikasi isi arsip dapat dilakukan secara berkala dengan membandingkan MD isi arsip sekarang dan MD dari arsip asli (MD yang telah disimpan sebelumnya). Jika hasilnya berbeda maka telah terjadi perubahan pada arsip

## 5. SARAN

Adapun beberapa saran dari penulisan penelitian ini adalah :

a. Agar kerahasiaan data tetap terjaga maka sebaiknya kerahasiaan kunci harus tetap dijaga kerahasiaannya, hanya orang yang besangkutan saja yang mengatahuinya.
b. Agar sistem ini dapat berjalan dengan lebih baik lagi dan sesuai dengan harapan, sebaiknya didukung oleh perangkat yang sesuai dengan kebutuhan dari sistem tersebut.

## DAFTAR PUSTAKA

[1].Doni Ariyus. 2005. ***Computer Security***. Penerbit Andi. Yogyakarta

[2].Doni Ariyus. 2005. Kriptografi Keamanan Data dan Komunikasi. Penerbit Graha Ilmu. Yogyakarta.

[3].Munir, Rinaldi., Pengantar Kriptografi, Institut Teknologi Bandung, 2004.