Jurnal Ilmiah Ilmu Komputer, Vol. 2, No. 2, September 2016
Fakultas Ilmu Komputer
Universitas Al Asyariah Mandar

(P) ISSN 2442-451X
(O) ISSN 2503-3832

IMPLEMENTASI ALGORITMA MD5 UNTUK KEAMANAN DOKUMEN

Rusdianto [1], Akhmad Qashlim[2]
Program Studi Sistem Informasi Fakultas Ilmu Komputer
Universitas Al Asyariah Mandar
rusdhy.anthy@gmail.com

ABSTRAK

Keamanan data dan informasi menarik banyak perhatian orang memastikan keaslian data atau dokumen masih terjaga, masalah ini begitu urgen untuk dan menyentuh berbagai bidang termasuk saluran komunikasi yang aman, teknik enkripsi data yang kuat dan dipercaya dibutuhkan untuk menjaga database. Message Digest 5 (MD) adalah Sebuah metode kriptografi yang menggunakan kunci seperti password dalam melakukan proses enkripsinya dan mengunakan kunci yang sama untuk melakukan proses dekripsinya sehingga akan dihasilkan dokumen yang sama dengan dokumen aslinya. Data plaintex yang telah dienkripsi akan menghasilkan sebuah *chipertex* yang tidak dapat dibaca oleh orang lain. *Chipertex* inilah yang akan dikirimkan ke pihak kedua sehingga akan memiliki kerahasiaan yang bisa diandalkan. Data *chipertex* yang dihasilkan akan berubah-ubah sesuai masukan data kunci password yang diberikan. Sistem ini dibuat dengan bahasa pemprokraman *Visual Basic.Net.*

Kata Kunci : Kriptografi, enkripsi, dekripsi, Password, Metode MD5

ABSTRACT

Data and information security interest in many peoples ensure the authenticity of data or documents are still awake, this issue is so urgent to and touching different areas including secure communication channel, strong data encryption technique and is believed needed to maintain the database. Message Digest 5 (MD) is a cryptographic method that uses a key as a password to perform the encryption process and use the same key to perform the decryption process that will produce the same documents as the original document. Plaintex the data that has been encrypted will produce a chipertex that can not be read by others. Chipertex is what will be sent to the second party will thus have a confidentiality unreliable. Data chipertex produced will vary according to input key data supplied password. The system is built with the programming language Visual Basic.Net.

Keyword* : *Criptografi, encripti, dekripsi, Password, Metode MD5

(P) ISSN 2442-451X
(O) ISSN 2503-3832

1. PENDAHULUAN

Pengiriman pesan atau dokumen dalam bentuk dokumen digital melalui internet merupakan pilihan yang efektif dan efisien [1]. Media internet memicu tindakan kejahatan yang semakin mudah dan marak terjadi [2]. Tindakan kejahatan dapat berupa, klaim produk, pemalsuan data dan identitas, merubah informasi pada page website, dan lebih jauh mengenai pencurian data dan informasi [3]. Persoalan ini menjadikan keamanan data dan informasi menerima banyak perhatian utamanya dari organisasi yang mengelola data dalam jumlah yang besar. Banyak kasus kebocoran informasi telah dilaporkan. Di antara kasus tersebut, Media berbasis kertas masih tercatat sebagai utama sumber kebocoran informasi [4], Para pelaku bisnis butuh memastikan keaslian data atau dokumen masih terjaga, masalah yang menantang komunikasi data dan menyentuh berbagai bidang termasuk saluran komunikasi yang aman, teknik enkripsi data yang kuat dan dipercaya untuk menjaga database [5]. Enkripsi bukan solusi ajaib dan enkripsi tidak bisa menyelesaikan semua masalah kemanan, tetapi sedapat mungkin mengurangi banyak risiko keamanan yang dihadapi organisasi. Enkripsi dapat membantu mencegah hilangnya data atau pencurian, serta mencegah penipuan dalam sebuah organisasi [6]. Teknik enkripsi dalam metode kriptografi dapat digunakan untuk menyelesaikan persoalan ini.

Kriptografi dapat menjamin keaslian data. Kriptografi mempunyai tiga aspek keamanan yaitu, kerahasian pesan, keabsahan pengirim, keaslian pesan dan nirpenyangkalan [1]. Kemampuan metode kriptografi dalam mengacak isi data, seperti teks, gambar, audio, video dan sebagainya untuk membuat data tidak terbaca, tersembunyi atau berarti semua jalan melalui transmisi atau penyimpanan *(Encription)* [7].

Salah satu metode kriptografi yang banyak digunakan yakni Algoritma MD5 metode ini dapat digunakan sebagai mekanisme tanda tangan digital [8];[9];[7]. MD5 banyak digunakan dalam beberapa algoritma kriptografi kunci publik dan komunikasi internet pada umumnya sehingga untuk memberikan perlindungan keamanan yang lebih tinggi, aplikasi dari algoritma MD5 diimplementasikan dalam jaringan yang memproduksi 640- bit message digest. Ini akan menjadi algoritma keamanan yang tinggi untuk transfer data dalam jaringan mobile [5]. Arah penelitian ini adalah teknik menyembunyikan informasi dalam dokumen, termasuk karakteristik menggunakan algoritma MD5.

2. LANDASAN TEORI

2.1. *Message Digest Algoritma 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 [5];[7]. 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 [5]. Algoritma MD5 digunakan untuk mengimplementasikan integritas pesan yang menghasilkan message digest dari ukuran 128 bit [8];[9];[7];[5]. 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 [5], dapat digunakan untuk mengirim file JPG, MPEG, [9], Docx, PDF [1]. 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. Algoritma MD5 melibatkan langkah-langkah berikut[8];[9];[7];[5]:

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

2.2. Engkripsi dan Deskripsi

Dokumen yang memiliki tanda tangan digital dimaksudkan untuk memvalidasi darimana data tersebut berasal. Tanda tangan digital dapat dilakukan melalui enkripsi. Algoritma yang biasanya dipakai untuk membuat sebuah tanda tangan digital yaitu *Algoritma Message Digest* 5 (MD5) yang juga salah satu fungsi *hash*.[1].

Enkripsi adalah kontrol kunci yang menerima banyak perhatian dalam organisasi saat. Kebutuhan organisasi untuk mengenkripsi data sensitif harus terpenuhi. Enkripsi dapat membantu mencegah hilangnya atau pencurian data, serta mencegah penipuan dalam sebuah organisasi. Dalam beberapa kasus, enkripsi juga digunakan untuk memenuhi persyaratan peraturan untuk perlindungan data konsumen [6].

Walaupun enkripsi data merupakan metode yang kuat dan dipercaya untuk menjaga database [5] Enkripsi tidak menjadi solusi ajaib dan enkripsi tidak bisa menyelesaikan semua masalah kemanan, tetapi sedapat mungkin mengurangi banyak risiko keamanan yang dihadapi organisasi. Enkripsi dapat membantu mencegah hilangnya data atau pencurian, serta mencegah penipuan dalam sebuah organisasi [6].

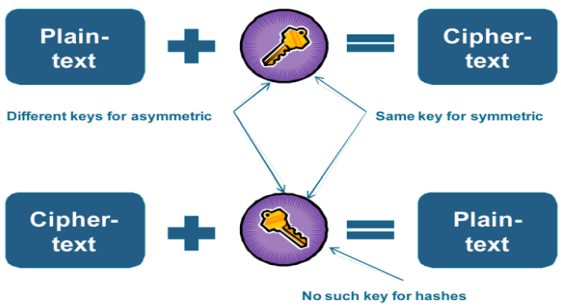
(P) ISSN 2442-451X
(O) ISSN 2503-3832

Algoritma kriptografi secara umum dapat dikelompokkan menjadi dua kategori yang berbeda:

1. kriptografi kunci simetris *(Symmetric key cryptosystems)*, yang menggunakan kedua kunci yang sama untuk mengenkripsi dan mendekripsi komunikasi data
2. kriptografi asimetris *(Asymmetric cryptosystems)*, yang menggunakan dua kunci yang berbeda bukan satu tombol - salah satu kunci untuk mengenkripsi komunikasi dan kunci yang lain untuk mendekripsi komunikasi.

Algoritma simetris adalah bahwa mereka cenderung lebih cepat dari algoritma asimetris. Namun, kelemahan adalah bahwa manajemen kunci dapat lebih sulit. Karena kunci yang sama digunakan untuk mengenkripsi dan mendekripsi data, siapa saja yang memiliki kunci untuk enkripsi dapat menggunakan tombol yang sama untuk mendekripsi salah satu data yang telah dienkripsi. Contoh umum dari algoritma simetris digunakan saat ini termasuk *Triple* DES dan AES (*Advanced Encryption Standard).*

Kriptografi asimetris juga dikenal sebagai kriptografi kunci publik dan bergantung pada penggunaan dua kunci-unik kunci publik dan kunci pribadi. Kunci publik digunakan untuk mengenkripsi data dan tidak dapat digunakan untuk mendekripsi data. Hanya kunci pribadi dapat mendekripsi data. Oleh karena itu, kunci bekerja sebagai pasangan dan sering disebut sebagai pasangan kunci. Kunci publik dapat diberikan kepada siapa saja yang ingin mengenkripsi data, tetapi kunci pribadi harus dijaga kerahasiaannya karena memberikan kemampuan untuk mendekripsi data. algoritma asimetris mengandalkan algoritma yang sangat rumit dan, oleh karena itu, umumnya lebih lambat dari algoritma simetris. Namun, dengan kriptografi asimetris, manajemen dapat lebih mudah untuk mengelola. Karena kunci yang berbeda yang digunakan untuk mengenkripsi dan mendekripsi data, kunci enkripsi dapat diberikan kepada siapa pun tanpa risiko mereka mampu mendekripsi komunikasi.

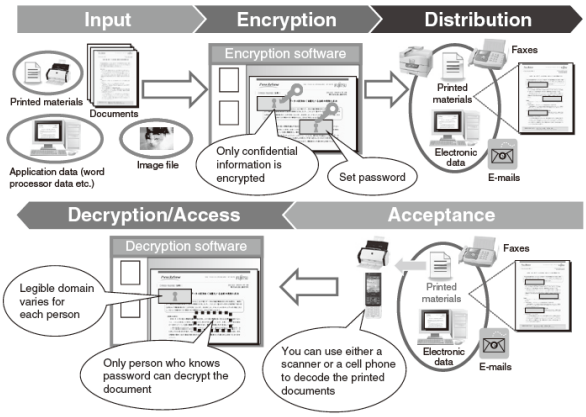


Gambar 2: Enkripsi Algoritma: Asymmetric (kiri) dan Symmetric (kanan) [6]

Pada saat data berada dalam database maka teknik enkripsi akan menjadi pilihan, kemampuan enkripsi ini dirancang dalam sebuah aplikasi sendiri. Pada saat database menerima data maka secara otomatis akan di enkripsi dan disimpan dalam database, selain cara ini data juga dapat di enkripsi pada saat perjalanan melalui lalu lintas jaringan. Semua tergantung pada kebutuhan pengguna solusi tambahan untuk tujuan enkripsi.

Gambar 3 Aplikasi Enkripsi [6]

Akses informasi pengguna perlu menggunakan aplikasi enkripsi *(Software)* hal ini dimaksukan untuk mengkonfirmasi pengguna aplikasi yang resmi atau pihak luar [6]. Aplikasi enkripsi banyak diterapkan pada akses dokumen organisasi untuk menghindari kebocoran informasi. Alur proses enkripsi dan deskripsi dokumen ditunjukkan pada gambar 4.



Gambar 4. Alur proses enkripsi dan deskripsi dokumen [4]

3. METODE PENELITIAN

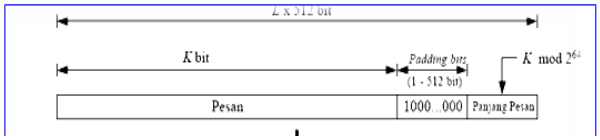
3.1. Implementasi algoritma MD5

Implementasi algoritma MD5 memiliki 5 tahap sebagai berikut:

1. Penambhan bit-bit penjanggal (padding bits).

Proses pertama yang dilakukan adalah menambahkan pesan dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512. Ini berarti setelah menambahkan bit-bit pengganjal, kini panjang pesan adalah 64 bit kurang dari kelipatan 512. Hal yang perlu diingat adalah angka 512 muncul karena algoritma MD5 memproses pesan dalam blok-blok yang berukuran 512.

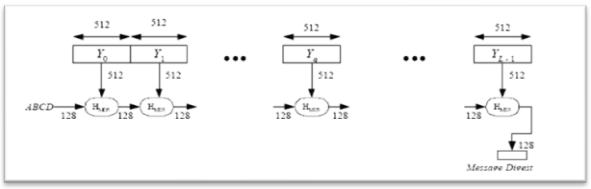
(P) ISSN 2442-451X
(O) ISSN 2503-3832



Gambar 5. Penambahan Bit Pengganjal

2. Penambahan nilai panjang pesan semula.

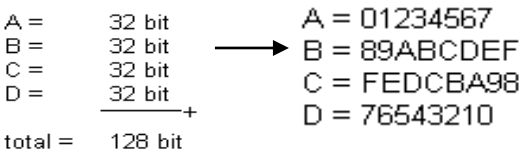
Kemudian proses berikutnya adalah pesan ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula. Apabila panjang pesan lebih besar dari 2_{64} maka yang diambil adalah panjangnya dalam modulo 2_{64}. dengan kata lain, jika pada awalnya panjang pesan sama dengan K bit, maka 64 bit yang ditambahkan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



Gambar 6 Penambahan nilai panjang pesan semula

3. Inisialisasi penyangga (buffer) MD.

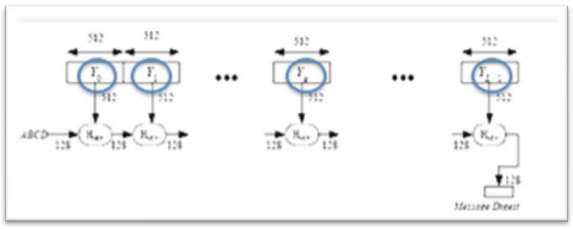
Pada algoritma MD5 dibutuhkan empat buah penyangga atau buffer, secara berurut keempat nama penyangga diberi nama A, B, C dan D. Masing-masing penyangga memiliki panjang 32 bit. Total panjang penyangga adalah 4 ´ 32 = 128 bit. Keempat penyangga ini menampung hasil antara dan hasil akhir Sehingga panjang total 128 bit.



Keempat penyangga diatas menampung hasil antara dan hasil akhir. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi Hexadesimal).

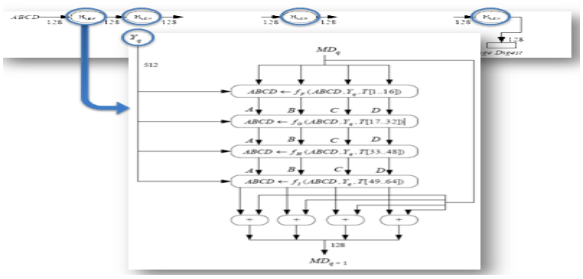
4. Pengolahan pesan dalam blok berukuran 512 bit.

Proses berikutnya adalah pesan dibagi menjadi L buah blok yang masing - masing panjangnya 512 bit (Y0 sampai YL-1). Setelah itu setiap blok 512 bit diproses bersama dengan penyangga MD yang menghasilkan keluaran 128 bit, dan ini disebut H_{MD5}. Berikut ini gambaran dari proses H_{MD5}.



Gambar 7. Pengolahan Pesan Dalam Blok 512 Bit

Gambar diatas menunjukkan bahwa proses H_{MD5} terdiri dari 4 buah putaran, dan masing-masing putaran melakukan opersi dasar MD5 sebanyak 16 kali. Dimana disetiap operasi dasar memakai sebuah elemen T. Sehingga setiap putaran memakai 16 elemen tabel T.



Gambar 8. Proses H_{MD5}

Operasi dasar MD5 yang diperlihatkan gambar 5.6 dapat dituliskan dengan persamaan berikut ini :

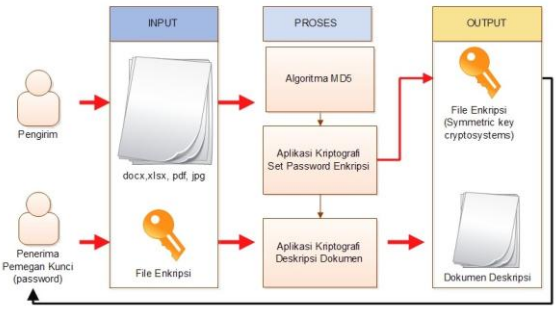
$$a \leftarrow b + \mathrm{CLS}_s(a + g(b, c, d) + X[k] + T[i])$$

Keterangan:
a, b, c, d : Empat buah peubah Penyangga 32-Bit (Berisi Nilai Penyangga A,B,C,D)
g : Salah satu fungsi F,G,H,I
CLSs : Circular left shift sebanyak s Bit
X[K] : Kelompok 32-Bit ke-K dari blok 512 bit message ke-q. Nilai k : 0 sampai 15
T[i] : Elemen tabel T ke-i (32-bit)
+ : Operasi penjumlahan module

3.2. Rncangan Aplikasi Kriptografi MD5

Aplikasi Kriptografi dibangun menggunakan bahasa pemrograman visual basic.net. Keragka sistem Enkripsi yang akan dirancang dalam penelitian ini dapat dilihat pada gambar 9.

(P) ISSN 2442-451X
(O) ISSN 2503-3832



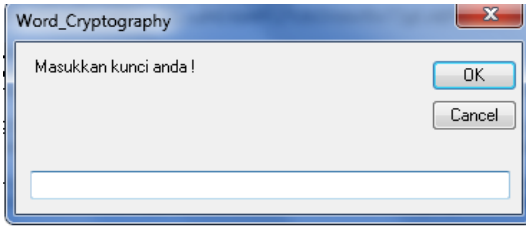
Gambar 9. Kerangka Sistem Aplikasi Kriptografi

Sebuah dokumen akan di proses dalam aplikasi kriptografi MD5 tujuannya untuk melakukan enkripsi dokumen dan menghasilkan kunci (password). Sistem ini menggunakan teknik *symmetric key* sehingga kunci yang sama akan diberikan kepada penerima untuk dapat membuka dokumen. File enkripsi akan kemnali diproses melalui aplikasi kriptografi sehingga menghasilkan dokumen deskripsi.

4. HASIL PENELITIAN

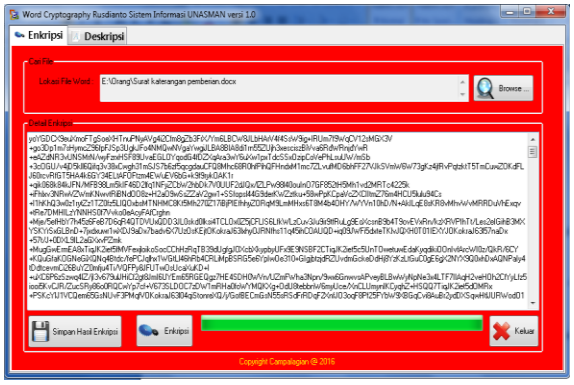
4.1. Proses Enkripsi

Sebuah aplikasi kriptografi telah dihasilkan dan dilakukan uji coba dengan sebuah dokumen. Peroses yang pertama dilakukan dalam enkripsi yaitu penambahan bit kedalam file yang akan dienkripsi berupa password yang akan menjadi *key secrect*, dapat dilihat pada gambar 5.8.



Gambar 10. penambahan bit kedalam file enkripsi

Selanjutnya sistem akan melakukan proses enkripsi seperti yang ditunjukkan gambar 11 dan gambar 12.

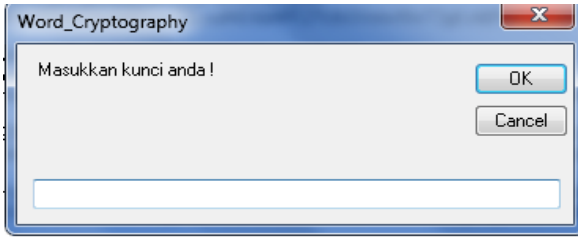


Gambar 11. Hasil enkripsi Aplikasi Kriptograsi

Gambar 12. Dokumen enkripsi

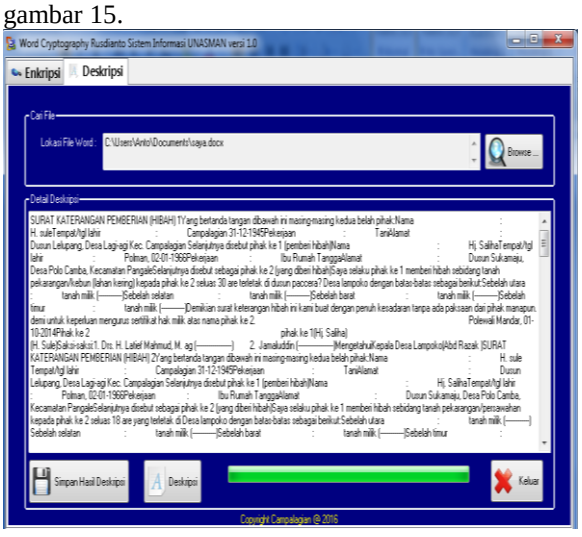
4.2. Proses Deskripsi

Peroses pertama yang dilakukan dalam mendekripsi file yang telah di enkripsi yaitu petama-pertama dilakukan memasukan kunci atau password yang sama dengan kunci enkripsi karena kunci tersebut merupakan kunci rahasia yang menggabungkan diri pada file yang di enkripsi, tampilan yang sama dengan yang dapat dilihat pada gambar 13.



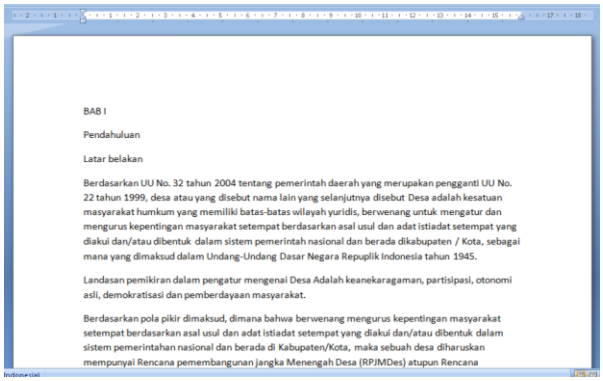
Gambar 13. Masukkan *password*

Selanjutnya sistem akan memproses kedalam file dan hasilnya ditunjukkan pada gambar 14 dan gambar 15.



Gambar 14. Hasil deskripsi aplikasi kriptografi

(P) ISSN 2442-451X
(O) ISSN 2503-3832



BAB I

Pendahuluan

Latar belakan

Berdasarkan UU No. 32 tahun 2004 tentang pemerintah daerah yang merupakan pengganti UU No. 22 tahun 1999, desa atau yang disebut nama lain yang selanjutnya disebut Desa adalah kesatuan masyarakat humkum yang memiliki batas-batas wilayah yuridis, berwenang untuk mengatur dan mengurus kepentingan masyarakat setempat berdasarkan asal usul dan adat istiadat setempat yang diakui dan/atau dibentuk dalam sistem pemerintah nasional dan berada dikabupaten / Kota, sebagai mana yang dimaksud dalam Undang-Undang Dasar Negara Repuplik Indonesia tahun 1945.

Landasan pemikiran dalam pengatur mengenai Desa Adalah keanekaragaman, partisipasi, otonomi asli, demokratisasi dan pemberdayaan masyarakat.

Berdasarkan pola pikir dimaksud, dimana bahwa berwenang mengurus kepentingan masyarakat setempat berdasarkan asal usul dan adat istiadat setempat yang diakui dan/atau dibentuk dalam sistem pemerintahan nasional dan berada di Kabupaten/Kota, maka sebuah desa diharuskan mempunyai Rencana pemembangunan jangka Menengah Desa (RPJMDes) atupun Rencana

Gambar 15. Hasil Deskripsi Dokumen

4.3. Coding Pemrograman

Aplikasi kriptografi dibangun menggunakan bahasa pemrograman *Visual Basic.Net*. dan bahasa pemrograman java. Berikut disajikan source kode untuk penambahan bit.

Visualbasic.Net

```
Imports Microsoft.Office.Interop.Word
Imports System.Windows.Forms
Imports System.Text
Imports System.Security.Cryptography

Public Class Form1
    Dim MD5Enc As New MD5CryptoServiceProvider
    Dim MD5Dec As New TripleDESCryptoServiceProvider
    Dim enc As New ASCIIEncoding
    Dim kunci As String = "rusdianto sistem"
    Function encrypt(ByVal text As String, ByVal key As
String)
        With MD5Dec
            .Key = MD5Enc.ComputeHash(enc.GetBytes(key))
            .Mode = CipherMode.ECB
        End With
```

Pemrograman java

```
package kelMD5;

import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;


public class kelMD5 {
private String plainTeks;
MessageDigest messageDigest;

public kelMD5(String plainTeks){
this.plainTeks = plainTeks;
}

public String encrypt(String plaintext) throws NoSuchAlgorithmException{
this.messageDigest = MessageDigest.getInstance("MD5");
System.out.println("Metode Enkripsi : " + this.getMessageDigest().getAlgorithm());
System.out.println("Provider : " + this.getMessageDigest().getProvider());
System.out.println("ToString :" + this.getMessageDigest().toString());

String input = this.getPlainTeks();
this.getMessageDigest().update(input.getBytes());
byte[] output = this.getMessageDigest().digest();
return bytesToHex(output);
```

5. KESIMPULAN

Algoitma kriptografi MD5 dengan kemampuan enkripsi yang dimiliki dapat menjadi rekomendasi untuk keamanan data dan jaringan sistem komputer. Algoritma kriptografi MD5 dapat dimanfaatkan secara bermacam-macam pada aplikasi keamanan, baik untuk kemanana file dokumen, database atau kemanan sistem jaringan. Walaupun hal ini bukan satu-satunya solusi ajaib dan belum tentu dapat menyelesaikan semua masalah kemanan, tetapi sedapat mungkin mengurangi banyak risiko keamanan yang dihadapi organisasi. Aplikasi kriptografi MD5 dapat dikembangkan dengan bahasa pemprograman yang lain serta kombinasi metode-metode lain untuk memperkuat keamanan integritas dokumen. Algoritma kriptografi MD5 tidak akan memberikan pengaruh atau mengganggu keaslian dari sebuah dokumen.

DAFTAR PUSTAKA

[1] A. Precilia, D.P. Izzuddin, "Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5)," *Tek. Elektro, Fak. Tek. Univ. Panca Marga*, vol. 5, no. 1, pp. 14–19, 2015.

[2] P.-M. H. Espejel-Trujillo A., Castillo-Camacho I., Nakano-Miyatake M.*, "Identity Document Authentication Based on VSS and QR Codes," *2012 Iberoam. Conf. Electron. Eng. Comput. Sci.*, vol. 3, pp. 241–250, 2012.

[3] Qashlim, Akhmad. Hasruddin, "Implementasi Teknologi QR-Code Untuk Kartu Identitas," *J. Ilmu Komput.*, vol. 1, no. 2, pp. 1–6, 2015.

[4] Anan T; Kuraki K; Takahashi J, "Paper Encryption Technology," *FUJITSU Sci Tech*, vol. 46, no. 1, pp. 87–94, 2010.

[5] Sharma D; Sarao P; Dudi S, "Implementation of Md5- 640 Bits Algorithm," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 3, no. 5, pp. 286–293, 2015.

[6] T. Baccam, "Transparent Data Encryption : New Technologies and Best Practices for Database Encryption," *Sans Inst.*

[7] D. Shah, "Digital Security Using Cryptographic Message Digest Algorithm," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 3, no. 10, pp. 215–219, 2015.

[8] H. Kozushko, "MD5 Algorithm," 2003, pp. 1–12.

[9] W. Xijin and F. Linxiu, "The Application Research of MD5 Encryption Algorithm in DCT Digital Watermarking," *Phys. Procedia*, vol. 25, pp. 1264–1269, 2012.