Kriptografi dan Aplikasinya pada Message Digest 5

Tami Utiwi Handayani
Program Studi Teknik Informatika ITB, Bandung 40135, email: if16059@students.if.itb.ac.id

Abstract – *Makalah ini membahas tentang kriptografi dan aplikasinya pada Message Digest 5.Kriptografi adalah ilmu untuk menjaga kerahasiaan suatu berita. Istilah-istilah dalam kriptografi adalah palinteks, chiperteks, enkripsi, dan deskripsi. Algoritma kriptografi adalah fungsi matematika yang digunakan untuk enkripsi dan deskripsi. .Algoritma kriptografi terbagi menjadi 3 bagian besar. Berdasarkan kesamaan kunci, kerahasiaan kunci, dan arah implementasi dan sejarahnya. Salah satu aplikasi pada kriptografi adalah fungsi hash satu arah, yang banyak digunakan pada massege digest 5. MD5 adalah suatu fungsi hash satu arah yang dapat mengubah masukan dengan panjang variabel menjadi keluaran tetap 128 bit.*

Kata Kunci*: Kriptografi, Plainteks,chiperteks,MD5*

1. PENDAHULUAN

Salah satu aplikasi aritmatika modulo dan bilangan prima adalah kriptografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan menyandikan pesan tersebut. Kerahasian menjadi sangat penting akhir-akhir ini. Dengan adanya pesan-pesan tersandi, hal-hal yang dianggap berharga dapat dan rahasia dapat diselamatkan. Konsepdari kriptografi adalah mengacak data dengan suatu metode teretentu. Contoh pada penggunaan PIN kartu kredit, dan lain sebagainya. Kriptografi dapat digunakan untuk menyimpan rahasia dari orang yang tidak berhak mendapatkan berita dari rahasia itu.

2. KRIPTOGRAFI

2.1 Kriptografi

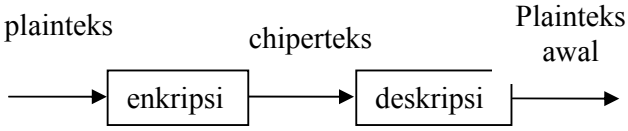
Dalam kriptografi dikenal istilah plainteks (*plaintext*), chiperteks (*chipertext*), enkripsi (*encryption*), dan dekripsi (*descryption*).

1. Plainteks (*Plaintext*)
   Plainteks berasal dari kata *plaintext* yang berarti teks jelas yang dapat dimengerti. Teks tersebut merupakan pesan yang akan dirahasiakan kemudian dikirim.

2. Chiperteks (*Chipertext*)
   Chiperteks berasal dari kata *chipertext* yang berarti teks yang yang tersandi. Chiperteks merupakan hasil penyandian dari plainteks.

3. Enskripsi (*Encryption*)
   Enkripsi berasal dari kata *encryption* merupakan proses penyandian pesan dari plainteks ke chiperteks. Hasil dari enkripsi adalah chiperteks.

4. Deskripsi (*Descryption*)
   Deskripsi berasal dari kata *descryption* merupakan proses pengembalian dari chiperteks ke plainteks. Deskripsi membuat pesan menjadi dapat dimengerti.



Tabel 1. Enkripsi da deskripsi

Jika chiperteks dilambangkan dengan C dan plainteks dilambangkan dengan P, maka persamaan enkripsi adalah

$$E(P)=C \quad (1)$$

dimana enkripsi merupakan pemetaan dari plainteks (P) ke chiperteks (C). Sebaliknya, deskripsi memetakan chiperteks (C) ke plainteks (P), sehingga persamaan deskripsi adalah

$$D(C)=P \quad (2)$$

Kriptografi memetakan plainteks ke chiperteks dan dari chiperteks ke plainteks kembali, maka persamaan

$$D(E(P)) = P \quad (3)$$

harus benar.

2.2 Tujuan Kriptografi

Tujuan utama dari kriptografi adalah:

1. Kerahasiaan
   Kerahasiaan adalah bahwa data yang dirahasiakan tidak dapat dibaca oleh orang yang tidak berkepentingan. Hanya orang yang mempunyai kuncinyalah yang dapat membaca data tersebut. Rahasia dilakukan dengan penyandian (enkripsi).

2. Autentikasi
   Autentikasi memberi jaminan bahwa data yang dikirim asli serta dengan siapa kita berhubungan. Dua pihak yang saling berhubungan harus saling mengenal.

3. Keutuhan
   Keutuhan memberi jaminan bahwa data yang dikirim sama dengan data yang diterima. Data dijamin tidak mengalami perubahan seperti penghapusan,penambahan, penyisipan, dan hal-hal lainnya.

4. Non-repudasi
   Non-repudasi yaitu mencegah penyangkalan. Si pengirim tidak dapat menyangkal bahwa data yang dikirimkan bukan darinya.

2.3 Algoritma Kriptografi

Algoritma kriptografi adalah fungsi matematika yang digunakan untuk enkripsi dan deskripsi. Algoritma kriptografi semakin kuat jika waktu untuk proses pemecahan sandi semakin lama. Dengan begitu algoritma tersebut semakin aman untuk digunakan.

Algoritma kriptografi harus memiliki kekuatan untuk

1. Konfusi atau pembingungan (*confusion*)
   Sulit untuk direkonstruksikan secara langsung tanpa kuncinya.
2. Difusi atau peleburan (*difusion*)
   Karakteristik dari plainteks tersebut hilang.

Algoritma kriptografi dibedakan menjadi:

1. Berdasarkan kesamaan kuncinya
2. Berdasarkan kerahasiaan kuncinya
3. Berdasarkan arah implementasi dan sejarahnya

Algoritma kriptografi berdasarkan kesamaan kuncinya dibedakan menjadi 2,

1. Kunci asimetris
   Kunci asimetris yaitu kunci enkripsi berbeda dengan kunci deskripsi (pada gambar, K1≠ K2). Contoh algoritma yang menggunakan algoritma ini adalah *RSA* (*Rivest-Shamir-Adleman*)
2. Kunci simetris
   Kunci simetris yaitu kunci enkripsi sama dengan kunci deskripsi (pada gambar, K1=K2). Contoh algoritma yang menggunakan algoritma ini adalah *DES* (*Data Encryption Standard*). Jumlah kunci yang dibutuhkan umumnya adalah :

$$ {}_nC_2 = \frac{n \,.\, (n-1)}{2} \qquad (3) $$

dengan n menyatakan banyaknya pengguna.

Algoritma kriptografi berdasarkan kerahasiaan kuncinya dibedakan menjadi 2:

1. Algoritma kunci pribadi
   Algoritma kunci simetris sering dianggap algoritma kunci pribadi karena kunci dari enkripsi dan deskripsi sama dan harus dirahasiakan. Kelemahan dari algoritma ini adalah si pengirim harus mencari cara untuk mengirimkan kunci kepada si penerima sehingga kunci untuk memecahkan sandi tidak diketahui orang lain.

2. Kunci publik
   Algoritma kunci asimetri sering disebut sebagai algoritma kunci publik. Algoritma ini mempunya 2 kunci, kunci publik, adalah kunci untuk enkripsi yang tidak dirahasiakan, dan kunci rahasia, adalah kunci untuk deskripsi yang harus dirahasiakan.

Algoritma kriptografi berdasarkan arah implementasi dan sejarahnya terbagi menjadi 2,

1. Algoritma kriptografi klasik
2. Algoritma kriptografi modern

2.3.1 Algoritma Kriptografi Klasik

Algoritma kriptografi klasik dibedakan menjadi 2,

1. Algoritma kriptografi subtitusi
   Algoritma ini pada awalanya adalah penyandian dengan menganti huruf plainteks ke karakter lain sebagai chiperteksnya. Terdapat berbagai macam metode subtitusi.
   1) Metode subtitusi sederhana
      Mengganti setiap huruf dari plainteks dengan huruf lain sebagai chiperteksnya yang sebelumnya telah didefinisikan oleh algoritma kunci.

      Contoh: Dengan subtitusi alfabet A=F,

      Plain teks:
      A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
      Chiperteks:
      F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

      Pesan
      HELLO WORLD
      akan menjadi
      MJQQT BTWQI

   2) Metode Caesar
      Metode ini digunakan ole Julius Caesar untuk menyandikan pesan yang ia kirim kepada gubernurnya. Pada metode ini setiap huruf disubtitusi dengan huruf ketiga berikutnya dalam susunan alfabet. Kunci dalam metode ini adalah pergeseran huruf sebanyak 3.

Plainteks:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Chiperteks:
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Dengan demikian, secara matematis metode Caesar dapat ditulis sebagai

$c_i = E(P_i) = (p_i + 3) mod\ 26$ (4)

dengan p_i adalah palinteks dan c_i adalah chiperteks.

Penerima pesan mengembalikan lagi chiperteks ke plainteks dengan aturan

$p_i = D(P_i) = (p_i - 3) mod\ 26$ (5)

Contoh:
Pesan

HELLO WORLD

akan menjadi

KHOOR ZRUOG

3) Metode Vigenére
Metode ini pertama kali dipopulerkan oleh Balise de Vigenére seorang diplomat Perancis. Metode Vigenére yaitu metode subtitusi multi-alfabet. Metode ini mirip dengan metode Caesar, tapi dengan pergeseran alfabet yang berlainan. Tidak ada huruf yang saling bersebelahan yang memiliki kunci yang sama.
Contoh: dengan kata kunci MERAPI

Plainteks:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Chiperteks:
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

R S T U V W X Y Z A B C D E F G H I J K L M N O P Q

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

P Q R S T U V W X Y Z A B C D E F G H I J K L M N O

I J K L M N O P Q R S T U V W X Y Z A B C D E F G H

Pesan

SUKSES

Akan menjadi

EYBSTA

Huruf S disandikan dengan A= M, huruf U disandikan dengan A=E, begitu seterusnya.

4) Metode *One Time Pad*
Metode ini terkenal sangat kuat sehinga tidak mudah dipecahkan. Metode ini pertama kali diperkenalkan oleh Gilbert Vernam dalam Perang Dunia I. Metode ini memberikan syarat-syarat khusus terhadap kunci yang digunakan yaitu terbuat dari karakter / huruf yang acak (kunci acak atau *pad*), dan pengacakannya tidak menggunakan rumus tertentu. Jika kunci yang digunakan benar-benar acak, maka dipastikan metode ini sangat kuat. Metode ini sangat bergantung kepada keacakan kuncinya, sehingga kunci pengacakan harus terlindungi dengan baik.

2. Algoritma kriptografi transposisi
Algoritma kriptografi transposisi adalah penyandian dengan mengubah letak plainteks. Beberapa metode algoritma kriptografi transposisi:
1) Metode *rail fence*
Metode ini menyandikan pesan dengan cara menuliskan huruf-huruf plainteks secara turun-naik dalam sebuah pagar imajiner.
Contoh: dengan algoritma 5 baris
Pesan

HELLO WORLD

Proses

H _ _ _ _ _ _ _ D
_ E _ _ _ _ _ L _
_ _ L _ _ _ _ R _ _
_ _ _ L _ _ O _ _ _
_ _ _ _ O W _ _ _ _

Chiperteks
HD EL LR LO OW

2) Metode *route*
Metode ini menyandikan pesan dengan cara menuliskan pesan secara kolom dari atas kebawah dalam kisi-kisi imajiner dengan ukuran yang telah disepakati.
Contoh: 5 baris dengan pembacaan dari kanan bawah spiral searah jarum jam
Pesan

DUNIA SEDANG HURA-HURA

Proses

D	S	G	-
U	E	H	H
N	D	U	U
I	A	R	R
A	N	A	A

Chiperteks
AANAI NUDSE G-HUR RADEH U

3) Metode kolom
Metode ini dituliskan secara baris dengan panjang yang telah ditentukan kuncinya. Teks sandi-nya dibaca secara kolom demi kolom dengan pengacakan melalui permutasian angka kuncinya. Panjang baris dan permutasian kolomnya disebut sebagai "kata kunci".
Contoh: kata kunci: KUNCI yang berarti 5 kolom, dengan urutan kolom 4 1 3 5 2
Pesan
DUNIA SEDANG HURA-HURA
Proses

4	1	3	5	2
K	U	N	C	I
D	U	N	I	A
S	E	D	A	N
G	H	U	R	A
-	H	U	R	A

Chiperteks
UEHH ANAA NDUU DSG- IARR

4) Metode ganda
Metode ini merupakan metode kolom yang digunakan 2 kali. Sehingga merupakan metode kolom yang dikolomkan.
Contoh:menggunakan contoh metode kolom, dengan kata kunci kedua SAPI, berarti 4 kolom dengan urutan kolom 4 2 1 3
Pesan
UEHH ANAA NDUU DSG- IARR
Proses

4	2	1	3
U	E	H	H
A	N	A	A
N	D	U	U
D	S	G	-
I	A	R	R

Chiperteks
HAUGR ENDSA HAU-R UANDI

5) Metode Myszkowski
Metode ini merupakan transposisi kolom yang dibedakan dalam pendefenisian dan permutasi kata kuncinya. Untuk mempersulit sandi, biasanya metode ini digabungkan dengan metode subtitusi.
Contoh: pada contoh metode kolom, urutan kolom 4 1 3 5 2 menjadi 1 1 3 5 4 dengan penulisan chiperteks kolom yang paling kiri ditulis terlebih dahulu.
Pesan
DUNIA SEDANG HURA-HURA
Proses

1	3	3	2	4
D	U	N	I	A
S	E	D	A	N
G	H	U	R	A
-	H	U	R	A

Chiperteks
DSG- IARR UNED HUHU ANAA

2.3.2 Algoritma Kriptografi Modern

Dalam perkembangannya, algoritma kriptografi klasik mudah untuk dipecahkan, sehingga muncul algoritma kriptografi modern. Algoritma kriptografi modern menggunakan sistem digital, yang sudah tentu mempunyai algoritma yang kuat. Metode penyandian subtitusi modern menggunkan sebuah program aplikasi tertentu dimana teks asli dalam sebuah file digital diganti menjadi kumpulan karakter lain, tetap dalam bentuk digital sehingga ,enghasilka file yang siap dikomunikasikan.

3. MESSAGE DIGEST 5

Salah satu bagian dari kriptografi adalah fungsi hash satu arah. Fungsi hash satu arah adalah dimana kita dengan mudah melakukan enkripsi tetapi sulit untuk melakukan deskripsi tanpa memiliki kuncinya.Fungsi hash yang paling umum berbentuk

$$h(k) = k \bmod m \qquad (6)$$

dimana m adalah jumlah lokasi memori yang tersedia. Fungsi h menempatkan record dengan kunci k yang beralamatkan di h(k).

Salah satu fungsi hash yang banyak digunakan adalah Message Digest 5 yang dirancang oleh Ron Rivest MD5 merupakan kelanjutan dari MD4 yang dirancang untuk tujuan keaman. Secara matematis tidak ada pesan yang memiliki fngsi hash yang sama. Tidak ada cara yang paling efisien untuk membongkar hash suatu pesan kecuali *brute-force.*

3.1 Cara Kerja MD5

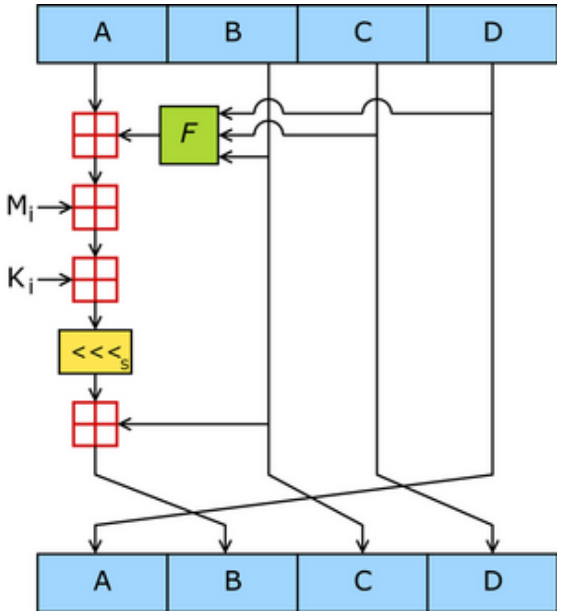
MD5 mengolah blok 512 bit, dibagi dalam 16 subblok berukuran masing-masing 32 bit. Keluaran algoritma diset menjadi 4 blok yang masing-masing berukuran 32 bit yang setelah digabungkan akan membentuk nilai hash 128 bit.

3.1.1 Agoritma MD5

5 langkah untuk menghitung intisari pesan

1. Menambahkan bit
2. Penambahan panjang pesan
3. Inisialisasi MD5
4. Proses pesa didalam blok 16 word
5. Keluaran MD5

Pesan akan diambahkan dengan bit-bit tambahan sehinga panjang bit kongruen dengan 448 mod 512 yang berarti pesan hanya memiliki panjang 64 bit dari kelipatan 512. Pada MD5 terdapat empat buah word 32 bit dimana berguna untuk menginisilisasi message digest pertama kali. Pada MD5 juga terdapat 4 buah fungsi nonlinear yang digunakan pada setiap operasinya. Keluaran MD5 adalah 128 bit dari word terendah A dan tertingi D.



Gambar 1: Algoritma MD5

3.1.2 Pseudocode

Pseudocode dari MD5 adalah sebagai berikut

```
//Catatan: Seluruh variable tidak pada 32-bit dan dan wrap modulo 2^32 saat melakukan perhitungan

//Mendefinisikan r sebagai berikut


var int[64] r, k
r[ 0..15] := {7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22}
r[16..31] := {5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20}
r[32..47] := {4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23}
r[48..63] := {6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21}

//Menggunakan bagian fraksional biner dari integral sinus sebagai konstanta:
for i from 0 to 63
    k[i] := floor(abs(sin(i + 1)) × 2^32)

//Inisialisasi variabel:
var int h0 := 0x67452301
var int h1 := 0xEFCDAB89
var int h2 := 0x98BADCFE
var int h3 := 0x10325476

//Pemrosesan awal:
append "1" bit to message
append "0" bits until message length in bits ≡ 448 (mod 512)
append bit length of message as 64-bit little-endian integer to message

//Pengolahan pesan pada kondisi gumpalan 512-bit:
for each 512-bit chunk of message
    break chunk into sixteen 32-bit little-endian words w(i), 0 ≤ i ≤ 15

//Inisialisasi nilai hash pada gumpalan ini:
    var int a := h0
    var int b := h1
    var int c := h2
    var int d := h3

//Kalang utama:
    for i from 0 to 63
        if 0 ≤ i ≤ 15 then
            f := (b and c) or ((not b) and d)
            g := i
        else if 16 ≤ i ≤ 31
            f := (d and b) or ((not d) and c)
            g := (5×i + 1) mod 16
  else if 32 ≤ i ≤ 47
      f := b xor c xor d
      g := (3×i + 5) mod 16
  else if 48 ≤ i ≤ 63
      f := c xor (b or (not d))

      g := (7×i) mod 16
```

```
        temp := d
        d := c
        c := b
        b := ((a + f + k(i) + w(g))
leftrotate r(i)) + b
        a := temp

    //Tambahkan hash dari gumpalan
sebagai hasil:
    h0 := h0 + a
    h1 := h1 + b
    h2 := h2 + c
    h3 := h3 + d

var int digest := h0 append h1
append h2 append h3

//(diwujudkan dalam little-endian)
```

4. KESIMPULAN

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan menyandikan pesan tersebut. Algoritma kriptografi adalah fungsi matematika yang digunakan untuk enkripsi dan deskripsi. Algoritma kriptografi terbagi menjadi 3:

1. Berdasarkan kesamaan kunci (kunci simetris dan asimetris)
2. Berdasarkan kerahasiaan kunci (kunci privat dan kunci publik)
3. Berdasarkan arah implementasi dan sejarahnya (klasik dan modern)

Salah satu aplikasi dari kriptografi adalah MD5. MD5 adalah sebuah fungsi hash satu arah yang mengubah masukan dengan panjang variabel menjadi keluaran tetap 128 bit.

DAFTAR REFERENSI

[1] Munir, Rinaldi. (2006). Bahan Kuliah IF2153 Matematika Diskrit. Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] Kriptografi. (2006). *http://id.wikipedia.org/wiki/Kriptografi* Tanggal akses: 31 Desember 2007,pukul 16.40

[3] Aplikasi Kriptografi dengan Algoritma Message Digest 5. (2006). *www.elektro.undip.ac.id/transmisi/jun06/5_aghus_abp.pdf* Tanggal akses: 1 Januari 2008 pukul 10.15

[4] Wikipedia. (2006). ***http://id.wikipedia.org/wiki/MD5*** Tanggal akses:1Januari 2007 pukul 10:30

[5] MD5 dan SHA-1 (Kriptografi dengan fungsi hash). 2007. http:// ilmukomputer.com/2007/03/14/**md5-dan-sha-1**-kriptografi-dengan-fungsi-hash/ Tanggal akses: 1 Januari 2007, pukul 10.45

[6] Pengamanan informasi dan kriptografi (2007) *http://hadiwibowo.wordpress.com/* Tanggal akses: 1 Januari 2008, pukul 10.40