Algoritma Message Authentication Code (MAC) dan Perbandingan Metode Penyerangannya

Desfrianta Salmon Barus - 13508107
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If18107@students.itb.ac.id; Salmonbarus@gmail.com

Abstrak – MAC (Message Authentication Code) adalah suatu metode pengamanan dengan melakukan otentikasi pada suatu pesan dimana pengirim dan penerima pesan butuh untuk memasukkan kunci untuk mengecek keotentikan dari pesan tersebut. Message Authentication Code berfungsi untuk melakukan otentikasi dari pesan tersebut untuk mengecek apakah pesan tersebut telah mengalami perubahan atau belum sehingga dapat dideteksi apabila ada yang melakukan modifikasi (man in the middle attack) pada pesan tersebut. Dalam penerapannya berbagai metode algoritma digunakan untuk Message Authentication Code. Dalam pemecahannya banyak juga metode penyerangan (attack) yang dilakukan oleh orang-orang yang ingin memperoleh isi pesan tersebut yang bersesuaian dengan algoritma Message Authentication Code yang digunakan. Dalam penggunaannya Message Authentication Code digunakan dalam berbagai aplikasi yang berkaitan dengan pengiriman pesan seperti email, messenger, dan berbagai metode pengiriman pesan elektronik lainnya.

Kata Kunci – MAC (Message Authentication Code), autentifikasi, komputasi ,attack.

I. PENDAHULUAN

Teknologi terus mengalami perkembangan dari hari ke hari, khususnya dalam bidang informasi. Perkembangan tersebut membawa metode pertukaran pesan yang dulunya dilakukan dengan menggunakan pesan dalam bentuk fisik menjadi pertukaran pesan melalui digital. Terutama di dukung dengan teknologi seperti internet yang memudahkan kita untuk bertukar pesan digital kapanpun dan dimanapun kita berada.

Penggunaan data dengan bentuk digital tersebut mengakibatkan kita memperoleh berbagai kemudahan-kemudahan dalam menyampaikan pesan, namun dilain sisi, dengan perkembangan teknologi juga pihak lain dapat dengan cukup mudah dapat melakukan gangguan terhadap pengiriman yang dilakukan. Padahal untuk keperluan tertentu kerahasiaan dari suatu informasi ataupun data sangatlah penting untuk dijaga agar tidak dimanipulasi oleh orang-orang yang bermaksud jahat dengan informasi ataupun data tersebut.Untuk mengatasi hal-hal tersebut maka diperlukan suatu metode pengamanan yang tepat untuk menjamin kebenaran dan ketepatan dalam penyampaian informasi dalam bentuk data digital tersebut. Salah satu metode pengamanan yang dapat digunakan adalah MAC atau Message Authentication Code.

Message Authentication Code adalah metode pengamanan pesan dengan menambahkan sepotong informasi yang digunakan untuk melakukan autentifikasi pada suatu pesan entah penambahan informasi tersebut secara terpisah dari pesanyang dikirim , atau ditambahkan pada pesan atau dengan metode yang lainnya. Dalam pembuatan Message Authentication Code ini digunakan Algoritma Message Authentication Code yang menerima suatu kunci tertentu untuk mengotentikasi pesan, dan untuk melakukan pengecekan integritas dari pesannya penerima pesan harus memasukkan kunci yang sesuai pula untuk melakukan pengecekan pada pesan tersebut.

Pada Message Authentication Code penulis dan pembaca pesan menggunakan kunci yang sama layaknya metode enkripsi simetris, berbeda dengan tanda tangan digital dimana penggirim pesan dan penerima pesan menggunakan kunci yang berbeda untuk menambahkan tanda tangan digital pada pesan tersebut. Perbedaan dari Message Authentication Code dan Hash adalah untuk suatu pesan tertentu meskipun ada seseorang yang berhasil memecahkan kunci rahasia dari suatu pesan, pada pesan lainnya yang dibuat dengan cara yang sama, penyerang tersebut tidak bisa menebak kuncinya tanpa melakukan sejumlah komputasi terlebih dahulu karena kunci untuk setiap pesan berbeda.

Attack adalah suatu istilah yang digunakan untuk merujuk pada gangguan yang dilakukan oleh suatu pihak tertentu yang berkepentingan ketika mencoba untuk memanfaatkan kelemahan dari fungsi ataupun algoritma penyusun suatu metode pengamanan yang ditambahkan pada suatu pesan.

Untuk melakukan perusakan terhadap isi awal dari pesan tersebut banyak metode penyerangan yang digunakan. berikut ini adalah contoh-contohnya:

-Collision attack
-Preimage attack
-Birthday attack

-Brute force attack
-Rainbow table
-Distinguishing attack
-Side-channel attack.

II. VARIASI ALGORITMA MESSAGE AUTHENTICATION CODE

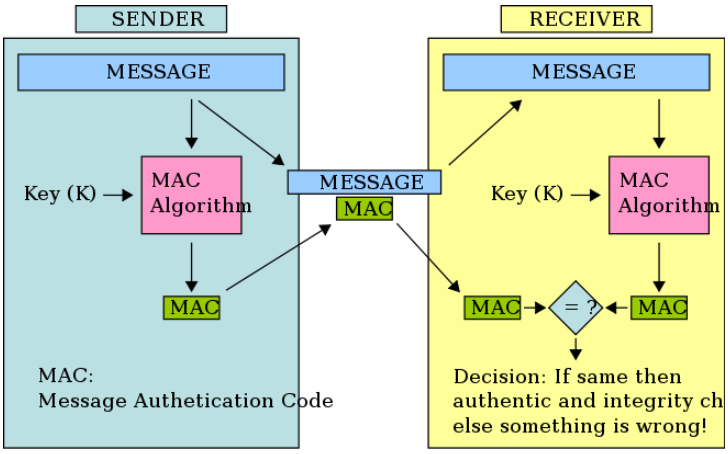
Message Authentication Code atau MAC adalah suatu fungsi pembangkitan nilai hash dari suatu pesan yang panjangnya tetap ataupun penggunaan algoritma tertentu dengan menggunakan suatu kunci rahasia yang akan digunakan untuk melakukan pengecekan pada pesan tersebut. Atau dapat dirumuskan sebagai berikut:

$$MAC = C_k(M)$$

Dimana:

MAC = nilai hash untuk otentikasi pesan
C = fungsi hash atau algoritma MAC
K = Kunci rahasia
M = Pesan yang akan dicari nilai hashnya

Atau dapat digambarkan sebagai berikut :



Dalam gambar diatas, seorang pengirim pesan melakukan pembangkitan suatu nilai Message Authentication Code dengan menggunakan kunci tertentu pada suatu algoritma Message Authentication Code. Lalu pesan tersebut dikirimkan pada seorang penerima. Setelah si penerima menerima pesan tersebut, si penerima lalu melakukan pengecekan pada pesan tersebut. Penerima akan membangkitkan suatu nilai Message Authentication Code dengan menggunakan kunci yang sama pada algoritma Message Authentication Code yang sama seperti yang digunakan oleh pihak pengirim pesan. Lalu pihak penerima akan mengecek kesamaan dari Message Authentication Code yang telah dibangkitkan dengan Message Authentication Code yang dikirimkan oleh pengirim untuk melakukan otentikasi pesan yang sikirimkan. Bila nilai Message Authentication Code yang diperoleh sama maka pesan tersebut merupakan pesan asli yang dikirimkan oleh si pengirim, jika nilainya berbeda maka pesan tersebut dicurigai telah mengalami serangan tertentu dalam proses pengirimannya.

Dalam membuat Message Authentication Code ada beberapa metode algoritma yang digunakan. Message Authentication Code dapat dibuat dari sebuah fungsi kriptografi hash yaitu Message Authentication Code ataupun dengan algoritma block-cipher sepereti OMAC CBC-MAC dan PMAC. Namun algoritma Message Authentication Code tercepat seperti UMAC dan VMAC dikonstruksi berdasarkan universal hashing.

A. Message Authentication Code dengan fungsi hash

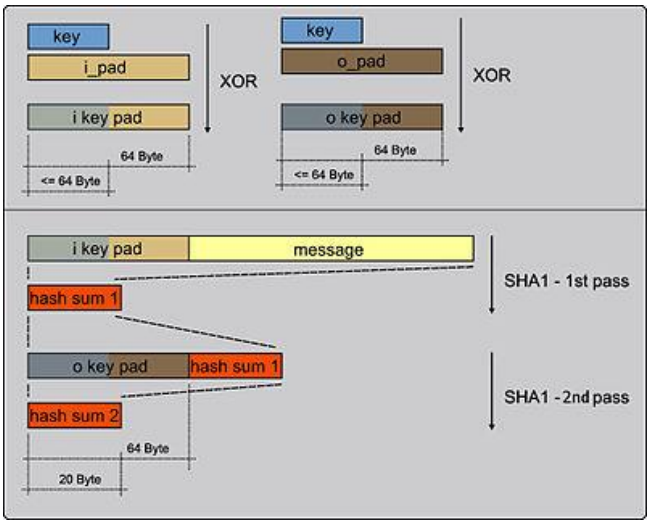
Pada bagian ini kita akan membahas tentang pembangkitan nilai Message Authentication Code dari suatu pesan dengan menggunakan fungsi hash satu arah dengan kombinasi suatu kunci rahasia tertentu. Pada algoritma ini digunakan fungsi pembangkit nilai hash seperti SHA-1 dan MD5 untuk memperoleh nilai HMAC dari suatu pesan. Sebagai contoh dari pembangkitan Message Authentication Code dengan fungsi hash dapat dijelaskan melalui rumus berikut:

$$HMAC = H((K \oplus opad) \,||\, H(K \oplus ipad) \,||\, m)$$

Dimana:

H = fungsi hash satu arah
K = kunci rahasia
M = Pesan yang akan dicari nilai HMACnya
Ipad = inner padding (0x5c5c5c…5c5c, hexadecimal konstan dengan panjang satu blok)
Opad = outer padding (0x363636…3636, hexadecimal konstan dengan panjang satu blok)

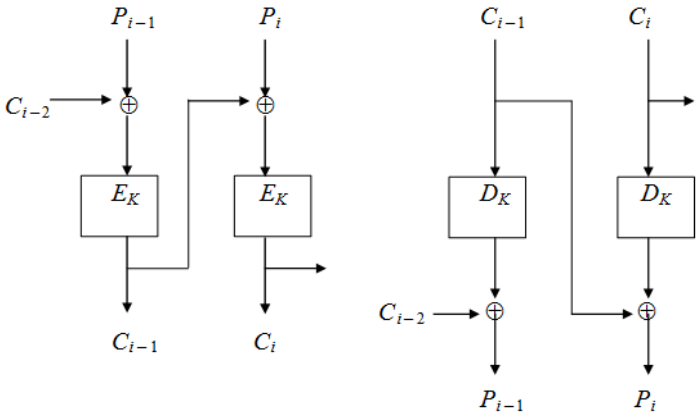
Atau dapat digambarkan sebagai berikut :



B. Message Authentication Code dengan Blok-Cipher

Algoritma Message Authentication Code ini disusun dengan menggunakan block-cipher. Blok-cipher merupakan cipher dengan kunci simetris yang bekerja dalam sekumpulan bit dengan panjang yang tetap yang disebut sebagai blok. Untuk pesan yang lebih panjang dari blok tersebut pesan akan dibagi menjadi blok-blok dengan panjang sama dan akan dienkripsi setiap bloknya secara terpisah. Beberapa contoh algoritma penyusun Message Authentication Code dengan menggunakan block-cipher adalah PMAC (Parrallelizable Message Authentication Code), OMAC(One-key Message Authentication Code), dan CBC-MAC (Cipher Block Chaining Message Authentication Code). Sebagai contoh pada bagian ini kita akan membahas tentang CBC-MAC.

CBC-MAC melakukan enkripsi pada pesan dengan menggunakan algoritma block cipher dalam mode CBC untuk membentuk serangkaian blok-blok dimana enkripsi pada tiap tahap disusun berdasarkan enkripsi tahap sebelumnya. Proses enkripsi dan dekripsi pada CBC apat dijelaskan melalui gambar berikut:



C. Message Authentication Code dengan Universal Hash

Beberapa Message Authentication Code yang tercepat berasal dari metode universal hashing. Universal hashing adalah pemilihan sebuah fungsi hash secara acak dari sekumpulan fungsi hash dengan fungsi matematis tertentu. Hal ini mengakibatkan jumlah kolisi yang lebih sedikit.

Andaikan himpunan fungsi hash yang terdiri dari fungsi hash h yang dipilih secara acak yang memetakan suatu himpunan kunci m pada n = {1,2,3,...,n}. H dapat dikatakan universal apabila semua x dan y ϵ m dimana x tidak sama dengan y, peluang nilai h(x) sama dengan nilai h(y) ,lebih kecil 1/|n|, dirumuskan sebagai:

$$^{Pr}{}_{h<=H}[h(x) = h(y)] \leq 1/n$$

Dari persamaan diatas jika h adalah fungsi hash universal, maka untuk setiap s himpunan bagian dari m, untuk setiap x anggota m dengan nilai h angka kolisi yang diharapkan antara x dengan elemen dari s adalah |s|n. Fungsi |s| universal dikatakan kuat jika x,x' pada M dan y,y' pada n:

$$^{Pr}{}_{h<=H}[h(x) = h(y) \text{ dan } h(x') = h(y')] \leq 1/n^2$$

III. JENIS ATTACK PADA DATA

Attack merupakan proses pengambilan atau pengubahan informasi yang dilakukan oleh seorang kriptoanalis yang berhasil memecahkan sebuah pesan terenkripsi. Dalam konteks kriptografi ada banyak jenis serangan yang dilakukan dengan tujuan tertentu oleh pihak-pihak yang bersangkutan. Tujuan tersebut antara lain seperti untuk mengetahui informasi rahasia, melakukan manipulasi data sehingga merugikan pihak tertentu, menghapus informasi tertentu dari suatu dokumen, serta berbagai tujuan lain-lainnya.

Oleh karena itulah kriptografi terus mengalami perkembangan dari waktu ke waktu. Karena kebutuhan dari keamanan data terus meningkat dari waktu ke waktu maka metode kriptografi terus dikembangkan. Message Authentication Code sendiri merupakan suatu metode pengamanan dalam kriptografi yang bertujuan untuk mengotentikasi isi dari suatu pesan, untuk mengetahui apakah suatu pesan tertentu merupakan pesan yang benar seperti yang di maksudkan oleh pengirim untuk diterima oleh pihak penerima.

Beberapa jenis dari attack pada suatu data adalah sebagai berikut ini:

A. Collision Attack

Collision attack adalah suatu metode attack yang dilakukan pada metode kriptografi fungsi hash yang bertujuan untuk mencari dua jenis kumpulan data yang memiliki nilai hash yang sama.

Bila suatu pesan dimodifikasi isinya dengan pesan lain yang memiliki nilai hash yang sama pihak penerima yang mengecek nilai Message Authentication Code dari pesan tersebut akan memperoleh nilai Message Authentication Code yang sama namun pesan yang salah. Sehingga terjadi kebingungan antara pihak pengirim dan penerima pesan. Ada dua metode dari collision attack ini yaitu collision attack dan prefix collision attack.

Teknik HMAC sangatlah rentan dengan metode attack ini. Karena tidak dilengkapi dengan suatu metode yang

dapatmencegah collision attack

B. Preimage Attack

Preimage attack adalah suatu metode attack dalam metode kriptografi yang menyerang fungsi hash untuk menemukan suatu pesan yang memiliki nilai hash yang spesifik.

Perbedaan metode ini dengan metode collision attack adalah dalam preimage attack pencarian dilakukan dengan focus pada fungsi hash untuk mencari pesan dengan nilai hash spesifik, sedangkan pada collision attack fokus hanya ada dalam pencarian data dengan fokus terhadap nilai hash tertentu

C. Birthday Attack

Birthday attack merupakan suatu metode attack dalam kriptografi yang memanfaatkan metode matematika dibalik birthday problem dan teori probabilitas. Metode ini merupakan salah satu metode yang dapat dimanfaatkan untuk melakukan collision attack, inti dari metode ini adalah mencari kemungkinan untuk menemukan dua informasi yang memiliki nilai hash yang sama.

D. Brute-force Attack

Dalam kriptografi, brute-force attack merupakan suatu teknik yang dapat digunakan untuk jenis kriptografi apapun. Dengan metode ini keseluruhan kemungkinan kunci akan dicari dan dicoba untuk digunakan untuk memecahkan enkripsi suatu pesan tertentu hingga ditemukan suatu kunci yang tepat.

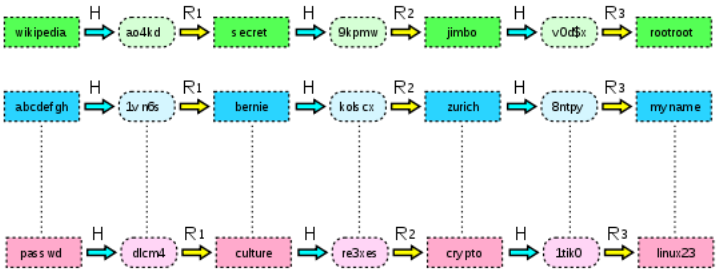
Seperti halnya dalam metode bruteforce pada umumnya dengan metode ini ada kemungkinan terburuk dimana seluruh kemungkinan yang ada harus dicek satu persatu. Efesiensi dan efektifitas dari metode ini akan berkurang sejumlah pertambahan jumlah variasi ruang yang harus dicari dari kemungkinan kunci yang ada.

E. Rainbow Table

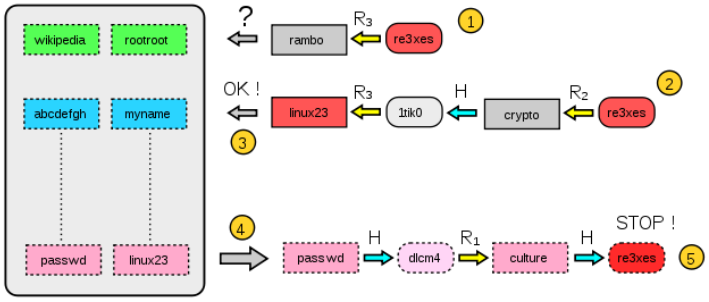
Rainbow table merupakan table perhitungan yang dapat digunakan untuk mengembalikan suatu fungsi hash, biasanya digunakan untuk memecahkan kunci dari nilai hash.

Seluruh rangkain dari semua kemungkinan kunci yang ada dalam fungsi hash di simpan dalam suatu table dan ketika ingin memecahkan suatu pesan tertentu yang perlu untuk dilakukan hanyalah penelusuran dari tebel tersebut sehingga hasil yang diinginkan dapat diperoleh.

Contoh dari rainbow table adalah sebagai berikut ini:



Contoh dari pemecahan dengan menggunakan rainbow table adalah:



1. Diawali dari hash (‘re3xes’), tahap ini mereduksi komputasi yang digunakan pada table dan mengecek apakah kunci tersedia dalam tabel
2. Bila gagal kunci tak ada dalam tabel, maka akan dihitung rangkaian dengan mereduksi 2 langkah terakhir.
3. Bila benar, maka kunci diambil dari awal rangkaian.
4. Pada tahap ini rangakain yang dibuat dibandingkan dengan tiap iterasi hash dengan hash yang dituju hingga diperoleh kunci yang benar.

F. Distinguishing Attack

Distinguishing attack adalah berbagai bentuk kriptanalisis dimana penyerang dapat mengekstrak sebagian informasi dari sejumlah data yang dienkripsi yang cukup untuk membedakannya dari data acak.

Dari segelintir informasi tersebut metode enkripsi yang digunakan dapat diketahui, bahkan terkadang dapat diperoleh kemungkinan kunci yang digunakan dalam membentuk pesan terenkripsi tersebut.

G. Side-Channel Attack

Side channel attack merupakan jenis attack berdasarkan informasi yang diperoleh dari implementasi fisik dari sebuah kriptosistem. Seperti mencari informasi timing, konsumsi daya, dam kebocoran elektromagnetis. Attack jenis ini membutuhkan kemampuan ataupun pengetahuan tentang keseluruhan informasi dari sistem dimana kriptografi diimplementasikan.

H. Chosen Plaintext Attack

Chosen Plaintext Attack adalah metode attack yang megasumsikan attacker mampu memilih plainteks yang dienkripsi dan memperoleh cipherteks yang bersangkutan. Tujuan dari attack ini adalah untuk memperoleh sebagian informasi untuk mengurangi keamanan dari enkripsi yang ada.

IV. ANALISIS DAN PERBANDINGAN METODE ATTACK TERHADAP ALGORITMA MESSAGE AUTHENTICATION CODE

Setelah membahas berbagai metode algoritma untuk menyusun Message Authentication Code dan berbagai untuk melakukan attack terhadap Message Authentication Code, pada bab ini akan dilakukan pembahasan tentang berbagai metode attack terhadap berbagai algoritma Message Authentication Code yang ada.

Pertama collision attack adalah sebuah metode yang sangat efektif apabila digunakan pada fungsi hash khususnya fungsi-fungsi hash sederhana yang tidak menangani pertahanan terhadap fungsi hash. Sehingga metode ini dapat digunakan untuk algoritma HMAC dan sejenisnya. Sedangkan untuk Message Authentication Code yang menggunakan algoritma universal hash sudah ada penanganan yang lebih baik dalam daya tahan terhadap kolisi, sehingga collision attack tak seefektif pada HMAC. Pada CBC-MAC dan algoritma MAC berdasarkan block-cipher lainnya attack jenis ini tidaklah berfungsi dengan baik.

Berikutnya adalah preimage attack. Attack jenis ini menyerang fungsi hash, sehingga untuk penyusunan algoritma dengan menggunakan block cipher attack jenis ini tak cocok untuk digunakan. Untuk HMAC karena kemungkinan fungsi hash penyusunnya dapat diketahui, teknik ini sangatlah efisien untuk digunakan, sedangkan untuk algoritma Message Authentication Code universal hash, metode ini lebih sulit untuk memecahkannya karena algoritma tersebut terdiri dari sekumpulan hash yang digunakan secara acak, sehingga pemilihan fungsi hash yang tepat lebih sulit dilakukan untuk memecahkan kunci penyusunnya.

Birthday attack, metode attack ini menggunakan teori peluang dalam menemukan dua pesan yang memiliki nilai hash yang sama. Karena masih membahas attack yang menangani hash, attack ini lebih cocok untuk pemecahan algoritma Message Authentication Code yang berdasarkan fungsi hash. Attack ini juga sering digunakan sebagai metode dari penerapan collision attack.

Brute-force attack, layaknya metode algoritma bruteforce, algoritma ini dapat digunakan dalam memecahkan masalah apapun namun memiliki efisiensi dan efektifitas yang tidak baik. Oleh karena itu attack jenis ini dapat diggunakan dalam melakukan pemecahan berbagai jenis algoritma Message Authentication Code yang ada, namun membutuhkan kinerja dan waktu lebih banyak juga.

Rainbow Table merupakan metode attack yang digunakan untuk mengembalikan fungsi hash, khususnya untuk menemukan kunci pembentuknya, sehingga attack jenis ini cocok untuk melakukan attack pada algoritma MAC yang dibuat berdasarkan fungsi hash.

Distinguishing attack merupakan metode yang dapat digunakan untuk memecahkan berbagai metode enkripsi, sehingga metode ini dapat digunakan untuk melakukan attack pada jenis algoritma MAC dengan berbagai bentukan. Namun kinerja attack ini ternilai untung-untungan karena berdasarkan pada nilai pembangkit acak pemecahnya.

Side channel attack,merupakan attack yang dilakukan pada perolehan informasi fisik dari suatu data. Teknik ini dapat diaplikasikan pada berbagai algoritma pembangkit MAC. Namun dibutuhkan keahlian dan pengetahuan khusus dalam menerapkannya.

V.KESIMPULAN

Berdasarkan analisis atas perbandingan yang dilakukan dalam pembuatan makalah ini, dapat ditarik beberapa kesimpulan:

1. Terdapat beberapa Algoritma Message Authentication Code yang dapat digunakan untuk menyusun suatu Message Authentication Code dan Algoritma Message Authentication Code yang tercepat dan memiliki tingkat keamanan yang baik adalah yang berdasarkan pada Universal Hashing seperti UMAC dan VMAC.

2. Terdapat berbagai metode attack yang dapat digunakan untuk melakukan attack pada Message Authentication Code yang masing-masingnya memiliki ciri khas yang tersendiri dan cocok digunakan untuk jenis algoritma Message Authentication Code yang dibuat dengan metode tertentu pula.

3. Untuk meningkatkan keamanan pada pengiriman pesan Message Authentication Code merupakan salah satu alternatif yang baik untuk digunakan, dan tersedia berbagai pilihan algoritma dengan tingkat keamanan dan kecepatan yang tertentu.

VI. UCAPAN TERIMA KASIH

Melalui bagian ini penulis ingin mengucapkan terima kasih kepada Tuhan YME atas segala berkat yang diberikan sehingga karya tulis ini dapat diselesaikan, kepada dosen Kriptografi pak Rinaldi Munir atas

bimbingannya dalam semester ini, kepada orangtua dan sahabat penulis yang telah banyak mendukung penulis dalam berbagai hal. Dan khususnya berbagai informasi tambahan dan sumber gambar yang diperoleh dari Wikipedia.

DAFTAR PUSTAKA

[1] Bishop,David,Introduction to Cryptography with Java Applet, Jones and Bartletts Publisher, 2003.
[2] Slide perkuliahan IF3058 Kriptografi oleh Rinaldi Munir.
[3] Makalah "FILES AUTHENTICATION CODE (FAC): PENGEMBANGAN MAC UNTUK DIGUNAKAN DALAM MENJAMIN INTEGRITAS BERKAS" oleh Raditya Arief, 2009.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Mei 2011
Ttd

Desfrianta Salmon Barus
13508107