PEMANFAATAN KRITOGRAFI AES

Adi Nugraha Setiadi - 13508062

Program Studi Teknik Teknik Informatika, Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10, Bandung
If18062@students.if.itb.ac.id

ABSTRAK

Perkembangan teknologi informasi berlangsung dengan sangat cepat, perpindahan informasi menjadi sangat tinggi. Dibutuhkan teknologi yang dapat menjaga keamanan informasi tersebut. Berbagai cara untuk melindungi data sampai saat ini sering dipakai adalah pengaman data menggunakan kriptografi. Hal tersebut memicu perkembangan teknologi kriptografi. Penelitian ini dilakukan dengan memulai pengumpulan litelatur untuk dianalisis, kemudian desain sistem meliputi flowchart dan data flow diagram selanjutnya perancangan form, pengkodean dan tahap terakhir pengujian aplikasi yang dilakukan dengan metode black-box test. Hasil penelitian ini adalah suatu aplikasi enkripsi dan dekripsi data dengan menggunakan algoritma kriptografi Rinjdael. Pengujian program telah dilakukan dan dapat disimpulkan bahwa aplikasi enkripsi dan dekripsi data dapat dilakukan untuk semua format file.

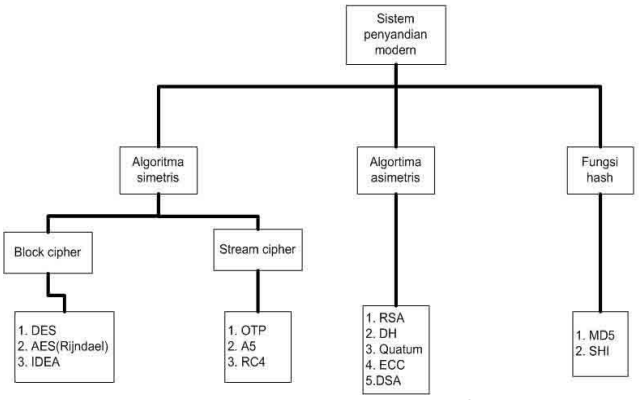
Kata kunci: *Kriptografi, Rijndael, Enkripsi File.*

1. PENDAHULUAN

Kriptograpi adalah ilmu dan seni untuk menjaga kerahasiaan informasi atau berita. kriptograpi merupakan salah satu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi. bedasarkan kunci kriptograpi dikelompokan menjadi 2 :

a) Asimetris
   - Knapsack
   - RSA – Rivert-Shamir-Adelman
   - Diffie-Hellman

b) Simetris
   - DES – Data Encription Standard
   - Blowfish
   - Twofish
   - MARS
   - IDEA
   - 3DES – DES diaplikasikan 3 kali
   - AES – Advanced Encription Standard, yang bernama asli Rijndael



Gambar 1. Hirarki Kriptografi

Pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan. Untuk memenuhi hal tersebut, dilakukan proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dikirimkan. Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

AES (*Advanced Encryption Standard*) adalah lanjutan dari algoritma enkripsi standar DES (Data Encryption Standard) yang masa berlakunya dianggap telah usai karena faktor keamanan. Kecepatan komputer yang sangat pesat dianggap sangat membahayakan DES, sehingga pada tanggal 2 Maret tahun 2001 ditetapkanlah algoritma baru Rijndael sebagai AES.Rijndael dipilih dari 15 algoritma yang didaftarkan oleh berbagai kalangan industri dan akademik di seluruh dunia ke NIST (National Institute of Standard and Technology), Amerika.

AES memiliki blok masukan dan keluaran serta kunci 128 bit. Untuk tingkat keamanan yang lebih tinggi, Secara de-fakto, hanya ada dua varian AES, yaitu AES-128 dan AES-256, karena akan sangat jarang pengguna

menggunakan kunci yang panjangnya 192 bit. Setiap masukan 128 bit *plaintext* dimasukkan ke dalam *state* yang berbentuk bujursangkar berukuran 4×4 byte. State ini di-XOR dengan key dan selanjutnya diolah 10 kali dengan subtitusi-transformasi linear-Addkey. Dan di akhir diperoleh ciphertext.

2. METODE

Seperti pada *DES*, *Rijndael* menggunakan substitusi dan permutasi, dan sejumlah putaran. Untuk setiap putarannya, *Rijndael* menggunakan kunci yang berbeda. Kunci setiap putaran disebut *round key*. Tetapi tidak seperti *DES* yang berorientasi bit, *Rijndael* beroperasi dalam orientasi *byte* sehingga memungkinkan untuk implementasi algoritma yang efisien ke dalam *software* dan *hardware* [1]

Terdapat 3 parameter pada algoritma *Rijndael* yaitu:

1. Plaintekx : merupakan array yang berukuran 16 byte, yang berisi data masukan.
2. Cipherteks : merupakan array yang berukuran 16 byte, yang berisi hasil enkripsi.
3. Key : merupakan array berukuran 16 byte, yang berisi kunci *ciphering* (disebut juga *cipher key*)

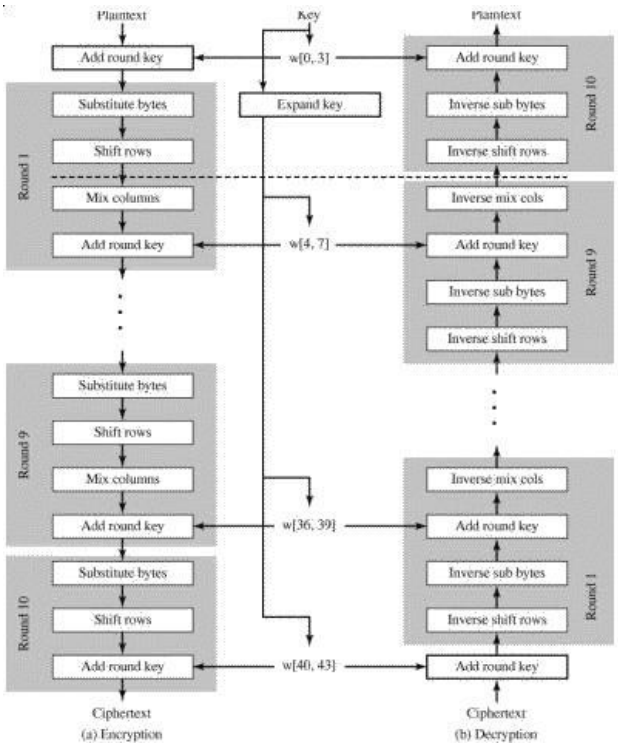
Dengan 16 *byte*, maka baik blok data dan kunci yang berukuran 128-bit dapat disimpan di dalam ketiga array tersebut (128 = 16 x 8). Selama kalkulasi plainteks menjadi cipherteks, status sekarang dari data disimpan di dalam *array of byte* dua dimensi, state, yang berukuran NROWS x NCOLS. Elemen *array* state diacu sebagai $S[r,c]$, dengan $0 \le r < 4$ dan $0 \le c < Nc$ (Nc adalah panjang blok dibagi 32). Pada AES, $Nc = 128/32 = 4$.

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Input yang telah dikopikan ke dalam state pada awal proses enkripsi akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi subBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns

Operasi enkripsi Rijndael dapat dinyantakan dengan kode semu (*pseudocode*) berikut ini:
Pseudocode Cipher Rijndael:

```
Cipher(byte in[], byte out[], word W[])
  /*Nama fungsi*/
Begin
In = 4 * Nb
Out = 4 * Nb
W = Nb * (Nr +1)
Byte state[4,Nb]
State = In /* Memasukkan Input ke
state*/
AddRoundKey(state,W)
For round=1 step 1 to Nr-1 /*proses
yang berlaku untuk semua ronde kecuali
ronde terakir*/
SubBytes(state)
shiftRows(state)
MixColumns(state)
AddRoundKey(state, w + round * Nb)
End for
SubBytes(state) /*proses yang berlaku
khusus untuk ronde terakhir*/
ShiftRows(state)
AddRoundKey(state, w+round * Nb) /*
Mengirimkan keluaran ke out */
Out = state
End
```

Pseudocode di atas, dapat diketahui enkripsi dilakukan dengan fungsi *cipher* yang memiliki parameter masukan in – 16 byte dengan Nb adalah panjang blok, keluaran out = 16 byte dan array 1 dimensi w = 44 byte untuk Rijndael-128 dengan Nr adalah jumlah ronde.

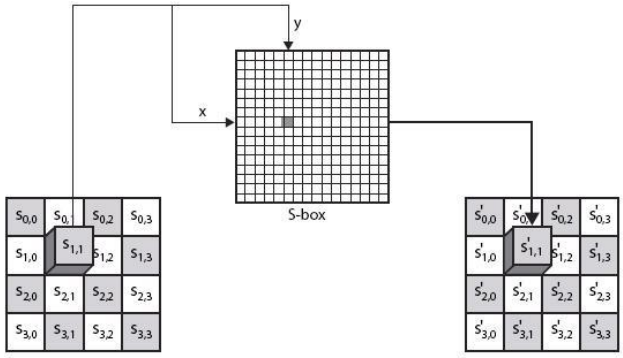


Gambar 2. Gambaran umum Enkripsi Dan Dekripsi algoritma kriptografi Rijndael

2.1 Sub-Byte

Adalah transformasi byte dimana setiap elemen pada *state* akan dipetakan dengan menggunakan sebuah tabel substitusi (S-Box). Hasil yang didapat dari pemetaan

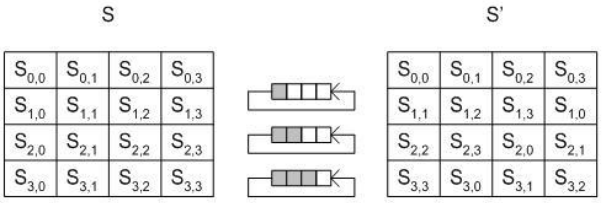
dengan menggunakan tabel S-Box ini sebenarnya adalah hasil dari dua proses transformasi *bytes*



Gambar 3. Sub-Byte

2.2 Shift-Rows

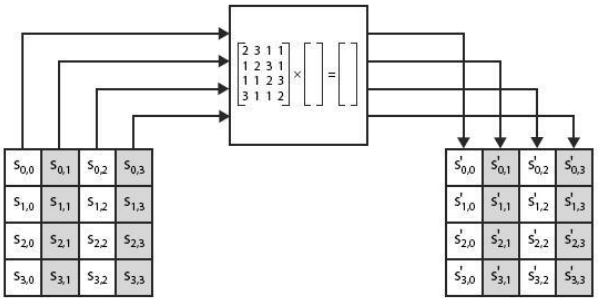
Transformasi Shiftrows pada dasarnya adalah proses pergeseran bit, yaitu bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit). Transformasi ini diterapkan pada baris 2, baris 3, dan baris 4. Baris 2 akan mengalami pergeseran bit sebanyak satu kali, sedangkan baris 3 dan baris 4 masing-masing mengalami pergeseran bit sebanyak dua kali dan tiga kali. Berikut ini adalah gambar transformasi *ShiftRows*.



Gambar 4. Shift-Row

2.3 Mix-Columns

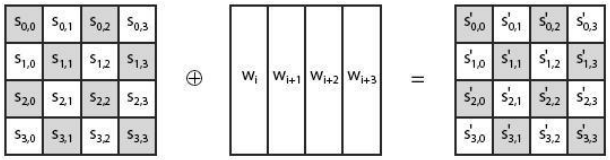
Mixolumns mengoperasikan setiap elemen yang berada dalam satu kolom pada *state*. Elemen pada kolom dikalikan dengan suatu polinomial tetap $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.



Gambar 5. Mix-Columns

2.4 Add Round Key

Proses AddRoundKey, sebuah *round key* ditambahkan pada *state* dengan operasi bitwise XOR. Setiap *round key* terdiri dari *Nb word*, tiap *word* tersebut akan dijumlahkan dengan *word* atau kolom yang bersesuaian dari *state*



Gambar 6. Add Round Key

Keempat proses tersebut akan di iterasi selama 10 kali. maka akan mendapatkan chiperkey hasil dari enkripsi.

3. Aplikasi

Kriptografi AES dapat memberikan tingkat keamanan yang tinggi bagi protokol yang digunakan. Beberapa contoh aplikasi yang memanfaatkan kriptografi AES dapat dibaca di bawah.

3.1 Perangkat Lunak untuk Keamanan Informasi pada Email

Penyadapan informasi dapat terjadi pada saat melakukan proses pertukaran informasi melalui e-mail. Proses penyandian diperlukan untuk mencegah terjadinya penyadapan informasi, karena proses tersebut dapat meningkatkan keamanan informasi. Kriptografi menyediakan beberapa layanan yang mendukung untuk meningkatkan keamanan informasi, yaitu: otentikasi (*authentication*), mencegah penyangkalan (*non-repudiation*), dan menjaga kerahasiaan (*confidentiality*).

Penelitian ini difokuskan untuk menjaga kerahasiaan informasi dengan proses penyandian dan mencegah penyangkalan oleh pengirim informasi menggunakan proses tanda tangan digital.

Pada penelitian ini algoritma AES digunakan untuk menyandikan (mengenkripsi) file lampiran yang dikirim melalui e-mail. Algoritma AES memiliki tingkat keamanan yang tinggi karena memiliki 3 tipe kunci yang berbeda (AES-128, AES-192 dan AES-256) dan setiap putaran proses akan menghasilkan kunci (*subkey*) yang berbeda. Sedangkan untuk memudahkan proses distribusi kunci yang digunakan pada algoritma AES dan tanda tangan digital maka digunakan algoritma RSA. Kelebihan dari algoritma RSA adalah faktor keamanannya karena didasarkan pada kesulitan untuk memfaktorkan bilangan besar modulus n menjadi faktor-faktor primanya.

Langkah ini bertujuan merancang perangkat lunak yaitu CARA (*Cryptosystem with AES and RSA Algorithm*) yang

dapat digunakan untuk menjaga kerahasiaan informasi yang dikirimkan melalui e-mail sekaligus dapat mencegah penyangkalan oleh pengirimnya. Hasil penelitian ini akan dapat memberi rasa aman bagi pengirim dan penerima informasi.

3.2 Meningkatkan Keamanan Layanan SMS Banking dengan AES

SMS Banking merupakan suatu mekanisme yang disediakan oleh bank bagi para nasabahnya untuk melakukan transaksi perbankan hanya dengan menggunakan layanan SMS Layanan ini ditujukan agar para nasabah bank dapat melakukan transaksi tanpa terkendala dengan masalah ruang dan waktu. Dengan adanya layanan SMS Banking transaksi-transaksi perbankan dapat segera dilakukan sehingga ketersampaian hasil transaksi dari pengirim kepada pihak penerima menjadi lebih cepat.

Advanced Encryption Standard (AES) dengan *One Time Password* merupakan suatu metode enkripsi alternatif yang dapat digunakan untuk menjaga kerahasiaan layanan SMS Banking**.** Metode ini memungkinkan terjadinya enkripsi pesan antara telepon seluler dengan server bank yang dituju (*end-to-end communication*). Dengan memanfaatkan metode ini, layanan SMS Banking dapat menjadi lebih aman karena algoritma enkripsi yang digunakan cukup tangguh dan kunci yang dipakai sukar dipecahkan.

Masalah-masalah yang terdapat pada SMS Banking disebabkan pesan SMS yang belum sepenuhnya aman. Masih banyak terdapat kelemahan pada arsitektur GSM yang dapat mengakibatkan *security shortfalls* pada SMS Banking. Salah satu contoh kelemahan GSM tersebut adalah proses enkripsi pesan SMS yang hanya terjadi antara telepon seluler dengan BTS (*Base Transceiver Station*). Kelemahan-kelemahan yang dimiliki oleh arsitektur GSM tersebut dapat ditangani menggunakan metode enkripsi *Advanced Encryption Standard* (AES) dengan *One Time Password* untuk menjaga kerahasiaan layanan SMS Banking yang dilakukan. Metode ini akan menyediakan enkripsi pesan antara telepon seluler dengan server bank yang dituju sehingga faktor keamanan pada layanan SMS Banking dapat meningkat.

Penggunaan *One Time Password* akan memberikan tingkat keamanan yang lebih tinggi bagi protokol yang digunakan. Apabila seorang *attacker* telah mengetahui PIN seorang nasabah dan *sequence number* seorang *user, attacker* tersebut tetap akan membutuhkan *One Time Password* untuk mengenkripsi pesan supaya server bank yang dituju dapat menjalankan transaksi perbankan yang diminta.

3.3 Enkripsi Video Menggunakan AES pada Video Streaming

Saat ini teknologi multimedia khususnya aplikasi video telah menjadi bagian dalam kehidupan sehari-hari. Aplikasi video terdistribusi seperti video-on-demand, video broadcast dan video conference harus dilengkapi dengan suatu sistem transmisi yang aman. Salah satu cara untuk mengamankan aplikasi distributed video seperti di atas adalah melakukan enkripsi pada data video dengan menggunakan algoritma AES atau DES, sehingga pihak lain yang tidak berhak tidak dapat melihat isi video yang asli meskipun data video berhasil diakses. Dalam tugas akhir ini, kami mendesain dan mengimplementasikan enkripsi video menggunakan algoritma Advanced Encryption Standard (AES) pada video streaming. Enkripsi akan diterapkan pada bit-bit piksel dari frame video, sehingga bit-bit piksel tesebut akan berubah Untuk menjaga keamanan distribusi kunci, maka diterapkan algoritma pertukaran kunci Diffie-Hellman. Transmitter dan receiver melakukan pertukaran kunci sehingga memiliki kunci sesi yang sama yang digunakan untuk enkripsi dan dekripsi.

3.4 Keamanan Aplikasi VoIP

Salah satu aplikasi VoIP yang memanfaatkan metode enkripsi *Advanced Ecryption Standard* adalah Skype. Skype adalah [[*software*]] aplikasi komunikasi suara berbasis IP melalui internet antara sesama pengguna Skype. Pada saat menggunakan Skype maka pengguna Skype yang sedang online akan mencari pengguna Skype lainnya lalu mulai membangun jaringan untuk menemukan pengguna-pengguna lainnya. Skype memiliki berbagai macam fitur yang dapat memudahkan penggunanya.

Skype menggunakan protokol HTTP untuk berkomunikasi dengan Skype server untuk otentikasi username/password dan registrasi dengan Skype directory server. Versi modifikasi dari protokol HTTP digunakan untuk berkomunikasi dengan sesama Skype client. Keuntungan yang dimiliki aplikasi ini adalah tersedianya layanan keamanan dalam pentransmisian data yang berupa suara. Skype menggunakan AES 256-bit untuk proses enkripsi dengan total probabilitas percobaan kunci (brute-force attack) sebanyak 1,1 x E-77 kali, sedangkan untuk proses pertukaran kunci (key exchange) simetriknya menggunakan RSA 1024-bit. Public key pengguna akan disertifikasi oleh Skype server pada saat *login* dengan menggunakan sertifikat RSA 1536 atau 2048-bit. Skype secara otomatis akan mengenkripsi semua data sebelum ditransmisikan melalui internet.

3.5 BitLocker Drive Enctyption

Sebuah fitur enkripsi satu cakram penuh yang biasanya terdapat di system operasi (contohnya: Microsoft Windows Vista dan Windows Server 2008) didesain untuk melindungi data dengan melakukan enkripsi terhadap keseluruhan partisi. Secara *default*, BitLocker Drive Encryption menggunakan

algoritma AES dalam mode *Code Block Chaining* (CBC) dengan panjang kunci 128-bit, yang digabungkan dengan *Elephant diffuser* untuk meningkatkan keamanannya.

BitLocker Drive Encryption hanya tersedia di dalam sistem operasi Windows Vista Ultimate Edition dan Windows Vista Enterprise Edition, dan tidak ada pada edisi-edisi Windows Vista lainnya. Pada saat WinHEC2006, Microsoft mendemonstrasikan versi prarilis dari Windows Server 2008 yang mengandung dukungan terhadap partisi berisi data yang diamankan oleh BitLocker selain tentunya partisi berisi sistem operasi.

Berbeda dengan namanya, BitLocker Drive Encryption sebenarnya hanya merupakan sistem enkripsi terhadap sebuah volume/partisi saja. Sebuah volume mungkin bisa berupa satu hard drive, sebuah partisi, atau lebih dari satu buah hard drive. Dengan menggunakan alat bantu yang bersifat command-line, BitLocker dapat digunakan untuk mengamankan volume yang digunakan oleh sistem operasi, tetapi juga volume yang tidak dapat dienkripsi dengan menggunakan antarmuka grafisnya. Sistem operasi masa depan (mungkin Windows Server 2008) diharapkan dapat mendukung enkripsi terhadap volume tambahan selain volume booting dengan menggunakan antarmuka grafisnya. Selain itu, ketika diaktifkan, TPM dan BitLocker juga menjamin integritas jalur booting yang digunakan (BIOS, Master Boot Record, boot sector dan lain-lain) agar mencegah serangan fisik secara offline (offline attack), virus yang menyerang boot sector dan lain-lain.

Agar BitLocker dapat beroperasi, hard disk paling tidak harus memiliki dua buah volume yang harus diformat dengan menggunakan sistem berkas NTFS, yang dinamakan dengan "System Volume" (sebuah volume di mana sistem operasi mampu melakukan booting yang memiliki kapasitas paling tidak 1.5 Gigabyte) dan juga "Boot Volume", yang mengandung Windows Vista. Perlu dicatat bahwa System Volume tidak dienkripsi, sehingga tidak boleh menyimpan data sensitif dan rahasia di sana. Tidak seperti versi Windows sebelumnya, alat bantu command-line diskpart bawaan Windows Vista mencakup kemampuan untuk mengecilkan ukuran volume NTFS sehingga system volume yang ditujukan untuk BitLocker pun dapat dibuat, tanpa harus melakukan repartisi hard drive.

Hanya volume yang berisi sistem operasi saja yang bisa dienkripsi dengan menggunakan antarmuka grafis. Akan tetapi, volume tambahan dapat dienkripsi dengan menggunakan skrip Windows Scripting Host,manage-bde.wsf. Fitur Encrypting File System (EFS) tetap disarankan sebagai solusi untuk enkripsi secara realtime dalam partisi NTFS. Penggunaan EFS juga sangat disarankan selain tentunya BitLocker, karena proteksi yang dilakukan oleh BitLocker akan berakhir mana kala kernel sistem operasi telah dimuat. Penggunaan dua fitur tersebut (BitLocker dan EFS) akan mampu melindungi beberapa jenis serangan.

Dalam lingkungan domain, BitLocker mendukung pembagian kunci terhadap dengan menggunakan Active Directory, selain tentunya antarmuka Windows Management Instrumentation (WMI) yang digunakan untuk melakukan administrasi jarak jauh terhadap fitur tersebut. Sebagai contoh penggunaan antarmuka WMI adalah skrip manage-bde.wsf (yang diletakkan di dalam \%WINDIR%\System32\) yang dapat digunakan untuk mengatur konfigurasi BitLocker dari command-line.

4. KESIMPULAN

Kesimpulan yang dapat dimbil dari studi dan implementasi AES adalah:

1. Advanced Encryption Standard (AES) merupakan salah satu solusi yang baik untuk mengatasi masalah keamanan dan kerahasiaan data yang pada umumnya diterapkan dalam pengiriman dan penyimpanan data melalui media elektronik.
2. CARA (Cryptosystem with AES and RSA Algorithm) dapat digunakan untuk menjaga kerahasiaan informasi yang dikirimkan melalui e-mail sekaligus dapat mencegah penyangkalan oleh pengirimnya.
3. Advanced Encryption Standard (AES) dengan One Time Password merupakan salah satu metode alternatif yang dapat digunakan untuk meningkatkan keamanan layanan SMS Banking.
4. Untuk menjaga privacy dalam VoIP, AES juga diterapkan, dalam hal ini menggunakan AES 256-bit untuk proses enkripsi dengan total probabilitas percobaan kunci (brute-force attack) sebanyak 1,1 x E-77 kali.

REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF2151 Matematika Diskrit* (*edisi keempat*), Institut Teknologi Bandung, 2004.

[2] Public Key Cryptography Standards (PKCS), No.1, RSA Encryption standard, http://www.rsasecurity.com/rsalabs/

[3] http://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingles2004.swf

[4] http://id.wikipedia.org/wiki/Voice_over_IP