LOFIAN: Jurnal Teknologi Informasi dan Komunikasi
Vol. 1, No. 1, September 2021, Halaman 1-6
Submited: 02 Agustus 2021; Accepted: 18 September 2021; Published: 20 September 2021
e-ISSN: 2798-9593
p-ISSN: 2798-9836

Perancangan Simulator Interlock Protocol saat Serangan Man-in-the-Middle-Attack pada Kriptografi Kunci Publik RSA

Maranata Pasaribu[1], Marice Hotnauli Simbolon[2]

[1,2]*AMIK Medan Business Polytechnic*
Jl. Jamin Ginting No. 285-287, Padang Bulan, Medan Baru, Kota Medan, Sumatera Utara, Indonesia - 20155

[1]*maranata@amikmbp.ac.id*, [2]*simbolonice@gmail.com*

DOI: xx.xxxx/j.ccs.xxxx.xx.xxx

Abstrak

Dalam proses transmisi data, walaupun data telah dienkripsi, namun terdapat kemungkinan bahwa data tersebut dapat dimiliki oleh orang lain. Salah satu kemungkinan tersebut adalah dengan terjadinya penyadapan media komunikasi yang digunakan oleh kedua orang yang sedang berkomunikasi tersebut. Problema man-in-the-middle-attack ini dapat dicegah dengan menggunakan interlock protocol. Algoritma inti dari protokol ini yaitu mengirimkan 2 bagian pesan terenkripsi. Bagian pertama dapat berupa hasil dari fungsi hash satu arah (one way hash function) dari pesan tersebut dan bagian kedua berupa pesan terenkripsi itu sendiri. Penelitian ini akan merancang perangkat lunak simulasi yang dapat menjelaskan proses kerja dari man-in-the-middle-attack dalam menyadap dan mengubah pesan, menjelaskan proses kerja interlock protocol untuk mengatasi problema Man-In-The-Middle-Attack. Setelah menyelesaikan perangkat lunak simulasi, peneliti menarik kesimpulan: Dengan menggunakan interlock protocol, walaupun kunci publik pihak penerima dan pengirim didapatkan dan diganti oleh penyadap, tetapi penyadap tidak dapat menjalankan prosedur man-in-the-middle-attack untuk melihat dan mengubah pesan. Hal ini dikarenakan pesan terenkripsi terbagi menjadi dua bagian pada variasi pertama dan terdapat fungsi hash untuk memverifikasi keaslian pesan pada variasi kedua.

Kata Kunci: Kriptografi, Rivest-Shamir-Adleman, Protokol Interlock, Enkripsi, Dekripsi.

1. Pendahuluan

Dalam proses transmisi data, walaupun data telah dienkripsi, namun terdapat kemungkinan bahwa data tersebut dapat dimiliki oleh orang lain. Salah satu kemungkinan tersebut adalah dengan terjadinya penyadapan media komunikasi yang digunakan oleh kedua orang yang sedang berkomunikasi tersebut. Hal inilah yang disebut dengan man-in-the-middle-attack. Dalam keadaan ini, orang yang menyadap berada di antara kedua orang yang sedang berkomunikasi. Data-data yang dikirimkan oleh orang yang sedang berkomunikasi satu sama lain selalu melalui orang yang menyadap tersebut, sehingga orang yang menyadap tersebut dapat mengetahui semua informasi yang dikirimkan satu sama lain. Keadaan ini muncul karena kedua orang yang sedang berkomunikasi tersebut tidak dapat mem-verifikasi status dari orang yang berkomunikasi dengannya tersebut, dengan mengambil asumsi bahwa proses penyadapan tersebut tidak menyebabkan gangguan dalam jaringan.

Problema man-in-the-middle-attack ini dapat dicegah dengan menggunakan interlock protocol. Algoritma inti dari protokol ini yaitu mengirimkan 2 bagian pesan terenkripsi. Bagian pertama dapat berupa hasil dari fungsi hash satu arah (one way hash function) dari pesan tersebut dan bagian kedua berupa pesan terenkripsi itu sendiri. Hal ini menyebabkan orang yang menyadap tersebut tidak dapat mendekripsi pesan pertama dengan menggunakan kunci privatnya. Ia hanya dapat membuat sebuah pesan baru dan mengirimkannya kepada orang yang akan menerima pesan tersebut.

Maka dari pemapanan di atas, peneliti akan merancang perangkat lunak simulasi yang dapat menjelaskan proses kerja dari man-in-the-middle-attack dalam menyadap dan mengubah pesan, menjelaskan proses kerja interlock protocol untuk mengatasi problema Man-In-The-Middle-Attack, menampilkan algoritma dari sistem kriptografi kunci publik metode RSA. Dengan harapan perangkat lunak simulasi yang dibangun dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar terutama untuk mata kuliah Kriptografi.

LOFIAN: Jurnal Teknologi Informasi dan Komunikasi e-ISSN: 2798-9593
Vol. 1, No. 1, September 2021, Halaman 1-6 p-ISSN: 2798-9836
Submited: 02 Agustus 2021; Accepted: 18 September 2021; Published: 20 September 2021

2. Landasan Teori

Dalam penelitian ini, peneliti akan memaparkan beberapa landasan teori yang digunakan dalam penelitian ini, antara lain:

2.1. Kriptografi

Kriptografi (Cryptography) berasal dari bahasa Yunani yaitu dari kata 'crypto' dan 'graphia' yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut cryptology. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

Menurut Stalling, ada beberapa tuntutan yang terkait dengan isu keamanan data, yaitu:

1. *Confidentiality*. Menjamin bahwa data-data tersebut hanya bisa diakses oleh pihak-pihak tertentu saja.
2. *Authentication*. Baik pada saat mengirim atau menerima informasi, kedua belah pihak perlu mengetahui bahwa pengirim dari pesan tersebut adalah orang yang sebenarnya seperti yang diklaim.
3. *Integrity*. Tuntutan ini berhubungan dengan jaminan setiap pesan yang dikirim pasti sampai pada penerimanya tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya, dan ditambahkan.
4. *Nonrepudiation*. Mencegah pengirim maupun penerima mengingkari bahwa mereka telah mengirimkan atau menerima suatu pesan/informasi. Jika sebuah pesan dikirim, penerima dapat membuktikan bahwa pesan tersebut memang dikirim oleh pengirim yang tertera. Sebaliknya, jika sebuah pesan diterima, pengirim dapat membuktikan bahwa pesannya telah diterima oleh pihak yang ditujunya.
5. *Access Control*. Membatasi sumber-sumber data hanya kepada orang-orang tertentu.
6. *Availability*. Jika diperlukan setiap saat semua informasi pada sistem komputer harus tersedia bagi semua pihak yang berhak atas informasi tersebut.

Dari keenam aspek keamanan data tersebut, empat diantaranya dapat diatasi dengan menggunakan cryptography yaitu confidentiality, integrity, authentication, dan nonrepudiation.

2.2. Algoritma Rivest-Shamir-Adleman (RSA)

RSA merupakan salah satu teknik enkripsi dan dekripsi dengan menggunakan dua buah kunci. Kunci-kunci tersebut diperoleh dari hasil perhitungan eksponensial, perkalian, pembagian, penjumlahan dan pengurangan. Perhitungan dilakukan terhadap dua buah bilangan prima.

Walaupun RSA cenderung aman bukan berarti tidak bisa dilakukan "attack" terhadap enkripsinya. Didukung perkembangan hardware komputer yang semakin cepat maka semakin terbuka kemungkinan memecahkan enkripsi RSA. Pada tahun 1977 Rivest, Shamir dan Adleman mempublikasikan tantangan memecahkan enkripsi RSA yang memakai 129 digit bilangan bulat. Tantangan ini diharapkan bisa bertahan dari "attack" untuk waktu yang lama. Tetapi pada tahun 1994 tantangan ini dipecahkan dengan menggunakan komputer yang kekuatan komputasinya berimbang dengan komputer untuk membuat film animasi "Toy Story" (kumpulan, 87 unit komputer dual prosesor, 30 unit komputer empat procesor, 100Mhz SPARCstation).

Secara garis besar, algoritma kunci publik RSA dapat dijabarkan sebagai berikut:

```
Key generation:

1. Hasilkan dua buah integer prima besar, p dan q.
   Untuk memperoleh tingkat keamanan yang tinggi
   pilih p  dan q yang berukuran  besar, misalnya
   1024 bit.
2. Hitung m = (p-1)*(q-1).
3. Hitung n = p*q
4. Pilih e yg relatif prima terhadap m.
   e relatif prima thd m artinya faktor pembagi
   terbesar keduanya adalah 1, secara matematis
   disebut gcd(e,m) = 1. Untuk mencarinya dapat
   digunakan algoritma Euclid.
5. Cari d, sehingga e*d = 1 mod (m), atau
   d = e^-1 * mod (m). Untuk mencarinya, dapat
   digunakan algoritma extended Euclid.
6. Kunci publik : e, n
   Kunci private : d, n
```

Gbr. 1. Key Generation

```
Public key encryption & decryption


B mengenkripsi message M untuk A

Yg harus dilakukan B :
  1. Ambil kunci publik A yg otentik (n, e)
  2. Representasikan message sbg integer M dalam
     interval [0,n-1]
  3. Hitung C = M ^ e (mod n)
  4. Kirim C ke A

Untuk mendekripsi, A melakukan :
  Gunakan kunci pribadi d untuk menghasilkan M =
  C ^ d  (mod n)
```

Gbr. 2. Public Key Encrytion & Description

2.3. Interlock Protocol

Problema man-in-the-middle-attack dapat atasi dengan menggunakan interlock protocol. Interlock

LOFIAN: Jurnal Teknologi Informasi dan Komunikasi
Vol. 1, No. 1, September 2021, Halaman 1-6
Submited: 02 Agustus 2021; Accepted: 18 September 2021; Published: 20 September 2021
e-ISSN: 2798-9593
p-ISSN: 2798-9836

protocol ini diciptakan oleh Ron Rivest dan Adi Shamir. Algoritma inti dari protokol ini yaitu protokol ini mengirimkan 2 bagian pesan terenkripsi.

Bagian pertama dapat berupa hasil dari fungsi hash satu arah (one way hash function) dari pesan tersebut dan bagian kedua berupa pesan terenkripsi itu sendiri.

Hal ini menyebabkan orang yang menyadap tersebut tidak dapat mendekripsi pesan pertama dengan menggunakan kunci privatnya. Ia hanya dapat membuat sebuah pesan baru dan mengirimkannya kepada orang yang akan menerima pesan tersebut.

3. Metodologi Penelitian

Adapun lokasi penelitian ini berada transmisi data yang di enkripsi antar pengirim dan penerima serta juga di pihak ketiga yang melakukan penyadapan.

3.1. Pengumpulan Data

Adapun metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Studi lapangan

   Degan metode ini peneliti mengamati bagaimana data ditransmisikan dari pengirim dan penerima serta penyadap.
2. Studi Kepustakaan

   Dengan melakukan studi pustaka, peneliti mendapatkan data-data yang bersifat teori ilmiah yang dipergunakan sebagai dasar dalam melakukan penulisan dan analisa terhadap kendala-kendala yang ada sehingga kendala tersebut dapat diselesaikan dengan baik.

3.2. Langkah dalam pembuatan perangkat lunak

Terdapat serangkaian langkah-langkah yang dilakukan secara terencana dan sistematis guna mendapatkan penecahan masalah atau menjawab pertanyaan-pertanyaan dari penelitian.

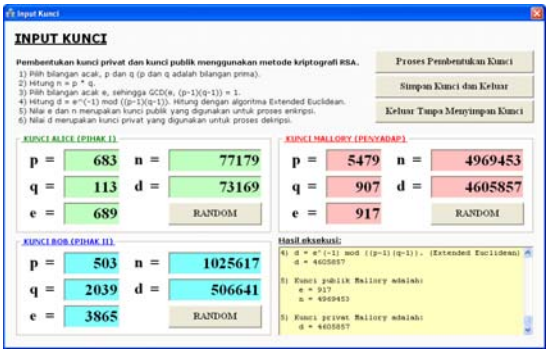
1. Membaca dan mempelajari buku-buku Kriptogafi terutama yang berhubungan dengan man-in-the-middle-attack ini dan interlock protocol.
2. Mempelajari teknik-teknik dasar pemrograman.
3. Mempelajari proses kerja dari problema man-in-the-middle-attack ini dan proses pencegahannya dengan menggunakan interlock protocol.
4. Mempelajari proses kerja dari algoritma RSA dan fungsi SHA-1 serta algoritma-algoritma pendukung yang digunakan.
5. Merancang algoritma dari RSA dan fungsi SHA-1 serta algoritma-algoritma pendukung lainnya.
6. Merancang interface dari perangkat lunak simulasi.
7. Merancang perangkat lunak simulasi yang mampu menjelaskan prosedur kerja dari problema man-in-the-middle-attack dan solusi untuk mengatasinya dengan menggunakan interlock protocol.
8. Menguji perangkat lunak dan memperbaiki kesalahan yang timbul.

4. Hasil dan Pembahasan

Penelitian ini selanjutnya mendapatkan hasil dan akan dibahas sebagai berikut:

4.1. Hasil

Misalkan, diambil contoh input kunci seperti terlihat pada Gbr. 3. berikut.



Gbr. 3. Contoh input kunci

Hasil eksekusi proses pembentukan kunci adalah sebagai berikut:

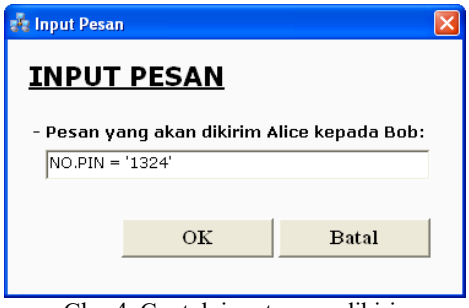
1. Perhitungan Kunci Alice
   - p = 683, q = 113
   - n = p * q
     n = 683 * 113
     n = 77179
   - e = 689, GCD(e,(p-1)(q-1)) = 1.
   - d = e^(-1) mod ((p-1)(q-1)). (Extended Euclidean)
     d = 73169
   - Kunci publik Alice adalah:
     e = 689
     n = 77179
   - Kunci privat Alice adalah:
     d = 73169
2. Perhitungan Kunci Bob

e-ISSN: 2798-9593
p-ISSN: 2798-9836

- p = 503, q = 2039
- n = p * q
  n = 503 * 2039
  n = 1025617
- e = 3865, GCD(e,(p-1)(q-1)) = 1.
- d = e^(-1) mod ((p-1)(q-1)). (Extended Euclidean)
  d = 506641
- Kunci publik Bob adalah:
  e = 3865
  n = 1025617
- Kunci privat Bob adalah:
  d = 506641

3. Perhitungan Kunci Mallory
   - p = 5479, q = 907
   - n = p * q
     n = 5479 * 907
     n = 4969453
   - e = 917, GCD(e,(p-1)(q-1)) = 1.
   - d = e^(-1) mod ((p-1)(q-1)). (Extended Euclidean)
     d = 4605857
   - Kunci publik Mallory adalah:
     e = 917
     n = 4969453
   - Kunci privat Mallory adalah:
     d = 4605857

Misalkan, Alice mengirimkan pesan kepada Bob dan Mallory mengubah pesan Alice. Contoh input pesan terlihat pada Gbr. 4 dan 5. berikut.



Gbr. 4. Contoh input pesan dikirim

Gbr 5. Contoh input pesan (ubah) dikirim

Tampilan proses simulasi terlihat pada Gbr. 6. berikut.

Gbr. 6. Contoh tampilan Form Utama

Hasil eksekusi proses man-in-the-middle-attack adalah sebagai berikut:

1. ALICE mengirimkan pesan kepada BOB dan dienkripsi dengan menggunakan kunci publik "BOB"

Pesan = 'NO.PIN = '1324"

Ubah pesan menjadi biner:
01001110010011110010111001010000010010010100111000100000001111010010000000010011100110001001100100111001100100011010000100111
Ubah setiap 3 bit biner menjadi bentuk desimal:
234474562404451610036440116304631443204 7

Masukkan setiap 4 digit desimal (m) ke fungsi enkripsi: c = (m ^ e) mod n

(Gunakan kunci publik Mallory)
c = (2344 ^ 917) mod 4969453 = 2401144
c = (7456 ^ 917) mod 4969453 = 1679420
c = (2404 ^ 917) mod 4969453 = 2967120
c = (4516 ^ 917) mod 4969453 = 2054777

Submited: 02 Agustus 2021; Accepted: 18 September 2021; Published: 20 September 2021

c = (1003 ^ 917) mod 4969453 = 4491255
c = (6440 ^ 917) mod 4969453 = 4898261
c = (1163 ^ 917) mod 4969453 = 166858
c = (0463 ^ 917) mod 4969453 = 3875803
c = (1443 ^ 917) mod 4969453 = 4764414
c = (2047 ^ 917) mod 4969453 = 2067413

Hasil enkripsi:
2401144 1679420 2967120 2054777 4491255 4898261 166858 3875803 4764414 2067413

2. Mallory mendekripsi pesan ALICE dengan menggunakan kunci publiknya

Cipher Text = '2401144 1679420 2967120 2054777 4491255 4898261 166858 3875803 4764414 2067413'

Masukkan cipher text (c) ke fungsi dekripsi: m = (c ^ d) mod n

(Gunakan kunci privat Mallory)
m = (2401144 ^ 4605857) mod 4969453 = 2344
m = (1679420 ^ 4605857) mod 4969453 = 7456
m = (2967120 ^ 4605857) mod 4969453 = 2404
m = (2054777 ^ 4605857) mod 4969453 = 4516
m = (4491255 ^ 4605857) mod 4969453 = 1003
m = (4898261 ^ 4605857) mod 4969453 = 6440
m = (166858 ^ 4605857) mod 4969453 = 1163
m = (3875803 ^ 4605857) mod 4969453 = 0463
m = (4764414 ^ 4605857) mod 4969453 = 1443
m = (2067413 ^ 4605857) mod 4969453 = 2047

Hasil dekripsi:
23447456240445161003644011630463144320 47

Ubah pesan menjadi biner:
01001110010011110010111001010000010010010100111100001000000011110100100000000100111001100010011001100110010001101000010 0111

Ubah setiap 8 bit biner ke bentuk ascii:
NO.PIN = '1324'

3. Mallory mengubah pesan dan mengenkripsi pesan samaran dengan menggunakan kunci publik BOB

Pesan = 'NO.PIN = '9999"

Ubah pesan menjadi biner:
01001110010011110010111001010000010010010100111100001000000011110100100000000100111001110010011100100111001001001111

Ubah setiap 3 bit biner menjadi bentuk desimal:
23447456240445161003644011634471162344 47

Masukkan setiap 4 digit desimal (m) ke fungsi enkripsi: c = (m ^ e) mod n

(Gunakan kunci publik Mallory)
c = (2344 ^ 3865) mod 1025617 = 814513
c = (7456 ^ 3865) mod 1025617 = 615339
c = (2404 ^ 3865) mod 1025617 = 566072
c = (4516 ^ 3865) mod 1025617 = 783295
c = (1003 ^ 3865) mod 1025617 = 750546
c = (6440 ^ 3865) mod 1025617 = 879723
c = (1163 ^ 3865) mod 1025617 = 457933
c = (4471 ^ 3865) mod 1025617 = 359231
c = (1623 ^ 3865) mod 1025617 = 93145
c = (4447 ^ 3865) mod 1025617 = 1020355

Hasil enkripsi:
814513 615339 566072 783295 750546 879723 457933 359231 93145 1020355

4. BOB mendekripsi pesan dengan menggunakan kunci privatnya

Cipher Text = '814513 615339 566072 783295 750546 879723 457933 359231 93145 1020355'

Masukkan cipher text (c) ke fungsi dekripsi: m = (c ^ d) mod n

(Gunakan kunci privat Mallory)
m = (814513 ^ 506641) mod 1025617 = 2344
m = (615339 ^ 506641) mod 1025617 = 7456
m = (566072 ^ 506641) mod 1025617 = 2404
m = (783295 ^ 506641) mod 1025617 = 4516
m = (750546 ^ 506641) mod 1025617 = 1003
m = (879723 ^ 506641) mod 1025617 = 6440
m = (457933 ^ 506641) mod 1025617 = 1163
m = (359231 ^ 506641) mod 1025617 = 4471
m = (93145 ^ 506641) mod 1025617 = 1623
m = (1020355 ^ 506641) mod 1025617 = 4447

Hasil dekripsi:
23447456240445161003644011634471162344 47

Ubah pesan menjadi biner:
01001110010011110010111001010000010010010100111100001000000011110100100000000100111001110010011100100111001001001111

Ubah setiap 8 bit biner ke bentuk ascii:
NO.PIN = '9999'

(PROSEDUR PENYADAPAN DAN PENYAMARAN PESAN OLEH MALLORY BERHASIL)

LOFIAN: Jurnal Teknologi Informasi dan Komunikasi e-ISSN: 2798-9593
Vol. 1, No. 1, September 2021, Halaman 1-6 p-ISSN: 2798-9836
Submited: 02 Agustus 2021; Accepted: 18 September 2021; Published: 20 September 2021

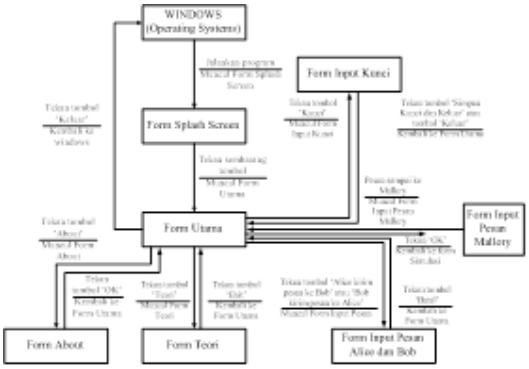
4.2. Pembahasan

Pada bagian ini, akan dibahas mengenai bagaimana alur kerja perangkat lunak dan proses-proses yang terjadi. Masing-masing pembahasan akan dibahas dalam sub bab berikut ini.

1. Alur Kerja

Di asumsikan terdapat dua pihak yang sedang berkomunikasi (Alice dan Bob) dan satu pihak sebagai penyadap (Mallory) yang berada di tengah-tengah saluran komunikasi. Sebelum proses simulasi dijalankan, user harus meng-input kunci privat dan publik Alice, Bob dan Mallory pada form Input Kunci. Input kunci juga dapat dihasilkan secara acak oleh komputer menggunakan random number generator. Setelah itu, ditampilkan proses simulasi penyadapan dan penukaran kunci yang dilakukan oleh Mallory terhadap Bob dan Alice.

Selanjutnya, user dapat meng-input sendiri pesan yang akan dikirim Bob kepada Alice atau sebaliknya dan pesan samaran yang dibuat oleh Mallory. Dalam proses simulasi ini, user juga dapat memilih untuk menggunakan opsi untuk menggunakan interlock protocol atau tidak. Mengatasi masalah man-in-the-middle-attack dengan interlock protocol ini terbagi lagi menjadi dua cara, yaitu: pisahkan hasil enkripsi menjadi dua bagian atau gunakan fungsi hash sebagai bagian pertama dan pesan terenkripsi menjadi bagian kedua. Kedua cara ini akan mengatasi tindakan penyamaran pesan oleh Mallory. Alur kerja perangkat lunak dapat digambarkan dalam bentuk state transition diagram (STD), seperti terlihat pada Gbr. 7.



Gbr. 7. State Transition Diagram (STD) Perangkat Lunak

5. Kesimpulan dan Saran

Dari hasil penelitian dan pembahasannya, maka dapat disimpulkan dan saran.

5.1. Kesimpulan

Setelah menyelesaikan perangkat lunak simulasi pemanfaatan metode interlock protocol untuk mengatasi man-in-the-middle-attack, peneliti menarik kesimpulan sebagai berikut:

1. Perangkat lunak mensimulasikan proses kerja man-in-the-middle-attack sebagai salah satu bentuk penyerangan terhadap metode kriptografi publik dan proses kerja interlock protocol untuk mengatasinya, sehingga perangkat lunak dapat digunakan untuk mendukung proses belajar mengajar, terutama dalam mata kuliah Kriptografi.
2. Dengan menggunakan interlock protocol, walaupun kunci publik pihak penerima dan pengirim didapatkan dan diganti oleh penyadap, tetapi penyadap tidak dapat menjalankan prosedur man-in-the-middle-attack untuk melihat dan mengubah pesan. Hal ini dikarenakan pesan terenkripsi terbagi menjadi dua bagian pada variasi pertama dan terdapat fungsi hash untuk memverifikasi keaslian pesan pada variasi kedua.

5.2. Saran

Peneliti ingin memberikan beberapa saran yang mungkin dapat membantu dalam pengembangan perangkat lunak ini yaitu:

1. Perangkat lunak ini dapat dikembangkan dengan menambahkan algoritma kunci publik lainnya, seperti: metode Rabin, ElGamal dan LUC.
2. Perangkat lunak dapat dikembangkan dengan menambahkan fitur multimedia, yaitu dengan menambahkan animasi yang lebih baik dan suara yang mendukung proses simulasi.

Referensi

[1] Schneier, B, 1996, Applied Crytography, Second Edition, John Willey and Sons Inc. Canada.
[2] Kurniawan, J., 2004, Kriptografi, Keamanan Internet dan Jaringan Komunikasi, Informatika, Bandung.
[3] Stallings, W., Cryptography and Network Security Third Edition, Prentice Hall.
[4] Putar, R., 2005, The Best Source Code Visual Basic, PT. Elex Media Komputindo, Jakarta.
[5] Suryokusumo.A, 2001, Microsoft Visual Basic 6.0, PT. Elex Media Komputindo, Jakarta.
[6] Novian.A, 2004, Panduan MS. Visual Basic 6, Andi, Yogyakarta.
[7] Supardi.Y, 2006, Microsoft Visual Basic 6.0 Untuk Segala Tingkat, PT. Elex Media Komputindo, Jakarta.
[8] en.wilkipedia.org/wiki/man in the middle attack
[9] www.computerhope.com/jargon/m/mitma.htm
[10] www.cs.umu.se/education/examina/rapporter/mattiasericsson.pdf
[11] www.ouah.org/mitmbrief.htm
[12] www.cs.steven.edu/~swetzel/publications/mim.pdf