Jurnal TIMES , Vol. IV No 2 : 1-6 , 2015
ISSN : 2337 - 3601

ANALISIS KEAMANAN PADA KOMBINASI PROTOKOL SECRET SHARING DAN THREE-PASS

Satria Prayudi[1], Robbi Rahim[2]

Program Studi Pasca Sarjana Teknik Informatika[1]

Universitas Sumatera Utara[1]
Jl.Universitas No.9, Kampus USU Padang Bulan, Medan 20155, Sumatera Utara[1]
e-mail : satryacode@gmail.com[1]

Program Studi Sistem Informasi Fakultas Teknik dan Ilmu Komputer[2]
Universitas Prima Indonesia[2]
Jl. Sekip Simp. Sikambing, Medan, North Sumatera, Indonesia[2]
e-mail : irvieboy@gmail.com[2]

,

ABSTRAK

Protokol Secret Sharing adalah metode yang digunakan untuk membagi atau memecah sebuah pesan rahasia (secret) kepada 2 (dua) atau lebih penerima, sehingga hasil dari pecahan pesan (shares) tersebut tidak dapat diketahui oleh para penerima secret, kecuali setiap penerima melakukan pertukaran shares untuk merekonstruksi secret. Permasalahan yang terjadi adalah ketika proses pertukaran shares, ada pihak lain yang mengetahui shares dari para penerima, maka pihak tersebut juga dapat merekonstruksi secret. Untuk menyelesaikan permasalahan tersebut, diperlukan pendekatan keamanan tambahan, seperti melakukan enkripsi pesan. Untuk itu digunakan Protokol Three-Pass, protokol ini akan mengamankan proses pertukaran shares antar penerima. Protokol Three-Pass juga memberikan kemudahan pada penerima untuk mengamankan share tanpa harus melakukan distribusi kunci enkripsi, dan share tersandi tersebut tetap terjamin keamanannya. Penelitian ini menganalisa keamanan pada pengiriman secret dengan mengkombinasikan Protokol Secret Sharing dan Protokol Three-Pass. Hasil penelitian ini menyatakan Protokol Three-Pass dapat mengamankan pertukaran shares, walaupun pihak penyerang mendapatkan shares tersandi pada saat pertukaran share, pihak tersebut harus melakukan brute-force terhadap shares tersandi tersebut sebanyak p^n bilangan acak (dimana p adalah modulo pada secret sharing, dan n adalah panjang share), dimana hal ini akan mustahil bagi pihak penyerang untuk mengetahui share yang benar, walaupun dia memiliki sumber daya komputer yang memadai.

Kata Kunci : protokol secret sharing, protokol three-pass, bilangan acak

1. PENDAHULUAN

Andaikan Alice ingin mengirim sebuah pesan rahasia kepada Bob dan Charlie melalui sebuah media komunikasi, satu diantara mereka baik itu Bob atau Charlie tidak dipercaya oleh Alice akan keamanan pesan tersebut sebelum mereka terima. Karena ketidak percayaan itu, Alice memecah (split) pesan itu sedemikian rupa sehingga Bob maupun Charlie tidak dapat membaca pesan tersebut, terlebih kepada siapapun yang mendapatkannya. Dikhawatirkan terjadinya perubahan pada pesan oleh pihak yang tidak berhak menerima pesan. Karena tak satu pun diantara mereka yang dapat mengetahui pesan rahasia tersebut, kecuali mereka bekerja sama untuk menyatukan pesan itu agar dapat mengetahui pesan rahasia dari Alice. Proses pemecahan pesan kedalam beberapa bagian (shares) itu disebut sebagai secret sharing [1]. Namun demikian siapapun yang dapat mengetahui shares tersebut, dapat juga melakukan rekonstruksi pesan [1]. Skenario yang dapat terjadi adalah, terdapat pihak yang tidak berhak mendapat pesan mengetahui share dari Bob dan Charlie pada saat mereka melakukan pertukaran share, maka pihak tersebut dapat juga merekonstruksi pesan.

Maka dari itu, penelitian ini menerapkan pengamanan tambahan dalam proses pertukaran shares, adapun pengamanan yang diusulkan adalah protokol three-pass. Protokol three-pass adalah sebuah skema yang memungkinkan masing-masing pihak dapat melakukan pertukaran pesan rahasia, tanpa memerlukan pertukaran kunci dalam mengamankan pesan, akan tetapi diperlukan kriptografi simetris (teknik penyandian pesan yang menggunakan kunci enkripsi dan dekripsi yang sama) dalam mengenkripsi dan mendekripsi pesan [1]. Kelebihan yang diberikan oleh protokol three-pass adalah penggunaan kriptografi simetris dalam proses enkripsi dan dekripsi, dimana kriptogradi simetris memiliki kompleksitas yang rendah dibandingkan dengan kriptografi asimetris (teknik penyandian pesan yang memiliki kunci publik dan kunci privat) [2].

Sehingga proses pengiriman secret oleh Alice menjadi, Alice memecah pesan menjadi 2 bagian masing-masing untuk Bob dan Charlie. Untuk dapat merekonstruksi pesan, Bob melakukan pertukaran share kepada Charlie melalui protokol three-pass, dimana share tersebut akan disandikan, sehingga dalam pertukaran tersebut share milik Bob tidak dapat diketahui oleh pihak lain selain Charlie, dan begitu pula sebaliknya.

2. LANDASAN TEORI

2.1. Protokol Secret Sharing

Suatu pesan atau informasi rahasia jika hanya dipegang oleh satu orang atau satu pihak akan meningkatkan resiko keamanan. Salah satu cara untuk mengatasi permasalahan ini adalah dengan melakukan pemecahan (*split*) pada informasi rahasia tersebut kedalam beberapa bagian. *Secret sharing* merupakan suatu metode untuk melakukan *split* informasi tersebut kedalam beberapa bagian yang disebut bagian (*shares*), untuk dibagikan kepada beberapa penerima (*participants*), dengan suatu aturan tertentu [3]. *Secret sharing* juga menangani masalah pendistribusian kunci rahasia yang telah dibagi dengan mengijinkan *t* dari *n* pengguna dimana $t \leq n$ untuk melakukan kunci awal. Skema *secret sharing* diperkenalkan oleh Blakley dan Shamir sebagai solusi untuk mengamankan kunci kriptografi. *Secret sharing* dapat juga digunakan untuk situasi apapun dimana akses kepada informasi harus terbatas, atau harus memiliki izin terlebih dahulu.

Menurut Shamir [3], *secret sharing* ideal untuk diaplikasikan pada sebuah grup yang setiap anggotanya saling mencurigakan akan tetapi setiap anggota itu harus dapat bekerja sama. *Secret sharing* memanfaatkan algoritma dari polinomial, polinomial umumnya digunakan untuk mencari sebuah nilai $P(x)$ yang dilalui oleh sejumlah titik-titik data (x_i, y_i), dimana x=0 adalah *secret* tersebut. Variabel yang terdapat dalam protokol ini memiliki fungsinya masing-masing seperti berikut ini:

1. t = jumlah bagian yang diperlukan agar pesan dapat dibaca. t harus lebih kecil atau sama dengan n ($t \leq n$).
2. n = *jumlah* bagian dari pesan.
3. k = koeffisien yang digunakan untuk membangkitkan *polinomial*, dengan jumlah $k = t-1$ ($k_1, k_2, \ldots, k_{t-1}$) dengan setiap k adalah bilangan acak.
4. m = variebel pesan berupa bilangan desimal.
5. p = bilangan prima yang lebih besar dari total varibel t, n dan m . Jika p yang digunakan lebih kecil dari total variabel t, n dan m, maka hasil dari kalkulasi akan salah.

Berikut ini adalah formula dari polinomial yang digunakan dalam protokol *secret sharing* untuk melakukan pemecahan *secret*:

$$P_n = m + k_1(n) + k_2(n)^2 + \ldots + k_{t-1}(n)^{t-1} \bmod p$$

Proses kerja dari protokol ini adalah:

1. Pesan dibagi menjadi n buah bagian ($P_1, P_2, \ldots, P_n$), yang disebut sebagai bayangan (*shadow*) atau bagian (*share*).
2. Bagian-bagian tersebut dibagikan kepada n orang, dengan setiap orang mendapatkan satu bagian yang berbeda-beda.
3. Tentukan nilai t sehingga diperlukan t buah bagian pesan agar dapat menyusun kembali pesan yang dirahasiakan.

Contoh:

Diberikan m = C, yang akan dibagikan kepada 3 orang penerima, maka $n = 3$, dan $t = 3$, dengan demikian *share* yang dibagikan pada ketiga orang tersebut saling dibutuhkan agar pesan asli dapat diterima. Koeffisien yang dibutuhkan adalah sejumlah n-1, yaitu 2 buah koeffisien, adapun $k_1 = 7$ dan $k_2 = 3$. Nilai $p = 107$.

Ubah m kedalam bentuk ASCII.

C = 67

Kemudian dibentuk polinomial P_1, P_2 dan P_3 untuk $m = 67$.

$P_1 = 67 + 7(1) + 3(1)^2 \bmod 107 = 77$
$P_2 = 67 + 7(2) + 3(2)^2 \bmod 107 = 93$
$P_3 = 67 + 7(3) + 3(3)^2 \bmod 107 = 8$

Untuk dapat membentuk kembali m, akan dilakukan pembentukan ulang *share* yang didapat oleh setiap penerima kedalam bentuk awal fungsi polinomial sebelumnya. seperti berikut ini.

$m = \{(1, P_1), (2, P_2), (3, P_3)\}$

Sehingga dapat dilihat m berupa titik-titik kordinat, dimana titik kordinat ini disebut sebagai (xi, yi). Sekumpulan titik-titik kordinat tersebut akan digunakan kedalam fungsi interpolasi lagrange untuk mendapatkan titik data pesan awal, atau dalam hal ini adalah *secret*. Interpolasi polinomial lagrange diterapkan untuk mendapatkan fungsi polinomial $P(x)$ berderajat tertentu yang melewati sejumlah titik data. Misalnya akan dicari $P(x)$ berderajat satu yang melewati 2 buah titik, yaitu $(x1, y1), (x2, y2)$. Adapun formula dari interpolasi polinomial lagrange order n yang digunakan dalam *secret sharing* adalah sebagai berikut [3].

$$Pn(x) = \sum_{i=0}^{n} yiLi(x) \bmod p$$

dengan

$$Li(x) = \prod_{j=0}^{n} \frac{x - xj}{xi - xj}$$

$$j \neq i$$

Berdasarkan formula dari interpolasi polinomial diatas, diberikan titik-titik untuk m_1, sehingga terbentuk fungsi polinomial berderajat 2 sebagaimana berikut ini.

$m = \{(1, 77), (2, 93), (3, 8)\}$
$x_0 = 1, \quad y_0 = 77$
$x_1 = 2, y_1 = 93$
$x_2 = 3, y_2 = 8$
$p = 107$

$L0(x) = (x - x1)(x - x2)$

$L1(x) = (x - x0)(x - x2)$

$L2(x) = (x - x0)(x - x1)$

$$P(x) = \left(y0\frac{L0(x)}{L0(x0)} + y1\frac{L1(x)}{L1(x1)} + y2\frac{L2(x)}{L2(x2)}\right) \bmod p$$

$$P(x) = \left(77\frac{(x-x1)(x-x2)}{(x0-x1)(x0-x2)} + 93\frac{(x-x0)(x-x2)}{(x1-x0)(x1-x2)} + 8\frac{(x-x0)(x-x1)}{(x2-x0)(x2-x1)}\right) \bmod 107$$

$$P(x) = \left(77\frac{(x-2)(x-3)}{(1-2)(1-3)} + 93\frac{(x-1)(x-3)}{(2-1)(2-3)} + 8\frac{(x-1)(x-2)}{(3-1)(3-2)}\right) \bmod 107$$

$$P(x) = \left(77\frac{(x-2)(x-3)}{2} + 93\frac{(x-1)(x-3)}{-1} + 8\frac{(x-1)(x-2)}{2}\right) \bmod 107$$

Kemudian diketahui bahwasanya $P(0)$ adalah nilai dari *secret*. Maka, bentuk diatas dimasukkan nilai x=0.

$$P(0) = \left(77\frac{(0-2)(0-3)}{2} + 93\frac{(0-1)(0-3)}{-1} + 8\frac{(0-1)(0-2)}{2}\right) \bmod 107$$

$$P(0) = \left(77\frac{6}{2} + 93\frac{3}{-1} + 8\frac{2}{2}\right) \bmod 107$$

$$P(0) = ((77 \times 3) + (93 \times (-3)) + (8 \times 1)) \bmod 107$$

$$P(0) = (231 + (-279) + 8) \bmod 107$$

$$P(0) = -40 + 107 \bmod 107$$

$$P(0) = 67$$

Dengan demikian dapat diperoleh hasil interpolasi polinomial dari setiap m_i sebagai berikut.

m = {(1, 77), (2, 93), (3, 8)} = 67 =>C

2.2. Protokol Three-Pass

Three-Pass merupakan suatu skema pada proses pengiriman dan penerimaan pesan rahasia, tanpa melakukan pertukaran kunci sehingga pemilik pesan terjaga kerahasiaanya. Konsep dasar *Three-Pass Protocol* bahwa masing-masing pihak dapat melakukan pertukaran pesan tanpa memerlukan pertukaran kunci *public* atau kunci *private*, akan tetapi memerlukan kriptografi simetris dalam mengenkripsi pesan [1].

Dalam penelitian ini penulis menerapkan algoritma *One Time Pad* sebagai kriptografi simetris. Adapun variabel yang terdapat dalam protokol yang memanfaatkan *One Time Pad* sebagai kriptografi simetris adalah sebagai berikut:

1. *A* sebagai pengirim
2. *B* sebagai penerima
3. k_a adalah kunci simetris *A*
4. k_b adalah kunci simetris *B*
5. *m* adalah pesan
6. c_1, c_2, adalah pesan terenkripsi dari hasil proses *e*
7. c_3 adalah pesan terenkripsi hasil dari proses *d*
8. e_i adalah proses enkripsi pada karakter ke-*i*
9. d_i adalah proses dekripsi pada karakter ke-*i*
10. *i* adalah inkremen (1, 2, ... , *i*+1)
11. *p* adalah batasan.

Formula yang digunakan untuk mengenkripsi adalah:

$$e_i = m_i + k_i \bmod p$$

Dan untuk mendekripsi adalah:

$$d_i = e_i - k_i \bmod p$$

Contoh penerapan protokol *three-pass*:

Bob mengirim pesan, m = C, dengan p = 255 (sebagaimana panjang ASCII), dengan k_a = 13
ubah m kedalam bentuk ASCII
m = 67
k_a = 13
e = 67 + 13 mod 255 = 80
c_1 = 80

Charlie menerima pesan berupa c_1 = 80. Kemudian mengenkripsi kembali menggunakan *One Time Pad* dengan kunci k_b = 75. Dan mengrimkannya kembali.

c_1 = 80
k_b = 75
e_1 = 80 + 75 mod 255 = 155
$c2$ = 155

Bob menerima pesan berupa $c2$ = 155 dan mendekripsi mengunakan k_a. Kemudian mengirimkannya kembali.

c_2 = 155
k_a = 13
d_1 = 155 - 13 mod 255 = 142
c_3 = 142

Charlie menerima pesan berupa $c3$ = 142 dan mendekripsi menggunakan k_b untuk mendapatkan pesan asli yang dikirim oleh Alice.

c_3 = 142
k_b = 75
d_1 = 142 - 75 mod 255 = 67
m = 67

Kemudian ubah ASCII dari m kedalam bentuk alfabet, sehingga didapat m = C.

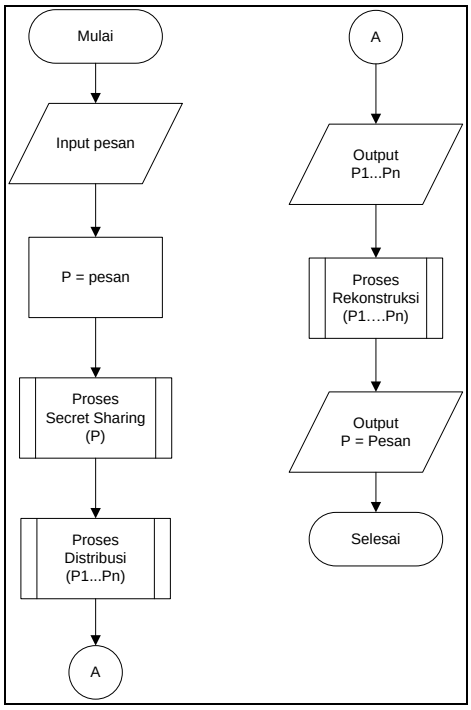
3. PERANCANGAN

3.1. Data Yang Digunakan

Data yang digunakan dalam penelitian ini adalah sekumpulan pesan teks, yang dapat dikenali dengan karakter ASCII.

3.2. Rancangan Sistem

Berikut ini adalah rancangan dari sistem yang akan penulis kerjakan untuk menyelesaikan permasalahan.

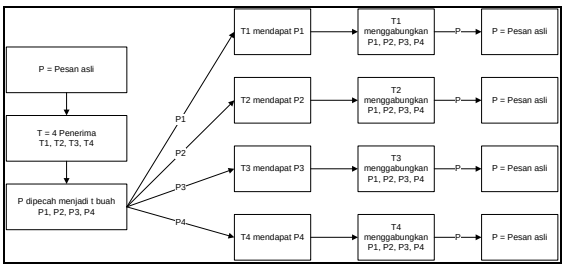


Gambar 1 Flowchart rancangan sistem.

Berdasarkan gambar 1 proses dimulai dengan input sebuah pesan, kemudian pesan akan masuk kedalam proses *secret sharing* untuk menciptakan *n* buah bagian. Kemudian dilakukan proses pendistribusian *n* buah bagian kepada penerima pesan. Setelah bagian-bagian pesan terdistribusi, pihak penerima dapat melakukan perekonstruksian pesan dengan mendapatkan bagian-bagian dari pesan tersebut dari penerima lainnya, langkah tersebut masuk kedalam proses rekonstruksi. Kemudian output dari proses rekonstruksi adalah pesan awal.

3.3. Rancangan Secret Sharing

Adapun gambaran dari proses *secret sharing* adalah sebagai berikut.



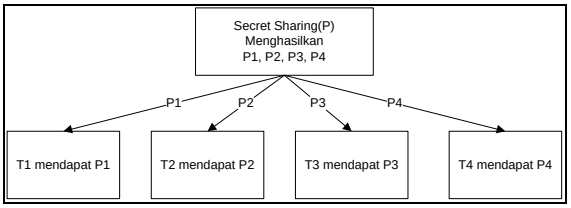
Gambar 2 Proses secret sharing.

Dari gambar 2 dapat dijelaskan bahwasanya, pesan asli akan dibagi kedalam T buah atau 4 orang sebagaimana dalam gambar, kemudian pecahan tersebut P1, P2, P3 dan P4 akan dibagikan masing-masing kepada T1, T2, T3 dan T4. Kemudian agar T1 dapat mengetahui pesan asli, T1 harus menggabungkan P1 miliknya dengan P2, P3 dan P4 dari masing-masing penerima.

Setelah proses pemecahan pesan (*split*) berhasil dilakukan, pecahan pesan tersebut akan didistribusikan dengan suatu cara sehingga masing-masing penerima menerima pecahan tersebut masing-masing. Terdapat dua tahapan yang akan dilakukan agar penerima mendapatkan pesan yang dipecahkan tersebut, yaitu proses distribusi pecahan pesan (*shares*) dan proses rekonstruksi pecahan pesan (*shares*)

3.4. Rancangan Distribusi Share

Setelah pecahan pesan berhasil dilakukan, pecahan pesan (*shares*) tersebut akan didistribusikan kepada tiap-tiap penerima. Adapun gambaran dari proses pendistribusian *shares* kepada setiap penerima adalah sebagai berikut.

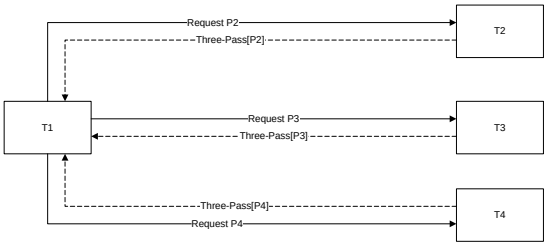


Gambar 3 Proses distribusi share.

Dari gambar 3 dapat dilihat bahwasanya, pecahan pesan dibagi sebanyak T penerima, kemudian pecahan tersebut yang berupa P1, P2, P3 dan P4 akan dibagikan masing-masing kepada T1, T2, T3 dan T4.

3.5. Rancangan Rekonstruksi Share

Setelah setiap penerima mendapatkan pecahan pesan, langkah berikut yang akan dilakukan adalah melakukan rekonstruksi *secret*, hal ini memerlukan pertukaran *shares* kepada setiap penerima lainnya. Adapun proses rekonstruksi *secret* adalah sebagai berikut.



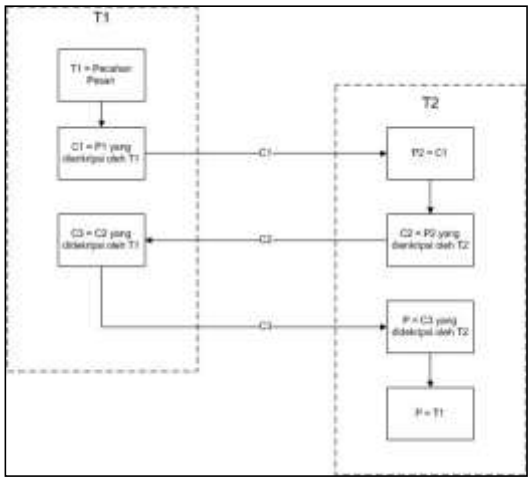
Gambar 4 Proses rekonstruksi secret

Berdasarkan gambar 4 bahwasanya setiap penerima (T1, T2, T3, dan T4) akan meminta *share* kepada penerima lainnya, kemudian penerima tersebut mengirimkan *share* miliknya melalui protokol *three-pass*. Seperti gambar, T1 meminta P2 kepada T2, kemudian T2 mengirimkan P2 menggunakan protokol *three-pass* kepada T1. T1 meminta P3 kepada T3, kemudian T3 mengirimkan P3 menggunakan protokol *three-pass* kepada T1. T1 meminta P4 kepada T4, kemudian T4 mengirimkan P4 menggunakan protokol *three-pass* kepada T1. Setelah T1 memiliki keseluruhan *shares*, T1 dapat

membentuk ulang *secret* menggunakan Protokol *Secret Sharing*.

3.6. Rancangan Three-Pass

Implementasi Protokol *Three-Pass* terdapat dalam proses pertukaran *shares* antar penerima, yang gunanya untuk mengamankan *shares* dari upaya pencurian oleh pihak lain. Adapun proses rekonstruksi pecahan pesan (*shares*) yang akan diimplementasikan kedalam protokol *secret sharing* sebagai pengamanan tambahan adalah sebagai berikut.



Gambar 5 Proses Three-Pass

Berdasarkan gambar 5 bahwasanya pesan terlebih dahulu harus dienkripsi oleh T1 (pengirim pesan), kemudian T2 (penerima pesan) mengenkripsikan kembali pesan terenkripsi yang sudah diterima dan dikirimkan kembali kepada T1, T1 mendekripsi pesan terenkripsi dari penerima dengan kunci miliknya dan mengirimkan kembali ke T2, T2 mendekripsi pesan dengan kunci yang miliknya, dengan begitu T2 mendapatkan pesan asli yang dikirim oleh T1.

4. PEMBAHASAN

4.1. Analisis Waktu

Pengujian ini bertujuan untuk mengetahui seberapa lama waktu yang digunakan untuk mengamankan pesan, mulai dari pesan dengan panjang 10 karakter, 50 karakter, 100 karakter, 500 karakter, hingga 1000 karakter.

Spesifikasi dari komputer yang digunakan:

1. Sistem Operasi Microsoft Windows 8.1
2. Prosessor Intel Core i5-3317U @1.70GHz
3. RAM 4 GB

Tabel 1. Analisis waktu.

No.	*Panjang Pesan*	*Jumlah Penerima*	*Waktu (milidetik)*
1	10	3	10
2	50	3	30.6
3	100	3	53.9
4	500	3	255.7
5	1000	3	493.5

Berdasarkan pengujian terhadap panjang pesan mulai dari 10 karakter, 50 karakter, 100 karakter, 500 karakter dan 1000 karakter pesan. Dapat disimpulkan bahwasanya lamanya waktu eksekusi dalam proses pemecahan pesan hingga rekonstruksi pesan, berbanding lurus dengan panjang pesan. Begitu juga dengan banyaknya penerima, jika penerima pesan semakin bertambah, maka lamanya proses eksekusi akan bertambah lama.

4.2. Analisis Keamanan

Pengujian ini dilakukan terhadap pesan dengan panjang yang bervariasi, mulai dari 10 karakter, 50 karakter, 100 karakter, hingga 1000 karakter. Hasil dari analisis keamanan ini akan memberikan jaminan terhadap keamanan pesan dari ancaman pihak ketiga yang melakukan serangan *brute-force* terhadap *shares* pada saat proses pertukaran *share* berlangsung.

Tabel 2. Analisis keamanan.

No.	*Panjang Pesan*	*Jumlah Penerima*	*Bilangan acak yang dihasilkan*
1	10	3	997^{10} x 3
2	50	3	997^{50} x 3
3	100	3	997^{100} x 3
4	500	3	997^{500} x 3
5	1000	3	997^{1000} x 3

Berdasarkan pengujian terhadap panjang pesan dan penerima pesan yang bervariasi dapat disimpulkan, semakin panjang pesan yang diberikan maka usaha penyerang untuk melakukan *brute-force* terhadap pesan akan semakin lama, dan semakin mustahil karena banyaknya jumlah bilangan acak yang dihasilkan setelah dilakukan proses enkripsi.

5. KESIMPULAN

Adapun kesimpulan pada penelitian ini antara lain:

1. Kombinasi protokol *Secret Sharing* dan *Three-Pass* berhasil mengamankan pesan dan mengirimkan pesan tersebut kepada setiap penerimanya.
2. Protokol *Three-Pass* berhasil mengamankan *shares* yang dihasilkan melalui Protokol *Secret Sharing* dari upaya perekonstruksian ulang oleh pihak yang tidak berhak menerima pesan.
3. Setiap penerima diharuskan untuk aktif dalam melakukan pertukaran *shares*, agar *secret* dapat direkonstruksi. Artinya jika salah satu saja penerima tidak melakukan pertukaran *share*, maka tidak satupun penerima akan menerima pesan yang dikirim.

6. DAFTAR PUSTAKA

[1] B. Schneier, Applied Cryptography 2nd Edition : Protocols, Algorithms, and Source Code in C Vol 2, California: John Wiley & Sons Inc, 1996.

[2] A. G. Uchôa, M. E. Pellenz, A. O. Santin dan C. A. Maziero, "A Three-Pass Protocol for Cryptography Based on Padding for Wireless Networks," dalam *Consumer Communications and Networking Conference*, Las Vegas, NV, USA , 2007.

[3] A. Shamir, "How to share a secret," *Communication of The ACM*, vol. 22, no. 11, pp. 612-613, 1979.