Implementasi Pembagian Rahasia dengan Menggunakan Teorema Chinese Remainder

Robertus Theodore / 13509008
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
robert_8891@yahoo.com

***Abstrak*— Skema pembagian rahasia adalah salah satu bagian dari ilmu kriptografi. Untuk tujuan pengelolaan keamanan, suatu rahasia dipecah menjadi beberapa partisi. Setiap partisi rahasia ini dibagikan kepada masing – masing orang dalam kelompok tertentu. Rahasia ini hanya dapat terpecahkan ketika sejumlah cukup orang yang memegang partisi awal, saling berbagi dan mengkombinasikan partisi rahasia yang mereka punya. Biasanya sebuah rahasia atau key digunakan untuk mengakses beberapa dokumen penting. Jika salah satu orang yang memegang partisi rahasia tidak turut mengkombinasikan partisinya, maka rahasia atau key secara keseluruhan tidak akan terungkap, dan dokumen yang diproteksi oleh key tersebut tidak dapat diakses. Dalam teorema Chinese remainder, dikatakan bahwa suatu sistem yang memiliki kesesuaian fungsi, pasti memiliki solusi yang selaras dengan kondisi dari kesesuaiannya. Dalam makalah ini, penulis akan mengkaji tentang implementasi dari pembagian rahasia dengan menggunakan teorema Chinese remainder.**

***Kata Kunci*—pembagian rahasia, teorema Chinese remainder.**

I. PENDAHULUAN

Dewasa ini, perkembangan teknologi semakin pesat. Informasi dan dokumen dapat dengan mudah didapatkan. Untuk data – data tertentu, tingkat kerahasiaan menjadi suatu hal yang amat penting. Oleh karena itu, berbagai upaya dilakukan agar data hanya dapat diakses oleh orang – orang yang memiliki hak akses.

Pada beberapa kasus tertentu, suatu data penting dapat diakses oleh beberapa orang dengan satu sandi lewat. Dengan cara seperti itu, risiko terjadinya penyalahgunaan data oleh oknum tertentu, tanpa sepengetahuan orang lain yang juga pemegang akses terhadap data itu, rentan sekali terjadi. Oleh karena itu, diperlukan suatu teknik pengamanan yang efektif untuk menanggulanginya. Salah satu cara untuk menanggulanginya adalah dengan menggunakan skema pembagian rahasia.

II. KAJIAN TEORI

Sebelum masuk ke implementasi dengan menggunakan teorema Chinese remainder, berikut penjelasan teori – teori yang terkait.

2.1 Teorema Chinese Reminder

Teorema Chinese Remainder yang asli terdapat pada buku AD Sun Zi suanjing. Kemudian dipublikasikan ulang pada tahun 1247 pada buku *Mathematical Treatise in Nine Sections* karangan Qin Jiushao. Isi dari Teorema Chinese Remainder adalah :

Misalkan $n_1,\ldots,n_k$ adalah bilangan bulat positif yang setiap pasangannya adalah koprima (yang artinya $FPB(n_i,..,n_j) = 1$ untuk setiap $i \neq j$). Maka, untuk setiap bilangan bulat $a_1,\ldots,a_k$, selalu ada bilangan bulat x yang merupakan penyelesaian dari sistem kongruensi simultan.

$X \equiv a_i \pmod{n_i}$ untuk i = 1,…, k

Pseudocode "subtitle":

```
x_solves_it=true;
for(i= 1; i <= k; i++)
   if(x % n[i] != a[i] % n[i])
      x_solves_it=false;
```

Terlebih lagi, semua penyelesaian x dari sistem ini adalah juga kongruen modulo dari perkalian $n = n_1...n_k$. Suatu penyelesaian x dapat ditemukan dengan cara sebagai berikut. Untuk setiap i, bilangan bulat n_i dan n/n_i adalah koprima, dan menggunakan ekstensi algoritma Euklidean kita dapat menemukan bilangan bulat r dan s sehingga $r\ n_i + s\ n/n_i = 1$. Jika kita menentukan $e_i = s\ n/n_i$, maka kita dapat

$$e_i \equiv 1 \pmod{n_i} \quad \text{and} \quad e_i \equiv 0 \pmod{n_j}$$

untuk $j \neq i$.

```
for (i= 1; i <= k; i++)
  {r, s}= ExtendedEuclid( n[i], n /
n[i] );
  e[i]= s * n / n[i];
  for(j= 1; j <= k; j++)
    if (j != i)
      assert( e[i] % n[i] == 1 && e[i]
% n[j] == 0 );
```

Penyelesaian dari sistem kongruensi simultan ini adalah

$$x = \sum_{i=1..k} a_i e_i$$

```
  for(i= 1; i <= k; i++)
    x += a[i] * e[i];
```

Sebagai contoh, misalkan kita ingin menemukan suatu bilangan bulat x sehingga

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{4}$$
$$x \equiv 2 \pmod{5}$$

```
x % 3 == 2 % 3 &&
 x % 4 == 3 % 4 &&
 x % 5 == 2 % 5
```

Menggunakan ekstensi algoritma Euklidean untuk 3 dan 4×5 = 20, kita memperoleh (-13) × 3 + 2 × 20 = 1, di mana e_1 = 40 *(e[1] == 40)*. Menggunakan algoritma Euklidean untuk 4 dan 3×5 = 15, kita memperoleh (-11) × 4 + 3 × 15 = 1. Oleh karena itu, e_2 = 45 *(e[2] == 45)*. Akhirnya, menggunakan algoritma Euklidean untuk 5 dan 3×4 = 12, kita memperoleh 5 × 5 + (-2) × 12 = 1, yang berarti e_3 = -24 *(e[3] == -24)*. Jadi, penyelesaian x adalah 2 × 40 + 3 × 45 + 2 × (-24) = 167. Semua penyelesaian yang lain adalah kongruen 167 modulo 60, yang berarti bahwa mereka semua kongruen 47 modulo 60.

Kadangkala, sistem kongruensi simultan dapat diselesaikan sekalipun n_i*(n[i])* setiap pasangnya tidak selalu koprima. Syarat-syarat yang lebih tepat adalah sebagai berikut: sistem mempunyai penyelesaian x jika dan hanya jika $a_i \equiv a_j$ (**mod** fpb(n_i, n_j)) (a[i] == a[j] % gcd(n[i], n[j])) untuk semua i dan j. Semua penyelesaian x adalah kongruen modulo kelipatan persekutuan terkecil dari n_i (n[i]).

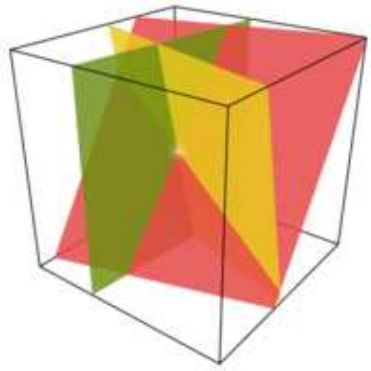
Dengan menggunakan metode substitusi, kita seringkali bisa menemukan penyelesaian dari sistem kongruensi simultan, sekalipun setiap pasang modulusnya tidak selalu koprima[1].

2.2 Pembagian Rahasia

Berdasarkan penjelasan dari Wikipedia, Skema pembagian rahasia ini ditemukan oleh Adi Shamir dan Geroge Blakley pada tahun 1979. Ide utama dalam pembagian rahasia ini adalah memecah *secret key* menjadi beberapa bagian dan membagi partisi – partisi *secret* tersebut kepada beberapa orang yang berbeda. Rahasia ini hanya dapat terpecahkan ketika sejumlah cukup orang yang memegang partisi awal, saling berbagi dan mengkombinasikan partisi rahasia yang mereka punya.

Biasanya sebuah rahasia atau key digunakan untuk mengakses beberapa dokumen penting. Jika salah satu orang yang memegang partisi rahasia tidak turut mengkombinasikan partisinya, maka rahasia atau key secara keseluruhan tidak akan terungkap, dan dokumen yang diproteksi oleh key tersebut tidak dapat diakses.

Dalam pembagian rahasia ini, ada seorang *dealer*, dan sejumlah n objek yang menerima partisi *secret key* tersebut. *Dealer* adalah orang yang mengetahui dan mempartisi *secret key*, lalu dealer juga yang membagikan partisi *secret* tersebut kepada objek pemain.



Gambar 1 Penggambaran Skema Pembagian Rahasia

Setiap partisi rahasia, digambarkan menjadi bidang segiempat. Titik di tengah, tempat semua bidang segiempat tersebut beririsan adalah titik dimana rahasia tersebut terungkapkan/ terpecahkan.

Pada skema pembagian rahasia yang baik, rahasia tidak dapat terungkap, jika kurang dari n objek penerima partisi, mengkombinasikan semua bagiannya. Sebagai contoh, untuk sebuah *secret* yang bernilai = "kunci" dipartisi menjadi lima bagian. Seseorang yang tidak mendapatkan partisi rahasia tersebut, perlu menebak 26^5 kemungkinan jawaban. Seseorang yang mendapat satu

bagian rahasia, perlu menebak sebesar 26^4 kemungkinan jawaban, dan seterusnya. Sistem yang seperti ini tidaklah aman, karena dengan makin banyak partisi yang diketahui, makin sedikit pula kemungkinan jawaban. Untuk skema pembagian rahasia yang aman, meskipun dia hanya kekurangan satu partisi rahasia, dia tetap saja menghadapi 26^5 kemungkinan jawaban.

Berdasarkan pada penemunya, ada dua cara membangun skema pembagian rahasia ini[2].

2.2.1 Shamir Secret Sharing

Shamir Secret Sharing adalah salah satu cara membangun skema pembagian rahasia yang ditemukan oleh Adi Shamir. Menurut Shamir,untuk kasus – kasus tertentu, mengumpulkan semua objek penerima rahasia dan mengkombinasikan partisi rahasia nya bersama, tidaklah praktis. Oleh karena itu, terkadang kita menggunakan skema *threshold*/ skema ambang dimana sejumlah *j* bagian rahasia sudah cukup untuk mengungkapkan rahasia secara keseluruhan.

Secara umum, Shamir Secret Sharing membagi sejumlah data P (cth: sandi lewat) menjadi *n* bagian $P_1,\ldots P_n$ dengan syarat:

1. Dengan sejumlah *j* bagian atau lebih, rahasia P dapat dipecahkan, atau ditemukan solusinya.
2. Untuk j-1 bagian, rahasia P tidak mungkin dapat dipecahkan.

Cirri khas dari Shamir's Secret Sharing adalah sebagai berikut:

1. Minimal: ukuran dari setiap partisi tidak melebihi ukuran data yang asli.
2. *Extensible* : ketika nilai *j* sudah ditentukan, partisi P_i dapat ditambahkan ataupun dihilangkan, tanpa mempengaruhi partisi atau potongan rahasia lainnya.
3. Dinamik : keamanan dapat ditingkatkan tanpa mengubah rahasia utama, tetapi dengan mengubah polinomialnya, atau dengan kata lain, merekonstruksi pembagian yang baru kepada para objek penerima.
4. Fleksibel : dalam sebuah organisasi yang mementingkan hirarki kepengurusan, kita dapat memberikan partisi rahasia yang berbeda bobotnya, berdasarkan tingkat kepentingannya dalam organisasi. Sebagai contoh, untuk Presiden, kita berikan partisi yang membuatnya dapat memecahkan rahasianya seorang diri. Dan untuk 4 orang bawahannya, diperlukan kombinasi secara bersama – sama untuk memecahkan rahasia utama.

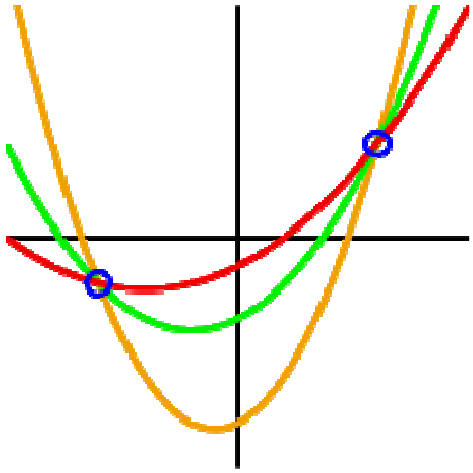
Notasi untuk skema ini adalah (j , n). Jika j = n, berarti semua objek penerima bagian rahasia, diperlukan untuk memecahkan rahasia ini.

Berdasarkan Wikipedia, ide esensial dari Shamir's secret sharing ini adalah 2 titik sudah cukup untuk mendefinisikan sebuah garis, 3 titik sudah cukup untuk mendefinisikan parabola, dan 4 titik sudah cukup untuk mendefinisikan *cubic curve.* Jadi, dibutuhkan *j* titik untuk mendefinisikan polynomial dengan derajat j – 1.

Andaikan kita ingin menggunakan (*k , n*) skema threshold untuk membagikan atau mempartisi rahasia Q. Pilih secara acak k – 1 koefisien $a_1, \ldots, a_{k-1}$ pada daerah F, dan isi a_0= Q. Berikut persamaan polinomialnya,

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_{k-1}x^{k-1} \quad (1)$$

Dari persamaan tersebut, kita bangun *n* titik, misalnya *i = 1, ... , n* untuk memperoleh (*i , f(i)*). Setiap objek penerima bagian rahasia, menyumbangkan satu titik. Diberikan irisan *k* dari bagian ini, lalu kita dapat mencari koefisien dari polinomial dengan menggunakan interpolasi dan rahasia yang terungkap adalah konstanta a_0.



Gambar 2 Gambar Ilustrasi dari Shamir's Secret Sharing

Gambar ini hanya sekedar ilustrasi. Skema Shamir's secret sharing menggunakan polinomial yang mencakup daerah terbatas, dan tidak ditampilkan pada bidang 2-dimensi.

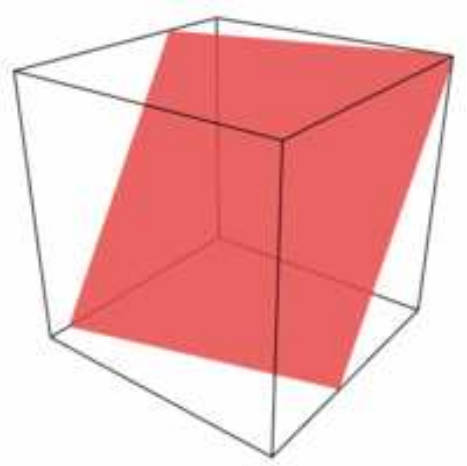
2.2.2 Skema Blakley

Secara umum, dalam suatu bangun ruang, bidang – bidang nonparalel yang berada di dalamnya pasti berpotongan di satu titik tertentu. Dua garis non- paralel pada bidang yang sama akan berpotongan pada satu titik. Tiga garis non – paralel dalam suatu bidang, akan berpotongan di satu titik tertentu juga, dan begitu juga seterusnya. Partisi rahasia dibangun dari tiap hyperplane pada bangun ruang.

Suatu rahasia dapat dikodekan sebagai salah satu koordinat pada titik yang berpotongan. Jika rahasia tersebut dikodekan menggunakan semua koordinat, meskipun secara acak, rahasia tersebut dapat dipecahkan atau ditemukan solusinya seorang diri. Seseorang tersebut mendapat informasi tentang rahasia itu, karena dia tahu bahwa rahasia nya pasti ada di bidang yang dia miliki.

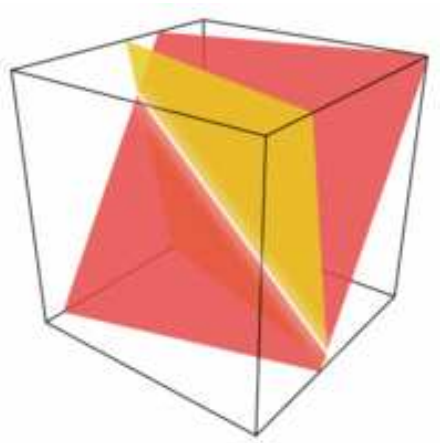
Untuk menjaga keamanan rahasianya, untuk setiap m partisi, maka bidang ruang yang digunakan juga m-dimensi. Jika hanya salah satu n koordinat yang digunakan, sulit bagi objek penerima partisi untuk mengungkap rahasia seorang diri (misalnya, diberikan petunjuk bahwa rahasia harus terletak pada sumbu – x untuk sistem dua dimensi). Setiap objek penerima partisi diberikan cukup informasi untuk mendefinisikan sendiri sebuah hyperplane. Cara mengungkap rahasianya adalah dengan mengitung titik – titik pada bidang, lalu memilih koordinat tertentu yang berpotongan.

Gambar diambil dari http://en.wikipedia.org/wiki/Secret_sharing



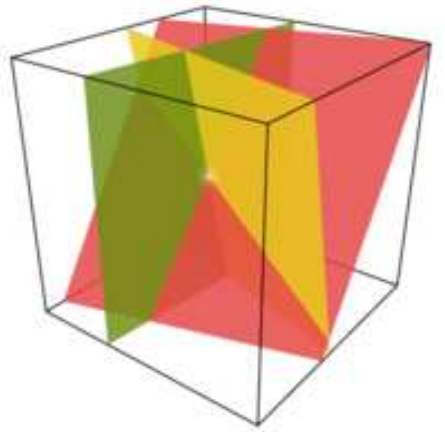
Gambar 3 Gambar Ilustrasi dari Blakley's Secret Sharing

Untuk ilustrasi gambar, kita menggunakan tiga pratisi rahasia. Sesuai dengan ciri khas dari skema Blakley's, untuk m – partisi rahasia, maka kita menggunakan m – dimensi bangun ruang. Pada gambar 3, ini adalah satu dari tiga bagian partisi.



Gambar 4 Gambar Ilustrasi dari Blakley's Secret Sharing

Pada gambar 4, ini adalah kasus untuk dua dari tiga bagian partisi yang dikombinasikan bersama. Koordinat yang berpotongan sudah mulai terlihat, dan membentuk garis. Namun, untuk dapat memecahkan rahasia, kita masih menghadapi sejumlah besar kemungkinan.



Gambar 5 Gambar Ilustrasi dari Blakley's Secret Sharing

Pada gambar 5, ini adalah kasus untuk tiga dari tiga bagian partisi yang dikombinasikan bersama. Jika partisi sudah lengkap, kemungkinan untuk mengungkap rahasia menjadi mudah. Satu titik koordinat, tempat ketiga bidang berpotongan adalah rahasianya.

III. PEMBAGIAN RAHASIA MENGGUNAKAN TEOREMA CHINESE REMINDER

Teorema Chinese Remainder menyatakan bahwa untuk sistem kekongruenan lanjar tertentu, terdapat solusi unik modulonya. Pembagian rahasia dapat menggunakan Teorema Chinese Remainder untuk membangun partisi dari persamaan – persamaannya yang kongruen, dan rahasia nya dapat terungkapkan dengan menyelesaikan sistem kongruen tersebut.

Teorema Chinese Remainder menyediakan detode untuk menetapkan nilai S modulo k pada beberapa bilangan relatif prima $m_1, m_2, ..., m_k$, diberikan $S < \prod_{i=1}^{k} m_i$, lalu kita membangun skema yang akan menentukan rahasia S dengan pembagian sejumlah k. Pilih sejumlah n bilangan relatif prima $m_1 < m_2 < m_n$ sehingga S lebih kecil daripada produk dari setiap pilihan bilangan bulat k, tetapi di lain sisi juga lebih besar daripada pilihan k-1. Kemudian partisi $s_1, s_2, ..., s_n$ didefinisikan sebagai $s_i = S \bmod m_i$ untuk i = 1, 2, …, n. Dengan Teorema Chinese Remainder kita dapat menentukan S dari set k, tetapi tidak untuk nilai yang kurang dari k.

Ada dua skema pembagian rahasia yang memanfaatkan ide Teorema Chinese Remainder antara lain; skema pembagian rahasia Mignotte dan skema Asmuth-Bloom[3].

3.1 Skema Pembagian Rahasia Mignotte

Skema pembagian rahasia Mignotte menggunakan Teorema Chinese Remainder. Urutan unik beberapa bilangan bulat disebut urutan Mignotte (k, n), yang terdiri dari bilangan bulat koprima n, sehingga produk dari nilai k yang paling kecil, lebih besar daripada produk dari k-1. Kondisi ini sangat penting karena skema ini dibangun dengan dasar pemilihan rahasia sebagai bilangan bulat antara dua produk. Kondisi ini memastikan bahwa setidaknya sejumlah k pembagian dibutuhkan untuk mengungkapkan rahasia[4].

Pilih bilangan bulat $n \geqslant 2$ dan k integer sehingga $2 \leqslant k \leqslant n$. Sebuah Mignotte *(k, n)* adalah urutan peningkatan bilangan bulat positif $m_1 <...< m_n$, dengan $(m_i,m_j)= 1$ untuk semua $1 \leqslant i < j \leqslant n$,sehingga $m_{n-k+2} ... m_n < m_1 ... m_k$. Retang ini disebut dengan kisaran rentang berwenang. Cara Kerja skema ini adalah : pertama kita membangun *(k,n)*. Lalu pilih S rahasia sebagai integer acak dalam rentang yang berwenang. Hitung setiap $1 \leqslant i \leqslant n$, dengan pengurangan modulo m_i dari S yang kita sebut s_i, ini adalah pembagiannya. Untuk sejumlah k pembagian rahasia yang berbeda, $s_{i_1}, ..., s_{i_k}$, Kami mempertimbangkan sistem kongruensi:

$$\begin{cases} x \equiv s_{i_1} \bmod m_{i_1} \\ \quad . \\ \quad . \\ \quad . \\ x \equiv s_{i_k} \bmod m_{i_k} \end{cases}$$

Dengan Teorema Chinese Remainder , karena $m_{i_1}, ..., m_{i_k}$ adalah koprima , sistem memiliki solusi unik modulo $m_{i_1} ... m_{i_k}$.

3.2 Skema Asmuth-Bloom

Skema ini menggunakan urutan khusus bilangan bulat. Pilih bilangan bulat $n \geqslant 2$, dan integer k $2 \leqslant k \leqslant n$. Urutan yang kita buat adalah koprima(yang artinya FPB(n_i,..,n_j) = 1 untuk setiap $i \neq j$) dan merupakan bilangan bulat positif $m_0 <...< m_k$ sedemikian, sehingga $m_0.m_{n-k+2}...m_n < m_1...m_k$ [5]. Dengan urutan tersebut, kita dapat menentukan rahasia S sebagai integer acak dari set $\mathbb{Z}/m_0\mathbb{Z}$. Ketika kita memilih random integer α sedemikian, sehingga $S+\alpha.m_0 < m_1...m_k$. Lalu kita dapat menghitung penurunan modulo m_i dari $S + \alpha.m_0$, untuk semua $1 \leqslant i \leqslant n$, berikut adalah partisi rahasia yang ke $I_i = (s_i,m_i)$. untuk sejumlah partisi k yang lain $I_{i_1}, ..., I_{i_k}$, sistem kekongruenannya adalah:

$$\begin{cases} x \equiv s_{i_1} \bmod m_{i_1} \\ \quad . \\ \quad . \\ \quad . \\ x \equiv s_{i_k} \bmod m_{i_k} \end{cases}$$

Karena $m_{i_1}, ..., m_{i_k}$ adalah koprima, maka sistem memiliki solusi unik S_0 modulo $m_{i_1} ... m_{i_k}$. Rahasia yang ingin diungkapkan adalah S yang merupakan hasil reduksi dari modulo m_0 dari S_0.

III. KESIMPULAN

Kita dapat menggunakan Teorema Chinese Remainder dalam skema pembagian rahasia yang akan kita buat. Namun, tingkat keamanan dari penerapan ini masih terus akan diuji dan ditingkatkan. Skema Mignotte dan Asmuth-

Bloom bukanlah skema yang sempurna. Dengan pemilihan urutan dan parameter yang tepat, sejumlah partisi yang kurang dari k, sudah dapat mengungkapkan rahasia yang diinginkan. Namun, skema Asmuth-Bloom adalah skema yang lebih baik tingkat sekuritasnya, karena skema ini menyertakan lebih banyak parameter yang dipilih secara acak.

REFERENCES

[1] Wikipedia. 2010. *Teorema Sisa Tiongkok*. (Online), (http://id.wikipedia.org/wiki/Teorema_sisa_Tiongkok, diakses 13 Desember 2010).

[2] Wikipedia. 2010. *Secret Sharing*. (Online), (http://en.wikipedia.org/wiki/Secret_sharing, diakses 15 Desember 2010).

[3] Wikipedia. 2010. *Secret Sharing using the Chinese Remainder Theorem*. (Online), (http://en.wikipedia.org/wiki/Secret_Sharing_using_the_Chinese_Remainder_Theorem, diakses 15 Desember 2010).

[4] M.Mignotte. *How to share a secret*. In T.Beth, editor, Cryptography-Proceedings of the Workshop on Cryptography, Burg Fererstein, 1982, volume 149 of Lecture Notes in Computer Science, pages 371-375. Springer-Verlag, 1983.

[5] C.Asmuth, J. Bloom. 1983. *A modular approach to key safeguarding*. IEEE Trans. Information Theory, 29(2):208-210.

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, 29 April 2010

ttd

Robertus Theodore / 13509008