Aplikasi Chinese Remainder Theorem dalam Secret Sharing

Dimas Gilang Saputra - 13509038
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
dimasgsaputra@yahoo.com

***Abstract*—Makalah ini membahas tentang salah satu aplikasi teori bilangan bulat yaitu *chinese remainder theorem* dalam salah satu metode menyimpan rahasia yaitu *secret sharing*. Skema *secret sharing* yang dibahas di makalah ini adalah skema *threshold secret sharing*. *Chinese remainder theorem* dapat digunakan untutk membuat suatu kunci rahasia dalam metode *secret sharing*. Ada dua skema dalam menggunakan *chinese remainder theorem* untuk *secret sharing*, yaitu skema Mignotte dan skema Asmuth-Bloom.**

***Index Terms*—teori bilangan bulat, chinese remainder theorem, secret sharing.**

I. PENDAHULUAN

Saat ini adalah saat dimana teknologi informasi sudah berkembang dengan pesat. Informasi-informasi yang ada sangat mudah menyebar dan penyebarannya pun cepat. Kadangkala beberapa informasi tersebut bukan untuk konsumsi khalayak umum melainkan menjadi rahasia. Suatu ketika mungkin ada pihak tertentu yang ingin mengetahui rahasia tersebut untuk kepentingan dirinya sendiri. Karena kita tidak menginginkan rahasia ini diketahui orang lain maka sebisa mungkin kita harus menjaga rahasia ini yaitu dengan menggunakan metode penyimpan rahasia yang baik.

Salah satu metode penyimpanan rahasia yang baik adalah dengan metode *secret sharing*. *Secret sharing* termasuk ke dalam kriptografi. Metode *secret sharing* ini adalah metode untuk membuat satu rahasia menjadi beberapa bagian lalu membagi bagian-bagian rahasia ini ke misalnya beberapa orang yang mendapat hak untuk mendapay]tkan bagian rahasia ini. Metode ini termasuk baik karena jika suatu rahasia hanya dikuasai satu orang saja maka kemungkinan rahasia tersebut bocor akan besar, sedangkan dengan metode *secret sharing* rahasia tidak mudah bocor karena jika mengetahui hanya sebagian rahasia maka rahasia tersebut tidak bisa diketahui. Untuk bisa mengetahui suatu rahasia yang disimpan dengan metode *secret sharing* maka kita membutuhkan sejumlah orang tertentu yang memiliki bagian-bagian rahasia yaitu jumlah orang minimum untuk membuka rahasia.

Dalam membuat kunci-kunci bagian rahasia dari metode *secret sharing* kita bisa menggunkan salah satu aplikasi teori bilangan bulat yaitu *chinese remainder theorem* atau teorema sisa tiongkok. *Chinese reminder theorem* adalah salah satu penerapan teori bilangan bulat.

II. CHINESE REMAINDER THEOREM

Chinese remainder theorem adalah teorema mengenai kekongruenan lanjar dalam teori bilangan bulat yaitu aritmetika modulo. Teorema ini pertama kali ditemukan oleh Sun Tze pada abad pertama. Aritmetika modeulo mempunyai pernan penting dalam penghitungan bilangan bulat. Aritmetika modulo banyak digunakan dalam kriptografi. Operator untuk menunjukkan modulo adalah "mod". Mod berarti sisa pembagian satu operan dari operan lainnya. Operan ini bertipe bilangan bulat (integer). Contohnya 7 jika dibagi 5 hasilnya 1 dan sisanya 2. Jadi 7 mod 5 = 2. Jika a mod $m = r$ maka $a = mq + r$ dengan $0 \le r < m$. Dalam contoh diatas a adalah 7, m adalah 5, q adalah 1, dan r adalah 2. Bilangan m disebut "modulus" atau modulo, dan hasil aritmetika modulo m terletak pada himpunan {0,1,2,...,m-1}. Hasil aritmetika modulo selalu bernilai positif. Sebagai contoh, hasil -41 mod 9 adalah 4 (-41 = 9 (-5) + 4) bukan -5 (-41 = 9 (-5) + (-5)). Jika a mod $m = 0$ berarti m adalah kelipatan a, yaitu a habis dibagi dengan m. Contohnya 8 mod 4 = 0, 4 adalah kelipatan 8, 8 habis ddibagi dengan 4.

Ada kemungkinan dua bilangan bulat, a dan b, memiliki sisa yang sama jika dibagi dengan bilagan bulat positif m. Ini artinya a dan b kongruen dalam modulo m dan ditulis sebagai

$$a \equiv b \pmod{m}$$

notasi '≡' dibaca 'kongruen'. Jika a tidak kongruen dengan b dalam modulo m maka ditulis

$$a \not\equiv b \pmod{m}$$

Contoh 5 mod 3 = 2 dan 17 mod 3 = 2, berarti $5 \equiv 17 \pmod 3$, sedangkan 7 mod 3 = 1 dan 11 mod 3 = 3 tidak kongruen, jadi $7 \not\equiv 11 \pmod 3$. Bentuk $a \equiv b \pmod m$ dapat pula dituliskan sebagai

$$a = b + km$$

k adalah sembarang bilangan bulat. Pembuktiannya adalah sebagai berikut:

Definisi formal dari kekongruenan adalah misalkan a

dan b adalah bilangan bulat dan m adalah bilangan > 0 , maka $a \equiv b \pmod m$ jika m habis membagi $a - b$, dapat ditulis $m \mid (a - b)$. Dan misalkan m dan n adalah dua buah bilangan bulat dengan syarat $n > 0$. Jika m dibagi dengan n maka terdapat dua buah bilangan bulat unik q (*quotient*) dan r (*remainder*), sedemikian sehingga $m = nq + r$ dengan $0 \le r < n$. Jadi jika m | (a – b) maka terdapat bilangan bulat k sedemikian sehingga $a - b = km$ atau $a = b + km$.

Karena $a \bmod m = r$ sama dengan $a = mq + r$ maka $a \bmod m = r$ dapat dituliskan sebagai

$$a \equiv r \pmod m$$

Sifat-sifat aritmetika modulo dinyatakan sebagai berikut:

Misalkan m adalah bilangan bulat positif.

1. Jika $a \equiv b \pmod m$ dan c adalah sembarang bilangan bulat maka
   (i) $(a + c) \equiv (b + c) \pmod m$
   (ii) $ac \equiv bc \pmod m$
   (iii) $a^p \equiv b^p \pmod m$ untuk suatu bilangan bulat tak negatif p
2. Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$ maka
   (i) $(a + c) \equiv (b + d) \pmod m$
   (ii) $ac \equiv bd \pmod m$

Berikut adalah bukti dari beberapa sifat di atas:

1(i) $a \equiv b \pmod m$
$\leftrightarrow a = b + km$
$\leftrightarrow a + c = b + km + c$
$\leftrightarrow (a + c) = (b + c) + km$
$\leftrightarrow (a + c) \equiv (b + c) \pmod m$

1(ii) $a \equiv b \pmod m$
$\leftrightarrow a = b + km$
$\leftrightarrow a - b = km$
$\leftrightarrow (a - b)c = ckm$
$\leftrightarrow ac = bc + Km$
$\leftrightarrow ac \equiv bc \pmod m$

2(i) $a \equiv b \pmod m \quad \leftrightarrow a = b + k_1 m$
$c \equiv d \pmod m \quad \leftrightarrow \underline{c = d + k_2 m}$ +
$\leftrightarrow (a+c) = (b+d) + (k_1+k_2)m$
$\leftrightarrow (a+c) = (b+d) + km$
$\leftrightarrow (a + c) \equiv (b + d) \pmod m$

2(ii) $a \equiv b \pmod m \quad \leftrightarrow a = b + k_1 m$
$c \equiv d \pmod m \quad \leftrightarrow \underline{c = d + k_2 m}$ *
$\leftrightarrow ac = bd+bk_2m+dk_1m+k_1k_2m$
$\leftrightarrow ac = bd+(bk_2+dk_1+k_1k_2)$m
$\leftrightarrow ac = bd+km$
$\leftrightarrow ac \equiv bd \pmod m$

Beberapa contoh :

Misalkan $17 \equiv 2 \pmod 3$ dan $10 \equiv 4 \pmod 3$, maka

$17 + 5 \equiv 2 + 5 \pmod 3 \leftrightarrow 22 \equiv 7 \pmod 3$ (sifat 1(i))

$17 . 5 \equiv 5 . 2 \pmod 3 \leftrightarrow 85 \equiv 10 \pmod 3$ (sifat 1(ii))

$17 + 10 \equiv 2 + 4 \pmod 3 \leftrightarrow 27 \equiv 6 \pmod 3$ (sifat 2(i))

$17 . 10 \equiv 2 . 4 \pmod 3 \leftrightarrow 170 \equiv 8 \pmod 3$ (sifat 2(ii))

Perhatikanlah pada sifat-sifat di atas tidak ada operasi pembagian karena jika kedua ruas dibagi dengan bilangan bulat maka kekongruenan tidak selalu dipenuhi. Contoh $10 \equiv 4 \pmod 3$ dapat dibagi dengan 2 karena 10 / 2 = 5 dan 4 / 2 = 2, dan $5 \equiv 2 \pmod 3$, tetapi $14 \equiv 8 \pmod 6$ tidak dapat dibagi dengan 2 karena 14 / 2 = 7 dan 8 / 2 = 4 tetapi $7 \not\equiv 4 \pmod 6$.

Kekongruenan lanjar adalah kongruen yang berbentuk

$$ax \equiv b \pmod m$$

dengan m adalah bilangan bulat positif, a dan b sembarang bilangan bulat, dan x adalah peubah. Bentuk kongruen lanjar berarti mencari nilai-nilai x yang memenuhi persamaan tersebut. Metode yang sederhana untuk menyelesaikan persamaan tersebut adalah dengan menggunakan $ax \equiv b \pmod m$ sama dengan $ax = b + km$ yang dapat ditulis sebagai

$$ax = b + km \rightarrow x = \frac{b + km}{a}$$

dengan k adalah sembarang bilangan bulat.

Contoh, misalkan kita akan menghitung solusi dari $4x \equiv 3 \pmod 9$, maka penyelesaiannya adalah sebagai berikut:

Kekongruenan $4x \equiv 3 \bmod 9$ ekivalen dengan menemukan k dan x bilangan bulat sedemikian sehingga

$$x = \frac{3 + k \cdot 9}{4}$$

Nilai k bilangan bulat yang menghasilkan x bulat adalah

$k = 0 \rightarrow x = (3 + 0 . 9) / 4 = 3/4$ (bukan solusi)
$k = 1 \rightarrow x = (3 + 1 . 9) / 4 = 3$
$k = 2 \rightarrow x = (3 + 2 . 9) / 4 = 21/4$ (bukan solusi)
$k = 3$ dan $k = 4$ tidak menghasilkan solusi
$k = 5 \rightarrow x = (3 + 5 . 9) / 4 = 12$
...
$k = -1 \rightarrow x = (3 + -1 . 9) / 4 = -6/4$ (bukan solusi)
$k = -2 \rightarrow x = (3 + -2 . 9) / 4 = -15/4$ (bukan solusi)
$k = -3 \rightarrow x = (3 + -3 . 9) / 4 = -6$
...
$k = -6 \rightarrow x = (3 + -6 . 9) / 4 = -15$

Jadi, nilai-nilai x yang memenuhi $4x \equiv 3 \bmod 9$ adalah 3,12,... dan -6,-15,... [1]

Sekarang jika kita akan mencari solusi bilangan bulat terkecil yang memenuhi kondisi jika bilangan bulat ini positif bersisa 1 jika dibagi 3, bersisa 2 jika dibagi 5, dan bersisa 3 jika dibagi 7 maka solusinya bisa dicari dengan menggunakan *chinese remainder theorem*. *Chinese remainder theorem* ini adalah jika diberikan sistem kongruensi

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$x \equiv a_3 \pmod{m_3}$
...
$x \equiv a_r \pmod{m_r}$

dimana $m_1,m_2,...,m_r$ adalah bilangan bulat positif yang relatif prima maka kita dapat mencari x dengan persamaan

$x \equiv (a_1M_1y_1 + a_2M_2y_2 + ... + a_rM_ry_r) \pmod M$

dimana

$M = m_1 \cdot m_2 \cdot ... \cdot m_r$

$M_k = M / m_k$ untuk setiap $k = 1$ sampai $k = r$

Dan y_k adalah invers dari M_k modulo m_k untuk setiap k = 1 sampai $k = r$

Sekarang kita cari solusi x dari contoh di atas.

$x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 7$

Karena 3, 5, dan 7 relatif prima jadi kita bisa menggunakan rumus *chinese remainder theorem*.

Pertama cari nilai M yaitu $M = 3 \cdot 5 \cdot 7 = 105$

Lalu cari nilai M_k untuk $k = 1$ sampai $k = r = 3$

$M_1 = 105 / 3 = 35$

$M_2 = 105 / 5 = 21$

$M_3 = 105 / 7 = 15$

Berikutnya cari nilai y_k untuk $k = 1$ sampai $k = r = 3$

$35y_1 \equiv 1 \pmod 3 \leftrightarrow 2y_1 \equiv 1 \pmod 3$

$\leftrightarrow y_1 = 2$

$21y_2 \equiv 1 \pmod 5 \leftrightarrow 1y_2 \equiv 1 \pmod 5$

$\leftrightarrow y_2 = 1$

$15y_3 \equiv 1 \pmod 7 \leftrightarrow 1y_3 \equiv 1 \pmod 7$

$\leftrightarrow y_3 = 1$

Sekarang tinggal memasukkan semua elemen ke dalam rumus

$x \equiv (1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1) \pmod{105}$

$x \equiv 157 \pmod{105}$

$x \equiv 52 \pmod{105}$

Dengan demikian, $x \equiv 52 \pmod{105}$ yang memenuhi ketiga kongruen tersebut. Dengan kata lain, 52 adalah solusi unik modulo 105.

Aplikasi *chinese remainder therorem* selain untuk *secret sharing* yaitu untuk algoritma RSA. Dalam algoritma RSA perhitungan menggunakan modulo n, dimana n adalah hasil perkalian dua bilangan prima p dan q yang mana kadang-kadang bilangan tersebut besar, perhitungan akan sangat memakan waktu, dengan *chinese remainder theorem* perhitungan akan semakin cepat. Selain itu *chinese remainder theorem* juga dapat digunakan untuk membangun urutan penomoran Gödel secara elegan yang dibutuhkan untuk membuktikan teorema ketidaklengkapan Gödel, algoritma transformasi cepat Fourier Good-Thomas, dan teorema Dedekin [2].

III. SECRET SHARING

Secret sharing ditemukan oleh Adi Shamir seorang kriptografer dari Israel dan George Blakey seorang kriptografer dari Amerika Serikat sendiri-sendiri pada tahun 1979. Dalam metode *secret sharing* ada seorang pembagi dan *n* pemegang bagian. Pembagi memberikan rahasia kepada pemegang bagian jika suatu syarat tertentu terpenuhi. Pembagi melakukannya dengan membagi masing-masing pemegang bagian suatu bagian dengan suatu cara hingga sejumlah *t* (*threshold* – batas ambang) pemegang bagian dapat merekonstruksi kembali rahasia tersebuat secara bersama-sama tapi jika jumlah pemegang bagian kurang dari *t* maka rahasia tidak dapat direkonstruksi. Sistem ini dinamakan sistem skema ambang (*n*,*t*).

Sebagai contoh misalkan ada seseorang yang menyimpan suatu rahasia di dalam lemari besi yang memiliki tiga kunci. Orang inilah yang menjadi pembagi. Orang kaya ini mendesain agar lemari besi tersebut hanya bisa dibuka jika ada tiga orang yang memiliki kunci membuka lemari besi ini bersama-sama. Tiga orang ini adalah *t*. Orang kaya ini kemudian membuat kunci ini menjadi empat kunci dan membagikannya kepada orang-orang kepercayaannya. Empat orang ini adalah *n*. Tiga orang dari empat orang kepercayaannya ini bisa membuka lemari besi sedangkan jika kurang dari tiga orang tidak bisa.

Ada beberapa skema dalam *secret sharing* ini, contohnya skema Shamir dan skema Blakley. Skema Shamir didasarkan pada interpolasi polinomial untuk menemukan *S* dari satu bagian tertentu, dan skema *secret sharing* geometri George Blakley menggunakan metode geometri untutk merekover rahasia *S*. Skema *secret sharing threshold* yang didasari oleh *chinese remainder theorem* adalah Mignotte dan Asmuth-Bloom, skema-skema ini menggunakan rangkaian bilangan bulat khusus bersama dengan *chinese remainder theorem*.

Chinese remainder theorem memiliki metode untuk menentukan *S* modulo *k* beberapa bilangan bulat yang relatif prima $m_1,m_2,...,m_k$, dengan $S < \prod_{i=1}^{k} m_i$. Idenya adalah mengkonstruksi satu skema yang akan membuat suatu rahasia *S* dalam beberapa *k* bagian (dalam kasus ini, sisa *S* modulo dari masing-masing m_i), jika kurang dari *k* maka rahasia tidak akan dapat diketahui. Pada akhirnya kita memilih n bilangan bulat relatif prima $m_1 < m_2 < ... < m_n$ sedemikian sehingga *S* lebih kecil daripada hasil kali tiap pilihan *k* dari bilangan bulat tersebut tapi tetap lebih besar dari setiap pilihan *k-1* tersebut. Lalu bagian $s_1,s_2,...,s_n$ didefinisikan oleh $s_i = S \bmod m_i$ untuk $i = 1,2,...,n$. Dengan cara ini berkat *chinese remainder theorem* kita bisa menentukan *S* dari sejumlah *k* atau lebih bagian tapi tidak lebih kecil dari *k*. Inilah yang disebut sebagai struktur akses *threshold*.

Kondisi ini dalam *S* juga dapat dianggap sebagai $\prod_{i=n-k+2}^{n} m_i < S < \prod_{i=1}^{k} m_i$. Jika *S* lebih kecil dari hasil perkalian terkecil dari *k* bilangan bulat, maka *S* ini akan lebih kecil dari hasil kali berapapun *k-1* bilangan bulat. Dan juga jika *S* lebih besar daripada hasil kali terbesar dari *k-1* bilangan bulat, maka *S* ini akan lebih besar dari hasil kali berapapun *k-1* [3].

Ada dua skema *secret sharing* yang memanfaatkan ide dasar ini, yaitu skema Mignotte dan skema Asmuth-Bloom.

Seperti disebutkan sebelumnya, skema Mignotte selain menggunakan *chinese remainder theorem* juga

menggunakan rangkaian bilangan bulat khusus yang disebut rangkaian (*k*,*n*)-Mignotte yang terdiri dari *n* bilangan bulat, koprima berpasangan, sedemikian sehingga hasil kali dari *k* terkecil lebih besar daripada hasil kali *k-1* yang terbesar. Kondisi ini sangat penting karena skema ini dibangun berdasarkan rahasia yang dipilih sebagai bilangan bulat antara dua hasil kali, dan kondisi ini menunjukkan bahwa paling tidak *k* bagian dibutuhkan untuk merekover rahasia sepenuhnya, bagaimanapun cara *k* dipilih.

Secara formal, anggap $n \geqslant 2$ suatu bilangan bulat, dan *k* suatu bilangan bulat sedemikian sehingga $2 \leqslant k \leqslant n$. Sebuah rangkaian (*k*,*n*)-Mignotte adalah sebuah rangkaian terurut membesar dari bilangan bulat positif $m_1 < ... < m_n$, dengan $(m_i,m_j) = 1$ untuk semua $1 \leqslant i < j \leqslant n$ sedemikian sehingga $m_{n-k+2}...m_n < m_1...m_k$. Kita sebut rentang ini rentang yang disahkan. Sekarang skema ini bekerja sebagai berikut: kita bangun sebuah skema *secret sharing* (*k*,*n*)-*threshold*. Kita pilih rahasia *S* sebagai sembarang bilangan bulat dalam rentang yang disahkan. Kita hitung untuk setiap $1 \leqslant i \leqslant n$, reduksi modulo m_i dari *S* yang kita sebut s_i adalah bagian. Sekarang untuk setiap *k* bagian yang berbeda $s_{i_1}, ..., s_{i_k}$, kita pandang sistem kongruensi

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

Dengan *chinese remainder theorem*, karena $m_{i_1}, ..., m_{i_k}$ adalah koprima berpasangan, sistem memiliki solusi unik modulo $m_{i_1}...m_{i_k}$. Dengan konstruksi dari bagian-bagian kita, solusi ini tidak lain adalah rahasia S untuk direkover.

Skema Ashmut-Bloom juga menggunakan rangkaian bilangan bulat khusus. Anggap $n \geqslant 2$ suatu bilangan bulat, dan *k* suatu bilangan bulat sedemikian sehingga $2 \leqslant k \leqslant n$. Kita pandang sebuah rangkaian bilangan bulat positif koprima berpasangan $m_0 < ... < m_k$ sedemikian sehingga $m_0.m_{n-k+2}...m_n < m_1...m_k$. Dari rangkaian yang diberikan ini, kita pilih suatu rahasia *S* sebagai sembarang bilangan bulat dalam himpunan $\mathbb{Z}/m_0\mathbb{Z}$.

Kita ambil sembarang bilangan bulat α sedemikian sehingga $S + \alpha.m_0 < m_1...m_k$. Kita hitung reduksi modulo m_i dari $S + \alpha.m_0$, untuk semua $1 \leqslant i \leqslant n$, ini adalah suatu bagian $I_i = (s_i,m_i)$. Sekarang, untuk setiap *k* bagian yang berbeda $I_{i_1}, ..., I_{i_k}$, kita pandang sistem kongruensi

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

Dengan *chinese remainder theorem*, karena $m_{i_1}, ..., m_{i_k}$ koprima berpasangan, sistem memiliki solusi unik S_0 modulo $m_{i_1}...m_{i_k}$. Dengan rekonstruksi bagian-bagian kita, rahasia *S* adalah reduksi modulo m_0 dari S_0.

Penting untuk diperhatikan bahwa skema Mignotte dan Asmuth-Bloom bukanlah skema yang sempurna, dalam arti bahwa sejumlah bagian yang kurang dari *k* mengandung beberapa informasi mengenai rahasia. Namun demikian, dengan pilihan rangkaian dan parameter (α dalam kasus Asmuth-Bloom) yang cocok seseorang bisa mendapat faktor keamanan yang layak. Inilah mengapa skema Asmuth-Bloom lebih aman, karena melibatkan lebih banyak sembarang parameter.

Sebagai contoh misalkan $k = 3$ dan $n = 4$. Bilangan bulat koprima berpasangan kita yaitu $m_0 = 3$, $m_1 = 11$, $m_2 = 13$, $m_3 = 17$ dan $m_4 = 19$. Bilangan-bilangan tersebut memenuhi sebagai rangkaian Asmuth-Bloom yang diperlukan karena 3.17.19 < 11.13.17. Kita pilih rahasia kita adalah 2. Pilih $\alpha = 51$, angka ini memenuhi kondisi yang diperlukan untuk skema Asmuth-Bloom. Kemudian $2 + 51 \cdot 3 = 155$ dan kita hitung bagian-bagian dari tiap bilangan bulat 11, 13, 17, dan 19. Hasilnya masing-masing 1, 12, 2, dan 3. Kita pandang sistem kekongruenan berikut:

$$\begin{cases} x \equiv & 1 \bmod 11 \\ x \equiv & 12 \bmod 13 \\ x \equiv & 2 \bmod 17 \end{cases}$$

Untuk menyelesaikan sistem, hitung $M = 11 \cdot 13 \cdot 17$. Dari algoritma konstruktif untuk menyelesaikan sistem tersebut diketahui bahwa solusi untuk sistem tersebut adalah $x_0 = 1 \cdot e_1 + 12 \cdot e_2 + 2 \cdot e_3$, dimana tiap e_i didapat dengan cara sebagai berikut:

Dengan identitas Bezout, karena $(m_i,M / m_i) = 1$, terdapat bilangan bulat positif r_i and s_i, yang dapat ditemukan dengan menggunakan algoritma euclidean lanjut, sehingga $r_i.m_i + s_i.M / m_i = 1$. Himpunan $e_i = s_i \cdot M_i/m_i$.

Dari identitas, 1 = 1 . 221 -20 . 11 = (-5) . 187 + 72 . 13 = 5 . 143 + (-42) . 17, kita dapat bahwa $e_1 = 221$, $e_2 = –935$, $e_3 = 715$, dan solusi unik modulo $11 \cdot 13 \cdot 17$ adalah 155. Jadi $S = 155 \equiv 2 \mod 3$ [4].

IV. KESIMPULAN

Teorema bilangan bulat memiliki kegunaan yang sangat banyak, terutam dalam bidang kriptografi. Contohnya adalah *chinese remainder theorem* yang merupakan aplikasi teorama bilangan bulat yang dapat digunakan untuk suatu metode penyimpanan rahasia yaitu *secret sharing*. Dengan penggunaan *chinese remainder theorem* maka rahasia akan semakin sulit dibongkar.

REFERENCES

[1] Munir, Rinaldi, *Matematika Diskrit*, Penerbit Informatika, 2005 halaman 191 - 200

[2] http://en.wikipedia.org/wiki/Chinese_remainder_theorem
Diakses tanggal 11 Desember 2010 pukul 23.37

[3] http://en.wikipedia.org/wiki/Secret_sharing
Diakses tanggal 10 Desember 2010 pukul 18.33

[4] http://en.wikipedia.org/wiki/Secret_sharing_using_the_Chinese_Remainder_Theorem
Diaskses tanggal 10 Desember 2010 pukul 18.34

[5] http://mathmagics.wordpress.com/2009/12/18/chinese-remainder-theorem/
Diakses tanggal 11 Desember 2010 pukul 23.37

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, 16 Desember 2010

Dimas Gilang Saputra - 13509038