DINING CRYPTOGRAPHERS PROTOCOL DAN PAILLIER CRYPTOSYSTEM

Stevie Giovanni – NIM : 13506054

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16054@students.if.itb.ac.id

Abstrak

Protokol adalah suatu kesepakatan antara dua orang atau lebih untuk berkomunikasi. Protokol berisi aturan-aturan mengenai bagaimana komunikasi antara orang-orang tersebut akan dijalankan. Protokol kriptografi adalah suatu protokol yang menggunakan teknik-teknik kriptografi. Protokol kriptografi banyak digunakan untuk berbagi komponen rahasia untuk menghitung sebuah nilai, membangkitkan rangkaian bilangan acak, meyakinkan identitas orang lainnya (otentikasi), dan sebagainya antara orang-orang yang berpartisipasi dalam protokol tersebut.

Pada banyak literatur mengenai protokol kriptografi umumnya menekankan pada penggunaan protokol kriptografi untuk menjaga kerahasiaan data atau informasi, atau untuk otentikasi peserta yang terlibat. *Dining Cryptographers Protocol* menjadi menarik di sini, karena berlawanan dengan penggunaan protokol kriptografi pada umumnya, *dining cryptographers protocol* justru menekankan penggunaan protokol kriptografi untuk membentuk komunikasi yang sifatnya *anonymous*. *Dining cryptographers protocol* memungkinkan seorang anggota dalam sebuah kelompok untuk melakukan multicast data kepada seluruh member lainnya. Namun, walaupun pesan tersebut bersifat publik, *dining cryptographers protocol* menjamin bahwa identitas si pengirim pesan tidak diketahui.

Dalam makalah ini, penulis akan membahas mengenai *dining cryptographers protocol* secara mendetil dan mengapa protokol yang mungkin mulanya belum dirasakan kegunaannya ini dapat menjadi sangat berguna untuk menyelesaikan beberapa masalah sehari-hari. Selain itu penulis juga akan membahas mengenai *paillier cryptosystem*, salah satu kriptosistem yang menerapkan skema kriptosistem aditif homomorfik. Yang dimaksud dengan sifat aditif homomorfik adalah jika diberikan public key dan enkripsi dari m1 dan m2, dapat dihitung enkripsi dari m1 + m2. Akan dilihat bahwa sifat ini sangat berguna untuk kasus-kasus seperti pengambilan suara, di mana suara masing-masing orang sebelumnya dienkripsi terlebih dahulu, kemudian pada penghitungan hasil akhir, seluruh suara akan didekripsi sekaligus untuk mendapatkan jumlah suara keseluruhan.

Penulis melihat bahwa kedua hal ini, *dining cryptographers protocol* dan *paillier cryptosystem* dapat mendukung satu sama lain. Oleh karena itu, mendekati akhir makalah, penulis akan mencoba menggabungkan protokol konsep *dining cryptographers* dan *pailier cryptosystem*.

***Kata kunci**: Dining Cryptographers Protocol, Paillier Cryptosystem,* protokol kriptografi, *anonymous, multicast.*

1. Pendahuluan

Dalam dunia kriptografi, satu orang dengan orang lainnya berkomunikasi secara rahasia. Informasi yang mengalir disandikan ke dalam bentuk yang tidak dapat dimengerti lagi untuk menjaga keamanan data agar tidak jatuh ke tangan orang yang tidak berkepentingan. Banyak metode yang digunakan untuk melakukan hal tersebut. Enkripsi dan dekripsi pesan dapat menggunakan algoritma kriptografi modern maupun algoritma kriptografi klasik. Dalam algoritma kriptografi klasik, pengirim dan penerima informasi berbagi kunci enkripsi dan dekripsi yang sama, sedangkan dalam algoritma kriptografi modern dua buah kunci, kunci privat dan kunci publik, digunakan untuk enkirpsi dan

dekripsi pesan antara keduanya. Baik algoritma kriptografi klasik maupun algoritma kriptografi modern memerlukan protokol yang harus diikuti oleh peserta komunikasi dalam menyampaikan informasi. Protokol yang menggunakan teknik-teknik kriptografi disebut dengan protokol kriptografi.

Umumnya protokol kriptografi digunakan untuk menjaga kerahasiaan data dan otentikasi. Namun pada kenyataannya protokol kriptografi juga dapat digunakan untuk hal sebaliknya, yaitu menjaga kerahasiaan identitas pengirim pesan. Komunikasi antar dua orang atau lebih yang mengharuskan kerahasiaan identitas pengirim pesan dan peserta komunikasi disebut dengan *annonymous communication* atau komunikasi yang sifatnya anonimus. Salah satu protokol kriptografi yang mendukung komunikasi anonimus adalah *dining cryptographers protocol.*

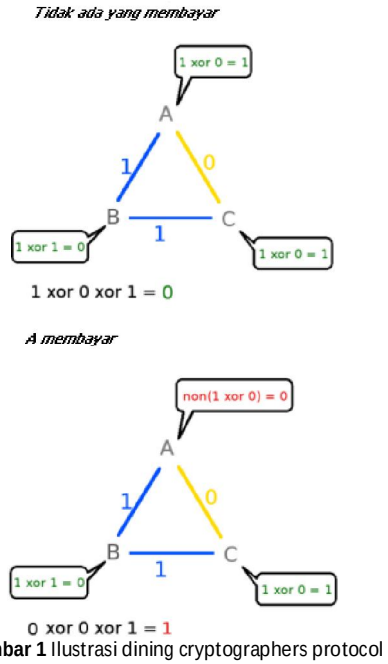
2. *Dining Cryptographers Protocol*

Dining cryptographers protocol adalah sebuah protokol kriptografi yang menjaga kerahasiaan identitas para peserta komunikasi. Dalam *dining cryptographers protocol*, pesan disiarkan secara publik kepada seluruh peserta protokol komunikasi tersebut dengan tetap menjaga kerahasiaan identitas pengirim pesan. *Dining cryptographers protocol* dicetuskan pertama kali oleh David Chaum pada tahun 1988.

Protokol ini bermulai dari permasalahan yang disebut dengan *dining cryptographers problem*. Rincian permasalahan tersebut adalah sebagai berikut. Tiga orang kriptografer Alice, Bob, dan Charlie mengunjungi sebuah rumah makan. Setelah selesai menyantap makanannya, ketiga kriptografer terkejut karena ternyata makan malam mereka sudah dibayar sebelumnya. Para kriptografer memikirkan dua kemungkinan. Kemungkinan pertama, salah satu dari mereka telah membayar makan malam tersebut. Kemungkinan kedua, makan malam tersebut dibayar oleh *National Security Agent*, tempat di mana mereka bekerja. Bagaimana cara mereka bisa mengetahui siapa yang membayar makan malam mereka? Seandainya makan malam dibayar oleh seorang kriptografer, dapatkah mereka tahu kriptografer mana yang membayar makan malam tersebut?

Solusi untuk hal tersebut adalah sebagai berikut. Tiap pasang kriptografer melempar koin secara rahasia. Dalam hal ini Alice melempar koin dengan Bob, lalu dengan Charlie, kemudian Charlie dengan Bob. Kemudian, masing-masing kriptografer berdiri dan menyatakan *different* jika kedua lemparan berbeda (*head* dan *tail*) atau *same* jika kedua lemparan sama (*head* dan *head* atau *tail* dan *tail*). Jika ternyata pembayaran dilakukan oleh salah satu kriptografer, demi menjaga rahasianya, kriptografer yang membayar harus berbohong dan mengatakan sebaliknya. Setelah semua kriptografer menyatakan *different* atau *same*, jumlah *different* dihitung. Jika jumlahnya ganjil, berarti pembayaran dilakukan oleh salah satu kriptografer, sedangkan jika jumlahnya genap, maka pembayaran dilakukan oleh *NSA*.

Untuk membuktikan hal ini, kondisi *different* ganjil tidak mungkin dicapai kecuali ada salah satu kriptografer yang berbohong. Jika dua dari tiga kriptografer menyatakan *same*, semestinya kriptografer ketiga juga menyatakan *same*, dan jika dua dari kriptografer menyatakan *different* kriptografer ketiga semestinya menyatakan *same*. Pada kedua kasus jumlah *different* genap. Jika ada kriptografer yang berbohong, berarti dialah yang membayar makan malam tersebut. Namun sayangnya tidak bisa dibuktikan siapakah yang berbohong. Sehingga identitas pembayar tidak diketahui. Berikut diberikan ilustrasi dari *dining cryptographers protocol.*



Gambar 1 Ilustrasi dining cryptographers protocol

3. Generalisasi *Dining Cryptographers Protocol*

Dining cryptographers protocol dapat dimodifikasi agar dapat bekerja untuk kasus-kasus yang melibatkan lebih dari tiga orang partisipan. Berikut adalah langkah-langkahnya.

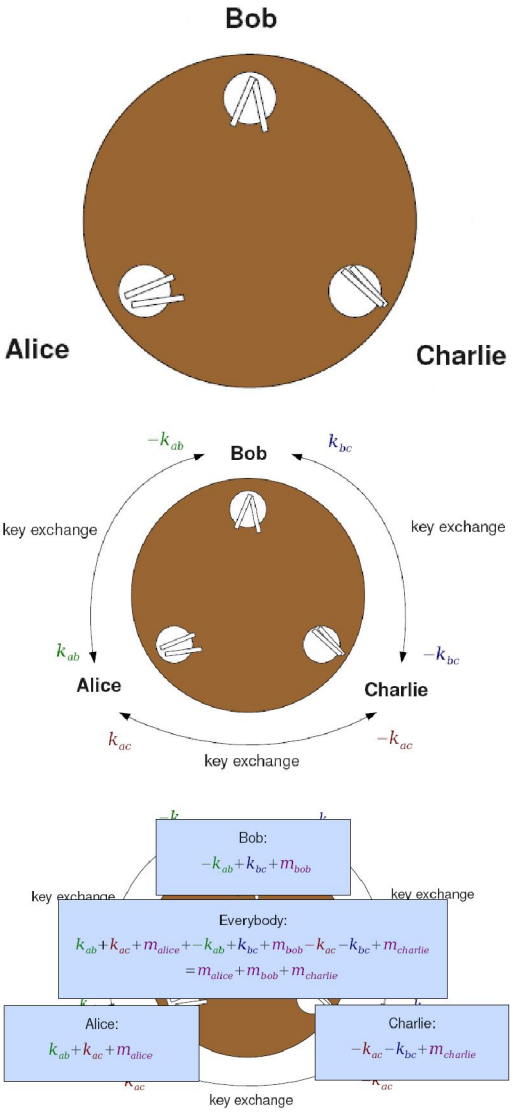
- Tiap pasang kriptografer memiliki sebuah kunci rahasia berupa bit 1 atau 0.
- Tiap kriptografer menjumlahkan semua kunci rahasia yang dimiliknya.
- Jika ada kriptografer yang membayar, dia harus berbohong dan menambahkan satu pada jumlah angka yang dimilikinya. tambahan satu di sini dapat berarti seorang kriptografer mengirimkan sinyal satu bit tanpa secara anonimus.
- Tiap kriptografer mengumumkan angka yang didapat olehnya.
- Seluruh angka dijumlahkankemudian dikenakan operasi modulo dua.
- Jika hasilnya adalah satu, maka seorang kriptografer membayar (sinyal satu bit terkirim ke seluruh partisipan dengan sukses secara anonimus). Jika hasilnya 0, tidak ada kriptografer yang membayar (tidak ada pesan yang dikirim).

Hal ini dapat terjadi karena jika tidak ada kriptografer yang berbohong, semua bit kunci akan masuk ke dalam perhitungan sebanyak dua kali sehingga ketika dimodulo dua, hasilnya 0.

4. Penerapan Dining Cryptographer Protocol dalam berkirim pesan

Sebelumnya telah dibahas bagaimana *dining cryptographers protocol* dapat dipakai dalam pengiriman sinyal secara anonimus dengan peserta lebih dari atau sama dengan tiga orang. Pengiriman sinyal yang hanya satu bit tidak terlalu bermanfaat. Yang ingin kita lakukan adalah menerapkan *dining cryptographers protocol* untuk berkirim pesan lebih dari satu bit. Untuk itu *dining cryptographers protocol* harus dimodifikasi lebih jauh lagi.

Jika sebelumnya *dining cryptographers protocol* menggunakan metode *coin flip* atau pelemparan koin secara rahasia untuk tiap pasang kriptografer, yang berarti kunci rahasia hanya berupa bit 0 atau 1, sehingga dengan operasi modulo dua di akhir protokol bisa didapatkan sinyal 1 jika ada kriptografer yang mengirim sinyal atau 0 jika tidak ada kriptografer yang mengirim sinyal, kali ini kunci rahasia dapat berupa apapun. Triknya adalah untuk tiap kunci rahasia k yang digunakan oleh sepasang kriptografer, seorang kriptografer harus memegang k, sedangkan kriptografer lain harus memegang –k. Berikut akan kita lihat bagaimana protokol tersebut dapat bekerja.



Gambar 2 *Dining cryptographers protocol* untuk berkirim pesan lebih dari 1 bit

Penjelasan dari gambar tersebut adalah :

- Bob, Alice, dan Charlie duduk di sebuah meja makan.
- Tiap pasang kriptografer menukarkan kunci rahasia (*key exchange*).
- Jika Alice adalah a, Bob adalah b, dan Charlie adalah c. Maka terdapat tiga buah kunci rahasia k_{ab}, k_{bc}, k_{ac}.

- Untuk tiap pasang kriptografer, jika salah satu memegang k, maka yang lain harus memegang –k. Pada gambar di atas Alice memegang k_{ab} dan k_{ac}, Bob memegang $-k_{ab}$ dan k_{bc}, dan Charlie memegang $-k_{ac}$, dan $-k_{bc}$.
- Selanjutnya, masing-masing kriptografer menjumlahkan kuncinya masing-masing. Pada tiap putaran, satu kriptografer akan menambahkan pesan rahasianya (m_{alice}, m_{bob}, atau $m_{charlie}$) ke dalam jumlah kunci rahasianya.
- Di akhir protokol, semua nilai yang diumumkan oleh tiap kriptografer dijumlahkan dan akan didapatkan pesan yang ingin disampaikan oleh kriptografer.

Dapat dilihat di sini mengapa syarat "untuk tiap pasang kriptografer yang berbagi kunci rahasia k, kriptografer satu harus memegang k sedangkan kriptografer lainnya memegang –k" harus dipenuhi. Pada tahap akhir, seluruh nilai yang diumumkan oleh para kriptografer akan dijumlahkan.

$k_{ab} + k_{ac} + m_{alice} + -k_{ab} + k_{bc} + m_{bob} + -k_{ac} + -k_{bc} + m_{charlie} = m_{alice} + m_{bob} + m_{charlie}$

Tiap dua kunci rahasia akan saling mengeliminasi dan meninggalkan pesan dari kriptografer di akhir protokol.

Dapat kita lihat bahwa *dining cryptographers protocol* juga memiliki batasan lain yaitu dalam satu putaran, hanya terdapat satu kriptografer yang boleh mengirim pesannya. Jika hal ini tidak dipenuhi, maka pada penjumlahan akhir, pesan-pesan para kriptografer akan bercampur dan menjadi pesan yang tidak dapat dimengerti lagi.

5. Kelemahan serta batasan *dining cryptographers protocol*

Dining cryptographers protocol memiliki beberapa kelemahan dan batasan antara lain :

- *Collision*-pada *dining cryptographers protocol*, jika ternyata ada dua orang yang mengirim pesan tersebut, maka pesan mereka akan menimbulkan tabrakan dan menghancurkan pesan tersebut. Bahkan *collision* dapat digunakan untuk mengungkap identitas pengirim pesan.
- *Disruption*-semua peserta harus mengikuti protokol tersebut dengan baik agar protokol dapat bekerja dengan benar. Jika ada kriptografer yang berbohong maka protokol akan kacau.
- *Complexity*-tiap kriptografer harus mempunyai satu kunci rahasia dengan tiap kriptografer lainnya adalah suatu kondisi yang sulit jika terdapat banyak kriptografer dalam komunikasi.

6. *Paillier Cryptosystem*

Sebuah kriptosistem adalah serangkaian algoritma yang digunakan untuk mengenkripsi dan mendekripsi pesan. Sebuah kriptosistem terdiri dari algoritma pembangkitan kunci, algoritma enkripsi, dan algoritma dekripsi. *paillier cryptosystem* adalah kriptosistem yang dikembangkan oleh Pascal Paillier pada tahun 1999.Algoritma pembangkitan kunci, enkripsi dan dekripsi kriptosistem paillier adalah sebagai berikut :

Pembangkitan kunci :

- Pilih dua bilangan prima p dan q secara random
- Hitung n = pq dan λ = lcm(p – 1, q – 1)
- Pilih bilangan bulat random g di mana $g \in \mathbb{Z}_{n^2}^*$
- Periksa n agar memenuhi
  $\mu = (L(g^{\lambda} \mod n^2))^{-1} \mod n$
  Dimana L adalah
  $$L(u) = \frac{u-1}{n}$$
- Kunci publik adalah (n,g) dan kunci privat adalah (λ,μ)

Enkripsi :

- Jika m adalah pesan yang akan dienkripsi dimana $m \in \mathbb{Z}_n$
- Pilih nilai r random di mana $r \in \mathbb{Z}_n^*$
- Maka cipherteks c adalah
  $c = g^{m} \cdot r^{n} \mod n^2$

Dekripsi :

- Jika c adalah cipherteks di mana $c \in \mathbb{Z}_{n^2}^*$
- Plainteks m adalah
  $m = L(c^{\lambda} \mod n^2) \cdot \mu \mod n$

Kriptosistem paillier mengandalkan sifat homomorfik aditif dari sebuah kriptosistem. Sifat homomorfik aditif ini memberikan beberapa keuntungan sebagai berikut :

$$\forall m_1, m_2 \in \mathbb{Z}_n \quad \text{and} \quad k \in \mathbb{N}$$

$$\mathrm{D}(\mathrm{E}(m_1)\,\mathrm{E}(m_2) \bmod n^2) = m_1 + m_2 \bmod n$$

$$\mathrm{D}(\mathrm{E}(m)^k \bmod n^2) = km \bmod n$$

$$\mathrm{D}(\mathrm{E}(m_1)\,g^{m_2} \bmod n^2) = m_1 + m_2 \bmod n$$

$$\left.\begin{array}{l}\mathrm{D}(\mathrm{E}(m_1)^{m_2} \bmod n^2)\\ \mathrm{D}(\mathrm{E}(m_2)^{m_1} \bmod n^2)\end{array}\right\} = m_1 m_2 \bmod n\ .$$

Salah satu keuntungan yang paling berguna adalah hasil kali dari enkripsi pesan m1 dan enkripsi pesan m2 bisa didekripsi untuk mendpatkan nilai m1 + m2. Fitur ini sangat berguna misalnya dalam *electronic voting*. Bayangkan dalam sebuah pemilihan suara, seorang pemilih dapat memilih *for* (1) atau *against (0).* Setiap pemilih mengenkripsi pilihannya sebelum dimasukkan di bilik suara. Petugas pemilihan kemudian menghitung hasil kali semua suara kemudian mendekripsinya untuk mendapatkan jumlah suara yang memilih *for*. Nilai random r dalam proses enkripsi menjamin tidak ada dua suara yang ekivalen yang akan menghasilkan cipherteks yang sama. Hal ini akan menjaga privasi dari para pemilih.

7. Pengembangan lebih lanjut *dining cryptographers protocol* dengan *paillier cryptosystem*

Walaupun dengan menggunakan kriptosistem paillier, jika pesan tiap individu di dekripsi secara terpisah, maka suara yang dimasukkan oleh setiap pemilih tetap dapat diketahui dengan mudah. Orang yang memasukkan suaranya dapat dilacak dan privasi pemilih suara tidak dapat dijaga. Di lain pihak, pada penjelasan mengenai *dining cryptographers protocol* sebelumnya, belum ada implementasi algoritma enkripsi dan dekripsi yang benar-benar diterapkan.

Penulis melihat bahwa kedua teknik yang telah dibicarakan sebelumnya, *dining cryptographers protocol* dan *paillier cryptosystem* memiliki keterkaitan yang kuat. Kedua teknik tersebut sama-sama melibatkan sekumpulan orang yang berbagi pesan rahasia di mana identitas si pengirim pesan disembunyikan demi menjaga privasi si pengirim pesan. Karena hal inilah penulis ingin mencoba mengembangkan *dining cryptographers protocol* dengan menggunakan kriptosistem paillier. Penulis menamakan protokol ini *Paillier's Midnight Feast* atau jamuan makan tengah malam Paillier. Penjelasan protokol tersebut adalah sebagai berikut.

Paillier berencana untuk mengadakan pesta jamuan makan malam dan mengundang teman-teman kriptografernya. Paillier adalah seorang dermawan yang ingin sekaligus mengumpulkan dana dari kawan-kawannya untuk disumbangkan ke yayasan kriptografer sedunia. Tidak semua teman-teman Paillier yang datang tentunya ingin menyumbang. Paillier menghargai privasi teman-temannya dan tidak ingin mengetahui berapa sumbangan teman-temannya tersebut. Untuk itu Paillier memikirkan sebuah cara untuk memastikan hal tersebut. Cara tersebut adalah :

- Pertama Paillier membangkitkan dua bilangan prima p dan q secara random
- Paillier menghitung n = pq dan λ = lcm(p – 1, q – 1)
- Paillier kemudian memilih bilangan bulat random g di mana $g \in \mathbb{Z}_{n^2}^*$
- Paillier memastikan n agar memenuhi
  $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$
  Dimana L adalah
  $$L(u) = \frac{u-1}{n}$$
- Paillier mendapatkan kunci publik adalah (n,g) dan kunci privat adalah (λ,μ)
- Paillier kemudian mengenkripsi kunci publik beserta undangan berisi instruksi jamuan makan malam dengan kunci publik milik teman-temannya, kemudian mengirimnya ke orang yang bersangkutan.
- Paillier jg menginstruksikan semua temannya untuk saling berpasang-pasangan dan berbagi kunci rahasia lain. Satu orang temannya harus memiliki kunci rahasia dengan tiap temannya yang lain.
- Pada saat jamuan makan malam, Paillier meminta teman-temannya untuk menyumbangkan sejumlah dana ke dalam rekeningnya. Paillier menginstruksikan teman-temannya untuk mengenkripsi terlebih dahulu jumlah dana yang disumbangkan dengan kunci publik Paillier yang

sebelumnya dikirim ke teman-temannya dengan rumus

$$c = g^{m} \cdot r^{n} \mod n^2$$

Di mana m adalah jumlah sumbangan dan r acak asalkan $r \in \mathbb{Z}_n^*$.

- Jamuan makan berjalan dengan sukses.
- Kesokan harinya, Paillier mengecek rekeningnya dan mendapatkan hasil perkalian seluruh sumbangan teman-temannya yang sudah terenkripsi. Paillier kemudian menggunakan kunci privatnya untuk mendekripsi angka tersebut dengan rumus

$$m = L(c^{\lambda} \mod n^2) \cdot \mu \mod n$$

dan mendapaatkan jumlah dari seluruh sumbangan teman-temannya.

Dapat kita lihat di sini, protokol yang digunakan mengimplementasikan *dining cryptographers protocol* dan mengembangkannya menggunakan kriptosistem Paillier. Pembangkitan kunci, enkripsi, dan dekripsi dilakukan sama seperti pada kriptosistem Paillier. Namun sekarang ditambahkan metode untuk menjaga kerahasiaan identitas penyumbang.

Langkah enam menjadi penting karena Paillier tidak ingin sembarang orang untuk ikut ke pestanya atau mungkin tidak ingin reporter pencari berita datang untuk meliput jamuan makan malam hebat tersebut. Karena maksud tersebut, Paillier mengenkripsi kunci publiknya dengan kunci publik milik rekan-rekannya sehingga menjadi kunci semi-publik yang hanya diketahui oleh rekan-rekannya.

Kehebatan lainnya dibandingkan dengan *dining cryptographers protocol* biasa adalah sekrang pesan dapat dienkripsi. Pada *dining cryptographers protocol* sebelumnya, kita hanya bisa tau jumlah dari sumbangan secara manual dengan mendekripsi terlebih dahulu pesan dari masing-masing penyumbang. Dengan kata lain, penghitung mengetahui jumlah sumbangan masing-masing penyumbang, dalam kasus ini penghitung adalah Paillier. Dengan modifikasi *dining cryptographers protocol* Paillier cukup mengetahui hasil kali seluruh enkripsi jumlah sumbangan rekan-rekannya untuk dapat mendekripsinya menjadi jumlah sumbangan kesemua rekannya. Sifat homomorfik aditif dari kriptosistem Paillier digunakan di sini untuk mendapat jumlah seluruh sumbangan.

Satu keunggulan lain adalah bahwa protokol ini dirancang memang untuk pesan dengan tipe angka sehingga kelemahan *dining cryptographers protocol* yang mengharuskan hanya satu orang yang dapat mengirim pesan dalam tiap putaran menjadi tidak perlu dipedulikan.

8. Kesimpulan dan Saran

Selama pengerjaan makalah, penulis mendapatkan beberapa kesimpulan dan saran pengembangan ke depannya sebagai berikut :

- *Dining cryptographers protocol* menjamin kerahasiaan identitas pengirim pesan jika protokol tersebut diikuti dengan baik.
- Walaupun protokol ini secara general tidak dapat bekerja jika terdapat lebih dari satu pengirim pesan pada tiap putarannya, hal tersebut dapat menjadi keunggulan jika data yang dikirim adalah bilangan.
- Kriptosistem Paillier mendukung *dining cryptographers protocol* dengan memberikan fitur enkripsi kepada protokol tersebut.
- Penulis menyarankan pengembangan lebih lanjut terhadap protokol ini, misalnya sebuah mekanisme agar protokol ini dapat menjadi lebih praktis dan mudah digunakan.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. Kriptografi. Informatika Bandung, 2006

[2] http://www.cs.cornell.edu/People/egs/herbivore/dcnets.html

[3] *www.ece.cmu.edu/~adrian/731-sp04/readings/dcnets.html*

[4] *www.cs.st-andrews.ac.uk/~tws/teaching/cryptography/diningcrypto.pdf*

[5] *https://365.rsaconference.com/click.jspa?searchID=9096&objectType=38&objectID=13159*

[6] *http://www.gemplus.com/smart/rd/publications/pdf/Pai99pai.pdf*

[7] *http://www.ippari.unict.it/~catalano/Corsi/Tesi-Cap3-Paillier.pdf*

[8] http://en.wikipedia.org/wiki/Paillier_cryptosystem

[9] http://en.wikipedia.org/wiki/Dining_cryptographers_protocol