Penggunaan Blind Signature pada *e-voting*

Fakhri 13510048
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510048@std.stei.itb.ac.id

***Abstrak*— Pemilihan suara (voting) hingga saat ini secara umum dilakukan melalui kertas atau dapat disebut manual. Waktu pemrosesan dan biaya yang besar menyebabkan dibutuhkannya sistem yang lebih baik, salah satunya yaitu e-voting. Sistem ini cukup sulit diterapkan untuk skala besar, untuk kala pemerintahan negara, baru dua negara yang dapat mengimplementasikannya. Ini terjadi akibat e-voting yang dilakukan menggunakan komputer harus mengimplementasikan aspek keamanan yang dijamin kuat, minimal setara dengan sistem manual. Salah satu aspek keamanan tersebut adalah privasi pemilih suara.**

Dalam menjaga privasi pemilih suara digunakanlah metode 'Blind Signature' ini. Secara singkatnya, metode ini memungkinkan pengiriman data dengan menyembunyikan identitas pengirim. Blind Signature yang lebih spesifik mengarah kepada RSA-Blind signature yang merupakan Blind-Signature yang sangat mudah diaplikasikan. Dalam penerapannya pada e-voting, terdapat kelemahan yang memungkinkan adanya 'blinding attack' sehingga pesan dapat didekrip melalui proses blind signature pada pesan lain.

Dalam makalah ini akan dibahas metode pencegahan melalui modifikasi blind signature sehingga dapat menghindari secara total ataupun meminimalisir ancaman kesalahan sistem yang disengaja.

***Kata Kunci*—Blind Signature, *e-voting*, RSA.**

I. PENDAHULUAN

Tandatangan adalah alat yang digunakan oleh manusia dalam menyatakan otentikasi terhadap objek yang ditandatangani. Tandatangan telah dilakukan sejak dahulu untuk kepentingan antar pihak. Tandatangan bersifat unik antar probadi dan tidak dapat ditiru dengan utuh. Akibat hal inilah tandatangan sesorang pada objek tertentu dianggap sebagai otentikasi oleh orang tersebut.

Tandatangan yang diterapkan pada suatu objek pada umumnya khusus untuk objek nyata. Untuk objek dijital tidak dimungkinkan untuk menggunakan tandatangan nyata berupa gambar. Ini diakibatkan oleh mudahnya duplikasi dan modifikasi data seperti gambar sehingga metode tidak menjamin otentikasi seseorang. Oleh karena itu dibuatlah bentuk baru dalam menrapkan tandatangan untuk objek digital.

Tandatangan pada objek digital diterapkan dengan mengaitkannya terhadap keseluruhan isi objek dan kunci tertentu sehingga dapat diperiksa kebenaran tentang objek apa yang ditandatangani, lalu dapat diketahui kebenaran tentang penandatangan. Dapat disimpulkan bahwa secara umum tandatangan baik secara nyata maupun digital ditujukan untuk memenuhi syarat otentikasi dan anti-penyengkalan pada suatu objek.

Tandatangan digital ini telah digunakan hingga pada penerapan yang lebih lanjut, yaitu e-voting. Namun terdapat perubahan pada tanda tangan digital menjadi metode baru, yaitu blind signature. Blind Signature membuat pemberi tandatangan didak dapat mengetahui informasi khusus dari pengirim dokumen. Yang daat diketahui oleh pemberi tanda tangan hanyalah peran dari pengirim terhadap sistem dan lingkup wewenang / hak peminta tandatangan tersebut. Perihal ini adalah pengetahuan yang minimal dan cukup untuk memutuskan memberikan tanda tangan atau tidak.

Tandatangan nyata dapat dimanfaatkan untuk hal yang tidak diinginkan seperti dengan dilakukannya peniruan oleh pihak yang tidak diinginkan. Untuk tandatangan digital terdapat juga serangan-serangan yang dapat mengganggu penggunaannya. Serangan-serangan ini juga tergolong kepada algoritma pembangun di dalamnya seperti RSA dan SHA. Salah satu bentuk serangan tersebut adalah blinding attack. Dengan adanya serangan ini, pesan dapat didekrip melalui proses blind signature pada pesan lain.

II. DASAR TEORI

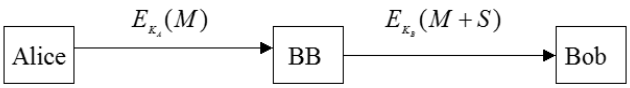
Terdapat dua bagian dalam penjelasan teori, yaitu tanda tangan dijital atau *digital signature, lalu blind signature.*

1. Digital Signature

   Penjelsan pada bagian ini berasal dari Munir (2005). Digital signature adalah alat yang digunakan untuk menjaga aspek otentikasi dan anti penyengkalan dalam kriptografi terhadap suatu data. Pembuatannya terinspirasi oleh tanda tangan pada dokumen cetak dengan sifat tidak dapat dilupakan, tidak dapat dipindahtangankan, tidak dapat disangkal, tergolong bukti otentik, dan dokument yang telah ditandatangani tidak dapat diubah. Meskipun menerapkan tanda tangan cetak pada dunia komputer, digital signature

menggunakan visualisasi dan pemebentukan yang berbeda. Apabila tanda tangan cetak menggunakan tandatangan yang berbasis perorangan sehingga untuk dokumen berbeda ditandatangani oleh orang yang sama akan menghasilkan tandatangan yang sama. Namun digital signature tidak demikian, tandatangan disesuaikan terhadap kunci yang diberikan pemberi tandatangan dan konten dari data keseluruhan, sehingga perbedaan kunci oleh orang yang sama ataupun tiap data dengan konten berbeda sekecil apapun akan menyebabkan perubahan pada digital signature. Penandatanganan dapat dilakukan menggunakan beberapa cara, yaitu kriptografi (simetri dan kunci publik) dan hash.

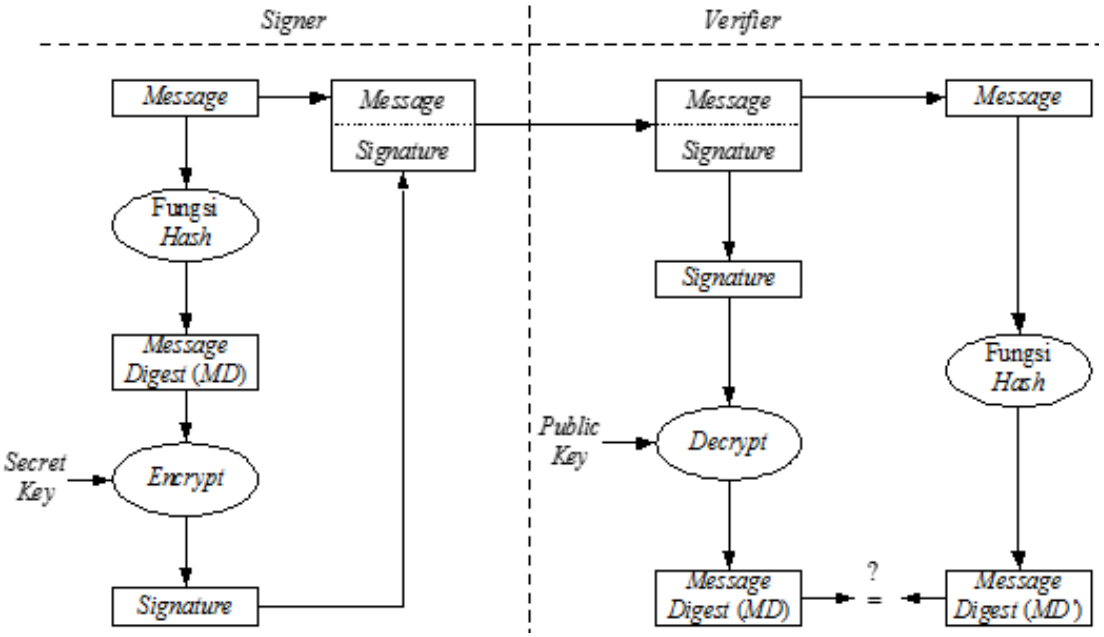
Pada penerapan digital signature dengan kriptografi simetri, tidak dilakukan secara biasa, yaitu sekedar dienkripsi, namun dibutuhkan beberapa penambahan untuk menutupi kekurangan metode ini. Hal yang ditambahkan adalah penggunaan pihak ketiga yang dipercaya pihak pengirim dan penerima sebagai arbitrase, lalu kunci simetri oleh pengirim terhadap pihak ketiga serta oleh penerima terhadap pihak ketiga dibedakan dan hanya diketahui oleh masing – masing set pihak tersebut. Hal ini dilakukan untuk menutupi kekurangan yaitu anti penyangkalan Tandatangan digital ini dibuat dengan proses enkripsi data sesuai dengan gambar 1.



Gambar 1 : Digital Signature dengan Enkripsi

Pada gambar 1 di atas digambarkan bahwa Alice ingin mengirimkan pesan kepada Bob. Alice Sebagai pengirim pesan atau dokumen melakukan enkripsi terhadap pesan $E_{KA}(M)$. Hasil enkripsi pesan diberikan kepada pihak ketiga yaitu BB. BB membuat tandatangan *S* sesuai pesan tersebut dengan terlebih dahulu mendikripsi pesan menggunakan kunci K_A. Pesan bersama dengan tandatangan dienkripsi dengan menggunakan kunci K_B, yaitu $E_{KB}(M + S)$ yang kemudian dikirimkan kepada Bob.Pesan yang diterima oleh Bob dapat dijamin berasal dari Alice karena BB dan Alice saja yang mengetahui K_A. Lalu Pesan tersebut tidak dapat disangkal oleh Alice karena pesan terebut telah diteruskan melalui BB.

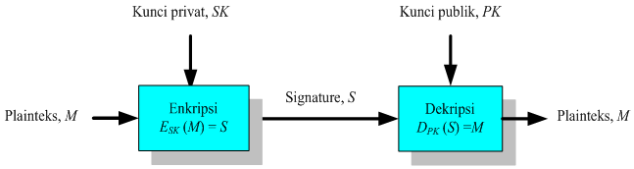
Pada penerapan digital signature dengan kriptografi kunci publik dilakukan dengan cara yang tidak seperti biasa. Kriptografi kunci publik biasa dilakukan dengan mengenkripsi pesan menggunakan kunci publik, lalu dekripsi menggunakan kunci prvat. Hal ini dibalikkan sehingga enkripsi dilakukan dengan menggunakan kunci privat dan dekripsi dilakukan dengan kunci publik (Diffie & Hellman). Hal ini dilakukan karena secara umum pemilik kunci publik lebih banyak dibanding kunci privat sehingga penerapan biasa dapat menyebabkan sumber pengirim yang tidak pasti. Pendeskripsian proses dapat dilihat pada gambar 2.



kriptografi kunci simetri. Sumber : Munir (2005)

Pada gambar 2, tandatangan *S* berasal dari pesan plainteks *M* dienkripsi menggunakan kunci privat *SK*, yaitu $E_{SK}(M) = S$ lalu penerima *S* melalkukan dekripsi menggunakan kunci publik *PK* sehingga menghasilkan pesan *M*, yaitu $D_{PK}(S) = M$.

Gambar 2 : Algoritma enkripsi menggunakan hash. Sumber Munir (2005)



Gambar 3 : Digital Signature menggunakan kriptografi kunci publik. Sumber Munir (2005)

Pada penerapan digital signature dengan hash dilakukan pula enkripsi kriptografi kunci simetri. Algoritma ini dejelaskan menggunakan diagram pada gambar 3. Sesuai gambar 3, pesan terlebih dahulu dihash sehingga menjadi ukuran tertentu yang tetap untuk pesan apapun dan sensitif terhadap perubahan pesan. Hash dapat dilakukan dengan metode hash apapun, namun yang paling umum digunakan adalah RSA dan ElGamal. Hasil hash adalah message digest yang kemudian dienkripsi dengan kunci privat layaknya teori Diffie & Hellman. Hasil enkripsi adalah signature dan disisipkan pada akhir pesan. Kemudian pesan dan signature ini dikirimkan ke tujuan. Penerima pesan melakukan pemisahan antara pesan dan signature. Signature didekrip dengna kunci publik dan pesan di hash kembali. Setelah itu dilakukan perbandingan message digest antara hasil dekripsi dan hasil hash. Melalui cara inilah digital signature dengan menggunakan hash dilakukan.

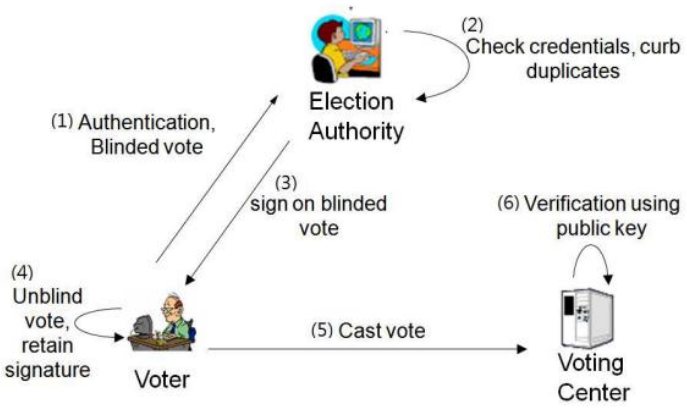
2. Blind Signature

Blind Signature digunakan sebagai protokol untuk hal-hal terkait privasi antar pesan dan pemberi tandatangan sehingga sangat aplikatif untuk kasus privasi pengirim pesan sebagai prioritas utama. Algoritma ini dikembangkan dari digital signature oleh Chaum (1983).

Blind Signature cocok untuk diaplikasikan pada sistem pemilihan dengan kriptografi (e-vote) dan skema uang digital (e-cash). Khusus untuk e-voting, blind signature diperlukan dengan fokus aspek untuk sisi integritas tiap pilihan (surat suara), yait harus divalidasi oleh pihak berwenang sebelum dapat disahkan untuk terhitung. Hal ini ditujukan untuk memeriksa hak memilih dan tidak memilih lebih dari satu. Namun perlu dijaga pula agar pihak berwenang ini tidak mengetahui seorang memilih apa. Sedangkan untuk e-cash, blind signature digunakan untuk menjaga agar nasabah suatu bank tidak dapat dilacak penggunaan uang dijitalnya dilakukan terhadap pihak mana. Hal ini diperlukan karena cakupan informasi yang dapat diperoleh pihak bank sangat besar dan privasi diperlukan untuk membatasi itu.

Secara umum, Blind signature dapat diibaratkan pada seorang user yang memiliki suatu dokumen rahasia. Dokumen rahasia ini tidak dapat diakses oleh pihak di atas user (bank/panitia pemilu). User ingin agar lembar dokumen tersebut ditandatangani oleh pihak di atasnya dan pihak di atas user tidak ingin adanya pembajakan tandatangan oleh user. Untuk kasus e-voting, pembajakan dapat mengancam adanya duplikasi pilihan.

Pada penerapannya, blind signature menggunakan hash dan eknkripsi kunci publik. Skema algoritma ini dapat dilihat pada gambar 4.



Gambar 4 : Diagram Blind Signature pada e-voting

Pada Gambar 4, voter atau pemilih terlebih dahulu diotentikasi dengan mengirimkan blinded vote kepada panitia pemilu atau election authority. Selnajutnya panitia pemilu memastikan pemilih dan mengirimkan blinded vote yang telah ditandatangani apabila pemilih berhak memilih. Pemilih membuka blinded vote karena dari awal telah mengetahui kunci publik dari blinded vote.

Jika dijelaskan pada konteks matematis, langkah pertama pemilih mengirim Ballot (*B*), hasil enkripsi dan hash pesan *(m),* yaitu

$$B = H(m).r^e \ldots\ldots\ldots\ldots(1)$$

dengan r^e adalah faktor random dengan kunci publik. Lalu panitia pemilihan melakukan pemeriksaan *B* dan memberikan balikan tandatangan yaitu persamaan (2)

$$Sign\ (B) = (H(m).r^e)^d \ldots.(2)$$
$$Sign\ (B) = H(m)^e.r.\ldots\ldots(3)$$

Persamaan (2) ini dapat didekrip oleh pemilih

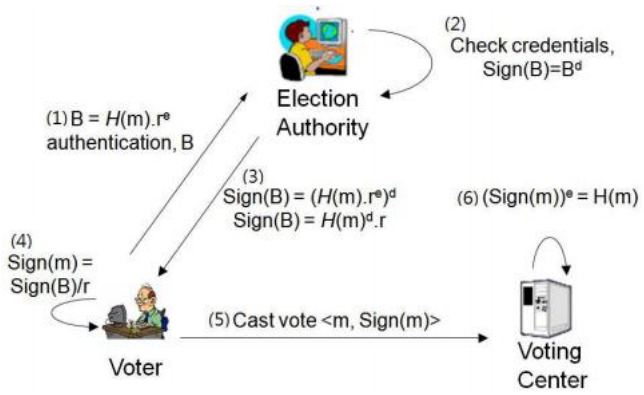
dengan kunci publik menjadi persamaan (3), lalu karena pemilih mengetahui faktor random random *r* maka dapat diperoleh *Sign(m)* melalui persamaan (4)

$$Sign(m) = Sign(B)/r = H(m)^d \ldots..(4)$$

Dari persamaan (4) diperoleh signature dari panitia pemilu. Setelah itu pemilih mengirimkan <*m, Sign(m)*> ke pusat pemilihan atau *voting center*. Pada pusat pemilihan input diproses menjadi persamaan (5).

$$(Sign(m))^e = H(m) \ldots.. (5)$$

Sehingga dapat divalidasi kembali antara hasil dari hash *m* dengan persamaan (5). Proses matematis ini digambarkan pada gambar 5.



Gambar 5 : Diagram Blind Signature secara matematis

Bentuk lain persamaan matematis adalah sebagai berikut:

$$m' \equiv mr^e \pmod N \ldots(6)$$

Dengan *m'* adalah pesan (blinding message) yang dikirim pemilih ke panitia pemilu pertama kali. r adalah bilangan random yang merupakan ekaponen publik *e* terhadap modulo *N* dan *r* relatif prima dengan *N*. Sehingga $r^e \bmod N$ adalah blinding factor yang random juga.

$$s' \equiv (m')^d \pmod N \ldots.(7)$$

s' adalah pesan balikan dari panitia pemilihan alias pesan buta (blinded message) bertandatangan. Pemilih dapat memisahkan blinding factor untuk memperoleh *s*.

$$s \equiv s'.r^{-1} \pmod N \ldots(8)$$

Persamaan di atas dapat diperoleh dengan menggunakan persamaan (10). Selanjutnya dapat diperoleh *s* yaitu tandatangan seutuhnya melalui persamaan (9).

$$s \equiv s'.r^{-1} \equiv (m')^d r^{-1} \equiv m^d r^{ed} r^{-1}$$
$$\equiv m^d r r^{-1} \equiv m^d \pmod N \ldots(9)$$

3. Blinding Attack

Serangan terhadap Blind Signature yang dapat dilakukan akibat hash pada blind signature pada umumnya menggunakan RSA. Konsep penyerangannya adalah melakukan dekrip pesan akibat penandatanganan pesan lain. Proses penandatanganan ekivalen dengan dekripsi pesan menggunakan kunci privat yang dimiliki penandatangan sehingga penyerang menyiapkan blinded message *m* yang dienkrip yaitu *m'* untuk ditandatangani.

$$r^{ed} = r \ldots..(10)$$

$$\begin{aligned} m'' &= m'.r^e \pmod N \\ &= (m^e \pmod N \,.\, r^e) \pmod N \\ &= (mr^e) \pmod N \ldots..(11) \end{aligned}$$

$$\begin{aligned} s' &= m''^{d} \pmod N \\ &= ((mr)^e \pmod N)^d \pmod N \\ &= (mr)^{ed} \\ &= mr \ldots\ldots..(12) \end{aligned}$$

Pada persamaan (11), adalah lanjutan dari persamaan (6) yang digunakan untuk persamaan (12). Pada persamaan (12), dilakukan pencarian *s'* sehingga disimpulkan pada persamaan (13).

$$m = s'.r^{-1} \pmod N \ldots(13)$$

Dari persamaan (13) dan persiapan menggunakan *m''* serta *s'*, maka dapat diperoleh informasi yang disembunyikan oleh pemilih, yaitu *m.*

III. ANALISIS DAN PERANCANGAN

Analisis dilakukan terhadap serangan pada skema algoritma ini, yaitu *blinding attack*.

A. *Analisis Kesalahan yang Dimanfaatkan*

Bagian dari algoritma ini yang dimanfaatkan dalam melakukan serangan adalah akibat penandatangan memberikan tandatangannya langsung pada pesan. Selain itu tandatangan dilkukan dengan mendekrip pesan terlebih dahulu. Hal inilah yang menjadi penyebab utama serangan ini dapat terjadi.

B. *Perancangan Solusi*

Terdapat beberapa solusi dalam mengatasi permasalahan ini. Satu solusi yang ditawarkan pada makalah ini adalah pembuatan mekanisme seleksi untuk *e* (kunci publik) dan *r* yang dapat digunakan oleh pemilih di awal sehingga memberikan nilai *m'* lain apabila terjadi kondisi seperti pada persamaan (11).

Dengan adanya pembatasan nilai ini, penyerang tidak dapat mempersiapkan *m''* dan *r* yang sesuai untuk dilanjutkan pada persamaan (12) hingga persamaan (13).

IV. IMPLEMENTASI

Implementasi dilakukan pada komputer dengan lingkunan pengembangan, yaitu :

1. Prosessor AMD E-350
2. RAM 2GB
3. OS Windows 7 Ultimate
4. Windows Visual Studio 2012
5. Bahasa Pemrograman C#

Implementasi dilakukan dengan memilih antara 'A', 'B, 'C', atau 'D' sebagai opsi pemilihan. Entitas seperti yang terdapat pada gambar 5 diimplementasikan sebagai kelas-kelas dalam program dengan method dan behaviour masing-masing.

Implementasi menggunakan prosedur RSA seperti biasa dan SHA untuk melakukan enkripsi serta dekripsi kunci publik. Algoritma implementasi yang dibuat adalah sebagai berikut :

1. Pemilih diberikan kunci publik
2. Pemilih mengisi lembar suara sesuai opsi pilihan
3. Lembar suara dienkrip menggunakan SHA dengan kunci publik dan random faktor yang disediakan oleh komputer
4. Lembar suara dikirim ke panitia
5. Panitia menandatangani pesan yang secara tidak langsung mendekripsi pesan
6. Panitia mengirimkan hasil tandatangan ke pemilih
7. Pemilih memisahkan nilai random faktor sehingga diperoleh tandatangan murni terhadap pulihan non enkrip dan non hash
8. Pesan dan tandatangan murni dikirimkan ke pusat pemilihan oleh pemilih
9. Pusat pemilih menghitung pilihan dengan mem-validasi pesan terebih dahulu

Bagian yang menjadi fokus adalah nomor 1 dan 3 yaitu pemberian kunci publik dan pemberian random faktor oleh komputer. Kunci publik yang diberikan telah diatur agar tidak memenuhi kondisi tertentu dan random faktor juga telah diatur agar tidak tergolong ke dalam kondisi nilai tertentu.

Penerapan ini tidak menimbulkan kecurigaan oleh pemilih karena fitur ini tidak memberikan dampak waktu proses yang lama, yaitu hanya menambahkan O(n) dengan n adalah kemungkinan nilai tergolong ke dalam kondisi penolakan.

Percobaan pada ini belum dapat memberikan hasil lebih lanjut sehingga status sementara menyatakan tidak adanya kesalahan untuk penerapannya.

V. KESIMPULAN

Menurut hasil implementasi yang telah dilakukan, penyeleksian *e* dan *r* dapat membantu meminimalkan blinding attack sehingga e-vote mengggunakan blind signature dapat lebih aman digunakan dalam bidang penjagaan privasi. Dengan langkah preventif seperti ini, blind signature dapat dihindari pula dari resiko serangan. Namun, tetap diperlukan pengembangan lebih jauh untuk menemukan cara yang lebih baik. Tergolong tidak baik karena metode ini membatasi *e* dan *r* yang digunakan sehingga mengancam menimbulkan permasalahan lain.

REFERENSI

[1] Munir, Rinaldi. (2005). *Tandatangan Digital – Bahan Kuliah IF3058 Kriptografi.*Institut Teknologi Bandung.

[2] Chen, R.J. (2010). *Blind Signature and Their Applications.* Chiao Tung University.

[3] EMC. *WHAT IS A BLIND SIGNATURE SCHEME?*. RSA Laboratories. http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/what-is-a-blind-signature-scheme.htm. Diunduh pada 16 Mei 2014 pukul 10:29 WIB.

[4] D. Chaum. (1983). *Blind signatures for untraceable payments, Advances in Cryptology - Crypto '82*, Springer-Verlag, 199-203.

[5] Juels, Ar.,. Luby, Michael., & Ostrovsky, Rafail. (2006). *Security of Blind Signature*. RSA Laboratiries.

[6] Salah I.K., Darwish, A., Oqeili, S. (2006). *Mathematical Attack on RSA Cryptosystem.* Journal of Computer Science 2 (8) : 665-671

[7] Balasooriya, A., Senanayake, K. (2012). *Blind Signature Scheme.*

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, 15 Mei 2014

Fakhri 13510048