Studi Terhadap Implementasi Key-Agreement Protocol pada Smart Card

Rizky Delfianto NIM : 13507032[1]

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]if17032@students.if.itb.ac.id

***Abstract* — Sejalan dengan perkembangan teknologi yang semakin maju, keamanan dalam melakukan transfer informasi atau pesan juga mau tidak mau harus maju pula. Teknologi sekarang sangat memungkinkan jenis atau macam serangan yang baru. Oleh karena itu, disinilah letak pentingnya protokol kriptografi. Protokol kriptografi merupakan protokol yang melakukan fungsi pengamanan dan menerapkan metode kriptografi. Protokol dalam proses kriptografi meliputi beberapa aspek : *Key-agreement, Entity Authentication, Symmetric Encryption, Secured application-level data transport,* dan *Non-repudation methods*. *Key-agreement* merupakan protokol dimana dua atau lebih pihak dapat menyetujui penggunaan sebuah kunci. Dengan begini dapat mencegah adanya pihak ketiga yang diluar pihak yang terlibat dalam mempengaruhi kunci yang disepakati.**

Perkembangan teknologi informasi juga memunculkan kebutuhan baru pada masyarakat, yaitu kebutuhan akan layanan yang baik dalam komunikasi khususnya aplikasi atau perangkat yang menggunakan teknologi *Smart Card*. Layanan ini meliputi keamanan dalam berkomunikasi. Kemanan pada aplikasi dan perangkat yang berteknologikan Smart Card ini akan banyak penggunaan kunci publik sehingga perlu adanya protokol yang mengaturnya. Disinilah *key-agreement protocol* berperan. Protokol inilah yang digunakan pada *Smart Card*.

Dalam *Smart Card* sendiri, *key-agreement protocol* yang digunakan bertipe AK (*Authenticated Key-Agreement Protocol*) yang mempunyai karakteristik *authenticated* dimana terjadi otentikasi dalam skema proses protokolnya. Selain itu, protokol yang digunakan juga menggunakan beberapa prinsip dari protokol Diffie-Hellman. Dalam makalah ini juga akan dijelaskan mengenai salah satu protokol yang seperti dijelaskan sebelumnya, menggunakan prinsip Diffie-Hellman dan bertipe AK, yang digunakan pada *Smart Card*, yaitu TP-AMP.

***Kata Kunci* — AK, Diffie-Hellman, Key-Agreement Protocol, Protokol kriptografi, Smart Card, TP-AMP.**

I. PENDAHULUAN

Protokol kriptografi merupakan protokol nyata atau abstrak yang melakukan fungsi pengamanan dan menerapkan metode kriptografi. Sebuah protokol dapat menjelaskan bagaimana sebuah algoritma kriptografi semestinya digunakan.Beberapa protokol menjelaskan hal yang mendetail seperti struktur data yang harus digunakan. Protokol kriptografi digunakan dalam pengamanan transfer data pada tingkat aplikasi. Misalkan untuk berbagi komponen rahasia untuk menghitung sebuah nilai, membangkitkan rangkaian bilangan acak, atau untuk memastikan identitas seseorang (otentikasi). Protokol kriptografi biasanya mencakup aspek-aspek berikut :

- *Key-agreement protocol*
- *Entity authentication*
- *Symmetris encryption*
- *Secured application-level data transport*
- *Non-repudiation methods*

Walaupun sebagian besar protokol kriptografi dirancang untuk digunakan oleh kelompok dengan 2 orang pemakai, namun sudah dikembangkan protokol yang dapat dipakai oleh kelompok yang memiliki lebih dari dua orang pemakai. Sebuah protokol juga seharusnya dapat menahan berbagai jenis serangan dari luar walaupun sebuah protokol tidak akan bisa tahan terhadap semua jenis serangan. Sebelum kita mengetahui lebih lanjut tentang protokol kriptografi ada baiknya kita mengenal terlebih dahulu serangan seperti apa yang harus dapat ditahan sebuah protokol.

Secara umum, ada dua tipe serangan :

1. serangan pasif dimana penyerang mencoba untuk mencegah sebuah protokol untuk mencapai tujuannya dengan melakukan observasi terhadap entitas yang terlibat dalam protokol tersebut
2. serangan aktif dimana penyerang mengganggu komunikasi dengan cara apapun seperti mengganti pesan komunikasi, mengambil pesan komunikasi, menambah pesn baru, dan lainnya.

A. Key-Agreement Protocol

Key-Agreement Protocol merupakan protokol yang mengatur mengenai kesepakatan kunci yang akan dipilih oleh beberapa pihak yang berkomunikasi bersama sedemikian sehingga semua pihak yang berkomunikasi mempengaruhi hasil keluaran dari kunci tersebut. Protokol ini diharapkan dapat mencegah pihak lain atau pihak yang tidak berkomunikasi dan tidak berkepentingan

untuk dapat mempengaruhi kunci yang dipilih oleh pihak-pihak yang berkomunikasi. Protokol ini juga mencegah adanya pihak yang dapat mencuri dengar kunci yang dipilih tersebut.

Berikut ini beberapa atribut dari *key-agreement protocol* :

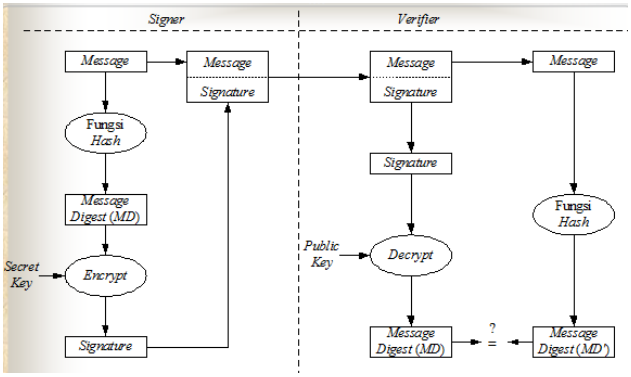
1. *known session key*. Protokol dapat mencapai tujuan walaupun penyerang mengetahui session key sebelumnya karena *session key* selalu berubah.
2. *(perfect) forward secrecy*. Jika rahasia jangka panjang dari satu atau lebih entitas terancam kerahasiaannya, kerahasiaan dari session key sebelumnya tidak akan terganggu.
3. *unknown key-share*. Sebuah entitas tidak akan dapat berbagi kunci dengan entitas lain tanpa kepercayaan dari ia sendiri.
4. *key-compromise impersonation.* Misalkan angka rahasia dari entitas *i* terbuka dan penyerang yang kemudian mengetahui nilai ini dapat berpura-pura sebagai *i*. Namun jika ini terjadi penyerang tidak akan bisa berpura-pura sebagai pihak lain kepada entitas *i*.
5. *loss of information.* Kebocoran informasi lain yang biasanya tidak dikethui oleh penyerang tidak akan mempengaruhi kemanan protokol.
6. *message independence.* Aliran individual dari protokol yang berjalan antara dua entitas berbeda yang tidak berhubungan.

B. Diffie-Hellman Exponential Key Exchange

Public-key agreement protocol pertama yang diperkenalkan kepada publik yang memenuhi kriteria dan karakteristik *Key-Agreement Protocol* adalah *Diffie-Hellman exponential key exchange*. Pada protokol ini, pihak-pihak yang berkomunikasi akan bersama-sama meng-exponentiate sebuah generator kunci dengan sebuah bilangan acak sehingga para pencuri dengar tidak bisa menebak kunci yang dihasilkan.

Dikarenakan pertukaran kunci yang tidak diketahui disebabkan oleh penggunaan masukan sebuah bilangan acak, *Diffie-Hellman Exponential Key Exchange* tidak melakukan otentikasi dari para pihak yang berkomunikasi sehingga protokol ini menjadi rentan terhadap serangan bertipe Man-in-the-Middle. Masalah ini coba diselesaikan dengan menggunakan berbagai macam skema dan protokol lain yang menyediakan kunci terotentikasi sehingga tidak rentan lagi terhadap serangan *Man-in-the-middle*. Akhirnya diperoleh cara untuk menanggulangi masalah ini diantaranya penggunaan pasangan kunci *Public/Private*, kunci rahasia yang diketahui bersama, dan menggunakan sandi lewat.

Penggunaan pasangan kunci *public* atau *private* dalam menanggulangi masalah serangan *Man-in-the-middle* adalah dengan menggunakan kunci yang ditandatangani secara digital sehingga integritas kunci dapat dipastikan. Jika pihak pertama akan mengirim pesan kepada pihak kedua, maka pesan harus disertai dengan tandatangan digital yang dihasilkan dengan menggunakan kunci *private* yang kemudian akan dicoba diverifikasi oleh pihak kedua menggunakan kunci *public*.



Gambar 1. Contoh skema penggunaan pasangan kunci *public* dan *private*

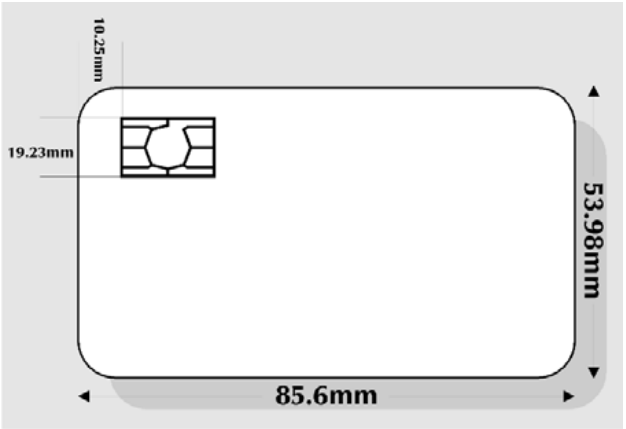
Sistem yang menggunakan kunci rahasia yang diketahui bersama dilakukan dengan memanfaatkan kriptografi kunci publik yang kemudian digunakan pada sistem kriptografi kunci simetris.

Password-authenticated key agreement protocol membutuhkan variabel baru yang terpisah dari kunci yang dihasilkan dan memunyai kemungkinan berukuran lebih kecil dari kunci itu sendiri yang keduanya bersifat *private* dan mempunyai integritas.

C. Smart Card

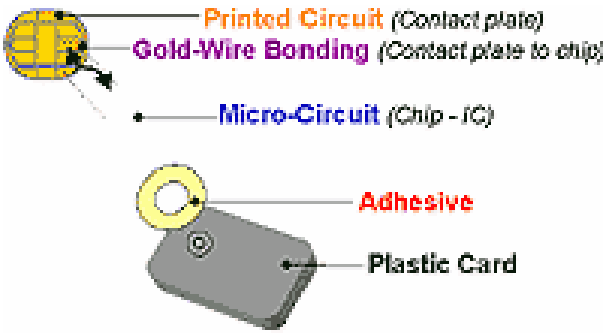
Smart Card merupakan kartu berbahan plastik atau biasanya menggunakan *polyvinyl chloride* yang didalamnya ditanamkan sebuah mikroprosessor dan mempunyai media penyimpanan untuk menyimpan program yang disediakan oleh pembuat kartu tersebut.

Spesifikasi dari *smart card* telah ditentukan oleh standar internasional yaitu, kartu plastik ini harus memiliki dimensi 85,60mm x 53,98mm x 0,76mm, yang ukuran tersebut merupakan urutan panjang, lebar, dan tebal dari kartu tersebut. Selain itu kartu ini juga harus dapat menahan sejumlah tekanan udara tanpa mengalami kerusakan secara langsung.



Gambar 2. Dimensi *Smart Card*

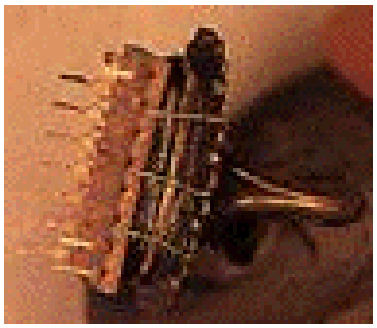
Sebuah *printed circuit* dan sebuah *integrated circuit chip* (*microcontroller*) ditanamkan pada sebuah *Smart Card*. *Printed circuit* merupakan lempengan emas tipis yang menyediakan hubungan arus listrik dengan lingkungan luar dan juga melindungi *chip* dari tekanan yang bersifat mekanik dan melindungi dari listrik statis. Sedangkan *microcontroller* yang dibuat haruslah memiliki ukuran yang sangat kecil sehingga dapat menahan sejulah tekanan udara.



Gambar 3. *Chip* dalam *Smart Card*

Penggunaan *Smart Card* akan menyediakan keamanan yang lebih tinggi. Keunggulan dari *Smart Card* adalah dalam hal mobilitasnya dikarenakan ukuran dari *Smart Card* yang kecil serta keamanannya dimana adanya penggunakan *printed circuit* yang saat dimasukkan ke dalam *card reader*, lempengan ini akan menyediakan energi listrik untuk *microprocessor* yang terletak di dalam *smart card*, yang pada akhirnya *smart card* dapat menyimpan dan memproses informasi dengan menggunakan kunci kriptografi dan algoritma yang menyediakan tanda tangan digital untuk digunkan dengan enkripsi yang lain.

Smart Card pertama kali diinisiasikan idenya pada tahun 1974 oleh seorang jurnalis berkebangsaan Perancis, Ronal Moreno. Beliau menemukan sistem pembayaran dengan menggunakan sebuah aplikasi elektronik yang ditanamkan pada sebuah benda berbentuk lingkaran.



Gambar 4. Bentuk Awal *Smart Card*

Ide ini kemudian dikembangkan pada Maret 1998 menjadi sebuah media bernama Java Ring.

Gambar 5. Java Ring

Dan pada tahun 1975, *Smart Card* pertama dihasilkan berupa kartu kredit dengan menggunakan *chip* dan *printed circuit* yang dibuat oleh perusahaan Perancis, CII-Honeywll-Bull.

Gambar 6. *Smart Card* produksi CII-Honeywell-Bull

Dan mengenai protokol yang digunakan *Smart Card* yang akan dibahas dalam makalah ini adalah protokol *three-pass password authenticated key agreement protocol* (TP-AMP) yang menerapkan model protokol Diffie-Hellman dan merupakan protokol kriptografi dengan jenis *Authenticated Key-Agreement Protocol* (AK).

II. PEMBAHASAN

Karena seperti dijelaskan di atas bahwa TP-AMP merupakan protokol yang menerapkan model Diffie-Hellman dan berjeniskan *Authenticated Key-Agreement Protocol* (AK), maka sebaiknya dipaparkan dulu mengenai Diffie-Hellman secara lebih lanjut dan mengenai AK itu sendiri.

A. Algoritma Diffie-Hellman

Misalkan dua orang berkomunikasi anggaplah Alice dan Bob. Di bawah ini adalah langkah-langkah algoritma Diffie-Hellman.

1. Alice membangkitkan bilangan bulat acak yang besar, misalkan x , dan kemudian mengirim hasil

perhitungan berikut kepada Bob :

$X = g^x \bmod n$

2. Bob membangkitkan bilangan bulat acak pula dan besar pula, misalkan *y*, dan kemudian mengirimkan hasil perhitungan berikut di bawah ini kepada Alice :

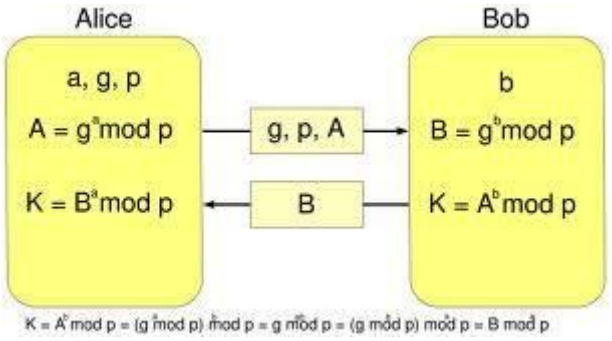
   $Y = g^y \bmod n$

3. Setelah Alice menerima kiriman dari Bob, ia melakukan perhitungan berikut :

   $K = Y^x \bmod n$

4. Setelah Bob menerima kiriman dari Alice, ia melakukan perhitungan berikut :

   $K' = X^y \bmod n$



Gambar 7. Skema algoritma Diffie-Hellman

Jika perhitungan Alice dan Bob dilakukan dengan benar, maka nilai *K* akan sama dengan *K'*, yaitu sama dengan $g^{xy} \bmod n$. Seorang penyadap atau pencuri dengar tidak akan dapat menghitung kunci *K* karena ia hanya memiliki informasi nilai *n*, *g*, *X*, dan *Y*. Sedangkan untuk mengetahui nilai kunci *K* dibutuhkan nilai *x* dan *y*. Karena nilai *x* dan *y* merupakan bilang acak dan besar, maka akan sulit bagi penyadap untuk mengetahui nilai *x* dan *y*.

Contoh berikut akan lebih menjelaskan mengenai algoitma Diffie-Hellman.

Pertama-tama Alice dan Bob menyepakati beberapa nilai sebagai berikut :

$n = 71$ dan $g = 7$ ($g < n$)

Berikut langkah-langkah algoritma Diffie-Hellman urut seperti langkah yang dijelaskan di atas.

1. Alice memilih bilangan bulat $x = 42$ dan menghitung :

   $X = g^x \bmod n = 7^{42} \bmod 71 = 57$

   Alice kemudian mengirimkan hasil perhitungan *X* kepada Bob.

2. Bob memilih bilangan bulat y = 38 dan menghitung :

   $Y = g^y \bmod n = 7^{28} \bmod 71 = 12$

   Bob kemudian mengirimkan hasil perhitungan *Y* kepada Alice.

3. Alice kemudian melakukan perhitungan kunci simetri *K*,

   $K = Y^x \bmod n = 12^{42} \bmod 71 = 25$

4. Bob kemudian melakukan perhitungan kunci simetri *K*,

   $K = X^y \bmod n = 57^{38} \bmod 71 = 25$

Jadi sekarang Alice dan Bob, sudah mempunyai kunci sesi yang sama, yaitu $K = 25$.

B. Authenticated Key-Agreement Protocol (AK)

Pengertian dari kata otentikasi pada protokol yang bersifat *authenticated* adalah adanya proses seperti proses *handshaking* yang biasa dikenal pada konteks jaringan. Berikut adalah skema dari protokol tersebut:

Misalkan dua entitas yang berkomunikasi adalah Alice dan Bob

1. Alice dan Bob mendapatkan salinan otentik dari kunci publik statik dari yang lain, Y_a dan Y_b (a:Alice dan b:Bob). Jika Alice dan Bob tidak mendapatkan salinan yang otentik, maka harus disertai dengan penanda bahwa itu asli.
2. Alice membangkitkan sebuah bilangan bulat positif secara acak r_a antara 1 hingga *n*-1, dan kemudian menghitung nilai $M_a = r_a Y_b$ yang kemudian dikirimkan pada Bob. Seperti dijelaskan pada penjelasan algoritma Diffie-Hellman, *n* ditentukan di awal komunikasi.
3. Bob menerima M_a dari Alice yang kemudian membangkitkan bilangan bulat positif acak r_b antara 1 hingga *n*-1 kemudian menghitung *session key* $K = h\left(\frac{r_b}{x_b} M_a + x_b Y_a\right) = h(r_a r_b + x_a x_b)g$.

   Jika hasil perhitungan $K = 0$, maka Bob akan memutuskan komunikasi. Jika tidak, maka Bob menghitung $M_b = r_b Y_a$ dan kemudian mengirimkannya ke Alice.
4. Alice menerima M_b dari Bob kemudian melakukan penghitungan *session key* $K = h\left(\frac{r_a}{x_a} M_b + x_a Y_b\right) = h(r_a r_b + x_a x_b)g$. Jika hasil $K = 0$. maka Alice akan menghentikan komunikasi dan session key kembali ke nilai terakhir $K = h(r_a r_b + x_a x_b)g$

Perkalian dengan variabel *h* ditujukan untuk mencegah dari serangan *small subgroup*. Sedangkan pengecekan nilai $K = 0$ digunakan untuk memastikan bahwa nilai *K* berhingga. Skema diatas terbukti memenuhi kriteria atribut *key-agreement protocol* yang penting dalam keamanan.

Dalam hal *known session key*, protokol dengan skema tadi akan membentuk terus-menerus *session-key* unik tiap kali dua entitas berkomunikasi yang nilainya bergantung pada nilai bilangan acak yang dibangkitkan kedua entitas yang berkomunikasi. Karena penyerang tidak dapat mengetahui nilai bilangan acak ini, walaupun penyerang mengetahui *session key* sebelumnya, ia akan kesulitan lagi karena harus mengulang proses pencarian nilai *session key*.

Protokol ini juga memenuhi atribut *perfect forward secrecy*. Walaupun nilai kunci privat dari dua entitas yang berkomunikasi diketahui oleh penyerang, penyerang tetap tidak akan bisa mengetahui *session key* sebelumnya.

Protokol ini memenuhi juga atribut *key-compromise*

impersonation. Misalkan penyerang mengetahui nilai kunci privat dari Bob sehingga ia dapat menyamar menjadi Bob kepada Alice. Namun ia tidak akan bisa menyamar sebagai Alice kepada Bob karena ia tidak bisa mengetahui kunci privat dari Alice.

Protokol ini juga mencegah *unknown key-share*. Misalkan Alice memiliki kunci privat yang berkoresponden dengan kunci publiknya, penyerang tidak akan dapat mengirim pesan kepada Bob dan menipu Bob bahwa pesan dari Alice bersumber dari penyerang itu sendiri hanya dengan menggunakan kunci publik dari Alice. Dengan begini, Bob tidak akan berbagi kunci dengan Alice tanpa pengetahuan Bob.

C. TP-AMP

Three-pass Password Authenticated Key-Agreement Protocol digunakan khususnya dalam lingkungan atau model jaringan client/server dimana dalam hal *Smart Card*, kartu bertindak sebagai client sedangkan *receiver* atau pembacanya bertindak sebagai server.

Gambar 8. *Smart Card* berkomunikasi dengan *Reader*

client gets (C, π)		server on S
$\gamma = H_0(C\|\pi)$, $\gamma' = \gamma^{-1} \bmod p$		$\gamma = H_0(C\|\pi)$, $\gamma' = \gamma^{-1} \bmod p$ $\nu = g^u \bmod p$ with $u = h_1(C\|\pi)$
choose x in $\mathbb{Z}_q^*$ randomly $m = g^x\gamma \bmod p$		
	$\xrightarrow{C, m}$	
		abort if there is no account for C choose y in $\mathbb{Z}_q^*$ randomly $\mu = \nu^y \bmod p$ $\beta = (m\gamma' g^m)^y \bmod p$ $k_1 = h_2(C\|S\|m\|\mu\|\beta\|\gamma')$
	$\xleftarrow{\mu, k_1}$	
$w = u^{-1}(x + m) \bmod q$ $\alpha = \mu^w \bmod p$ $k_1' = h_2(C\|S\|m\|\mu\|\alpha\|\gamma')$ abort if $k_1 \neq k_1'$ $k_2 = h_3(C\|S\|m\|\mu\|\alpha\|\gamma')$		
	$\xrightarrow{k_2}$	
		$k_2' = h_3(C\|S\|m\|\mu\|\beta\|\gamma')$ abort if $k_2 \neq k_2'$
$sk_C = h_4(C\|S\|m\|\mu\|\alpha\|\gamma')$		$sk_S = h_4(C\|S\|m\|\mu\|\beta\|\gamma')$

Gambar 9. Skema Protokol TP-AMP

Pertama-tama, baik client dan server harus menyepakati terlebih dahulu parameter-parameter dasar dari Diffie-Hellman *key-agreement protocol*. Pada tahap pendaftaran, client memilih sebuah nama dan sebuah sandi lewat yang kemudian disimpan pada server. Kemudian protokol pada server dan client menurunkan beberapa nilai menggunakan parameter-parameter γ, γ', *u*, dan *v*. Bila skema pada gambar 8 dapat dieksekusi dengan baik, maka kedua pihak, baik client maupun server akan mempunyai *session key*.

Terlihat bahwa α dan β dalam gambar 8 berkoresponden dengan rahasia bersama yang dikomputasi pada kedua sisi. Untuk proses kriptografi dengan *one-way hash function h*, protokol baru dianggap berhasil jika nilai α = nilai β.

III. KESIMPULAN

Protokol kriptografi sangat berperan dalam menjaga keamanan dalam komunikasi dalam jaringan karenannya penggunaannya adalah hal yang penting jika ingin mencapai komunikasi yang ideal apalagi jika menginginkan kerahasiaan. Protokol kriptografi memenuhi beberapa aspek diantaranya *Key-agreement*, *Entity Authentication*, *Symmetric Encryption*, *Secured application-level data transport*, dan *Non-repudation methods*. *Key-agreement* merupakan protokol dimana dua atau lebih pihak dapat menyetujui penggunaan sebuah kunci. Dengan begini dapat mencegah adanya pihak ketiga yang diluar pihak yang terlibat dalam mempengaruhi kunci yang disepakati.

Protokol *key-agreement* pertama yang digunakan dan dipublikasikan secara luas adalah protokol yang dibuat oleh Diffie-Hellman. Skema Diffie-Hellman cukup tahan terhadap serangan dari luar karena menggunakan angka bulat besar yang dibangkitkan secara acak. *Key-agreement protocol* memiliki beberapa kriteria harapan seperti *known session key*, *(perfect) forward secrecy*, *unknown key-share*, *key-compromise impersonation*, *loss*

of information, dan *message independence* yang harapannya dipenuhi oleh *key-agreement protocol* yang baik.

Protokol *key-agreement* yang digunakan pada *Smart Card* merupakan *Authenticated Key-Agreement Protocol* (AK) yang menggunakan otentikasi seperti proses *handshaking* pada komunikasi jaringan. AK ini juga sudah memenuhi kriteria harapan dari *key-agreement protocol* yang baik. Protokol nyatanya adalah *Three-pass Password Authenticated Key-Agreement Protocol* (TP-AMP) memiliki dasar sama dengan AK hanya saja lebih dapat diterapkan langsung pada pada teknologi *Smart Card* karena sudah langsung menggunakan model jarigngan client/server dimana dalam hal *Smart Card*, kartu bertindak sebagai client sedangkan *receiver* atau *reader* bertindak sebagai server.

Protokol yang diimplementasikan pada *Smart Card* sudah memenuhi kriteria harapan sari protokol yang baik namun masih memiliki kelemahan. Protokolnya dinamakan TP-AMP atau *Three-pass Password Authenticated Key-Agreement Protocol* yang menggunakan sandi lewat untuk otentikasi client pada server. Proses selanjutnya menggunakan proses yang sama dengan AK seperti yang sudah dijelaskan pada bahasan sebelumnya, yaitu komunikasi yang menggunakan *session key* untuk memastikan bahwa entitas dengan siapa ia berkomunikasi merupakan entitas yang benar dan pembangkitan bilangan acak.

REFERENSI

[1] Buku Mata Kuliah IF3058 - Kriptografi
Rinaldi Munir, "Kriptografi", Program Studi Informatika Institut Teknologi Bandung, 2010.

[2] Halaman web
http://en.wikipedia.org/wiki/Cryptographic_protocol
Tanggal Akses : 29 April 2010 Pukul 03.48

[3] Halaman web
http://en.wikipedia.org/wiki/Key_agreement
Tanggal Akses : 29 April 2010 Pukul 03.48

[4] Makalah Ilmiah
www.magdysaeb.net/images/Sultan_paper.pdf
Tanggal Akses : 29 April 2010 Pukul 03.49

[5] Makalah Ilmiah
http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah2/Makalah-034.pdf
Tanggal Akses : 14 Mei 2010 Pukul 08.13

[6] Kuliah Kriptografi
http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Algoritma%20Diffie-Hellman.ppt
Tanggal Akses : 15 Mei 2010 Pukul 08.27

[7] Kuliah Kriptografi
http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Protokol%Kriptografi.ppt
Tanggal Akses : 15 Mei 2010 Pukul 08.27

[8] Makalah Ilmiah
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.27.8493&rep=rep1&type=pdf
Tanggal Akses : 28 April 2010 Pukul 21.59

[9] Makalah Ilmiah
http://events.iaik.tugraz.at/RFIDSec08/Papers/Publication/14%20-%20Ullmann%20-%20PW%20Authenticated%20Key%20Agreement%20-%20Paper.pdf
Tanggal Akses : 29 April 2010 Pukul 03.49

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, 17 Mei 2010

Rizky Delfianto NIM : 13507032