Perancangan dan Implementasi Aplikasi Bluetooth Payment untuk Telepon Seluler Menggunakan Protokol Station-to-Station

Emir M. Husni
Sekolah Teknik Elektro & Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung 40132
Tel.: 022-2500960, Faks.: 022-2534217
ehusni@lskk.ee.itb.ac.id

Abstrak

Pada penelitian ini dilakukan perancangan dan implementasi aplikasi bluetooth payment untuk telepon seluler dengan menggunakan protokol Station-to-Station yang merupakan pengembangan dari algoritma Diffie-Hellman. Aplikasi ini diimplementasikan menggunakan bahasa Java Micro Edition, khususnya J2ME, dan bahasa C. Sedangkan program server dan client diimplementasikan menggunakan NetBeans IDE versi 6 dan Java Wireless Toolkit pada sistem operasi Windows XP Professional. Pengujian menunjukkan bahwa implementasi aplikasi ini bekerja dengan baik sesuai dengan rancangan yang dibuat.
Kata Kunci: *Diffie-Hellman, protokol Station-to-Station, Bluetooth payment*

1. Pendahuluan

Kriptografi, atau ilmu penyandian data, adalah suatu kombinasi bidang ilmu yang bertujuan untuk menjaga kerahasiaan suatu pesan dari akses oleh orang-orang yang tidak berhak. Bidang ilmu ini semula hanya populer dalam bidang militer, untuk menyandikan pesan-pesan panglima perang kepada garis depan pasukannya. Namun seiring dengan semakin berkembangnya teknologi dan semakin padatnya lalu lintas informasi yang terjadi, yang tentu saja semakin menuntut adanya suatu komunikasi data yang aman, bidang ilmu ini menjadi semakin penting. Kini bidang ini menjadi salah satu topik riset yang tidak habis-habisnya dengan melibatkan semakin banyak peneliti. Ibu keilmuan dari kriptografi sebenarnya adalah matematika, khususnya teori aljabar.

Pada tahun 1976, Diffie-Hellman [1] memperkenalkan algoritma pertukaran kunci rahasia yang kemudian menjadi inspirasi revolusi algoritma kunci publik dalam ilmu kriptografi. Algoritma Diffie-Hellman ini memungkinkan dua orang atau lebih menentukan satu kunci bersama secara rahasia. Tingkat kerahasiaan tersebut bisa dicapai karena kunci rahasia tidak dipertukarkan melalui kanal komunikasi tetapi dihitung dari kunci publik dan kunci pribadi. Penemuan ini telah mengubah perjalanan kriptografi. Riset tentang sistem keamanan tidak lagi terfokus pada desain protokol dan verifikasi tetapi secara intensif juga merambah ke bidang teori bilangan dan aljabar.

Penelitian yang dilakukan adalah perancangan dan implementasi aplikasi Bluetooth Payment untuk telepon seluler yang menggunakan protokol Station-to-Station. Dimana protokol Station-to-Station adalah pertukaran kunci dengan metode Diffie-Hellman yang harus menyediakan proses autentifikasi sehingga kedua pihak yang akan berkomunikasi yakin bahwa mereka bertukar kunci dengan pihak yang diinginkan. Algoritma yang digunakan dalam protokol Station-to-Station merupakan algoritma yang telah disetujui oleh NIST (*National Institute of Standards and Technologies*).

Implementasi perancangan algoritma dalam penelitian ini menggunakan bahasa Java Micro Edition. Selanjutnya dilakukan simulasi dengan simulator NetBeans IDE versi 6.

2. Dasar teori

2.1 Skema Enkripsi

2.1.1 Skema Enkripsi Kunci Simetrik

Dalam sistem kriptografi skema enkripsi kunci simetrik, kunci yang digunakan untuk proses enkripsi dan dekripsi adalah sama atau simetrik. Karena kuncinya sama, kedua pengguna yang berkeinginan untuk berkomunikasi dengan rahasia harus setuju terhadap kunci yang digunakan dan keduanya bersama-sama menjaga kunci rahasia yang digunakan. Setiap pengguna yang terlibat harus saling menaruh kepercayaan untuk tidak membocorkan kunci yang telah disepakati.

2.1.2 Skema Enkripsi Kunci Publik

Sistem kriptografi kunci publik mempunyai dua penggunaan utama, yaitu untuk enkripsi dan *digital signature*. Dalam sistem ini, digunakan sepasang kunci, satu kunci sebagai kunci publik (*public key*) dan yang lainnya sebagai kunci pribadi (*private key*). Kunci publik dipublikasikan untuk umum sedangkan kunci pribadi dijaga kerahasiaannya oleh penerima pesan.

2.1.3 Skema Enkripsi Gabungan

Kedua skema enkripsi diatas, masing-masing mempunyai kelebihan dan kelemahan. Skema enkripsi kunci publik mungkin lebih unggul dibandingkan dengan skema kunci simetrik karena tingkat keamanannya yang cukup tinggi dan pengaturan kunci yang lebih baik. Meskipun demikian, sistem kriptografi kunci simetrik masih secara luas digunakan karena kecepatannya dalam memproses data lebih unggul dibandingkan dengan sistem kriptografi kunci publik. Dengan melihat kelebihan masing-masing, keduanya dapat digabung untuk membentuk sistem kriptografi yang lebih aman dan lebih cepat.

2.2 Digital Signature

Digital signature berfungsi sebagai tanda tangan pada komunikasi digital [1]. Untuk menandatangani sebuah pesan, **A** melakukan sebuah perhitungan meliputi kunci pribadi dan pesannya sendiri. Output dari perhitungan inilah yang disebut *digital signature* yang dilampirkan dengan pesan. Untuk memeriksa *signature*, **B** melakukan perhitungan yang meliputi pesan, *signature* yang dimaksudkan, dan kunci publik **A**.

Protokol yang digunakan untuk membuktikan kebenaran bahwa pesan dan signature yang diterima **B** benar-benar dikirim oleh **A** :

1. **A** mengambil pesan dan menghitung atau membuat *signature* (**S**) dengan pesan **M** dan kunci pribadinya (**d**), sehingga didapat $\mathbf{D_d\ (M) = S}$.
2. **B** mendapatkan **M** dan **S**, dan kunci publik **A** (**e**).
3. **B** menghitung $\mathbf{E_e\ (S) = M'}$. Jika **M' = M**, maka signature valid atau benar-benar milik **A**. Jika **M** atau **S** dimodifikasi maka *signature* tidak akan valid.

2.3 Protokol penentuan kunci Diffie-Hellman

Pertukaran kunci dengan metode Diffie-Hellman (*Diffie-Hellman Key Exchange*) merupakan suatu aplikasi dari skema enkripsi gabungan yang mengijinkan dua pengguna melakukan pertukaran kunci secara rahasia melalui saluran komunikasi yang tidak aman [2]. Dua pengguna yang akan berkomunikasi melakukan pertukaran kunci menggunakan sistem kriptografi kunci publik. Setelah keduanya sepakat dan memperoleh kunci yang sama, kemudian digunakan sistem kriptografi kunci simetrik untuk tahap komunikasi selanjutnya.

Tingkat keamanan pertukaran kunci ini tergantung pada tingkat kesulitan masalah logaritma diskret yang didefinisikan sebagai berikut :

- Untuk bilangan acak *b* dan sebuah akar primitif *a* dari bilangan prima *p*, kita dapat menemukan eksponen unik *i* sedemikian sehingga

$$\mathbf{b = a^i \bmod p \quad dimana\ 0 \le i \le (p-1)}$$

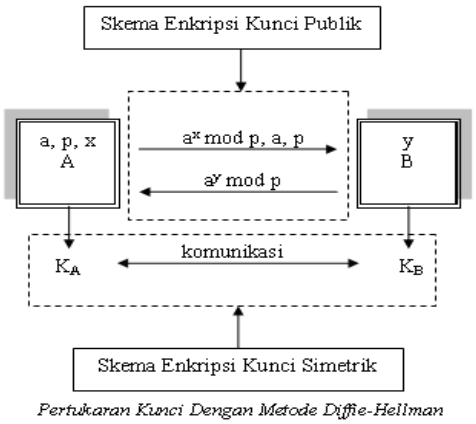
- Pangkat **i** disebut sebagai logaritma diskret, dan tingkat kesulitan menemukan **i** dari bilangan (a, b, p) disebut **persoalan Logaritma Diskret**.

Akar primitif (*primitive root*) dari sebuah bilangan prima p adalah bilangan a, $1 \le a \le p-1$, yang pangkatnya membangkitkan semua integer dari 1 sampai p-1. Jika a akar primitif dari sebuah bilangan prima p, maka bilangan-bilangan (a mod p), (a^2 mod p),…, (a^{p-1} mod p) adalah berbeda dan terdiri dari bilangan mulai dari 1 sampai p-1.

Bentuk dasar pertukaran kunci dengan metode Diffie-Hellman sebagai berikut :

- Pihak A dan B akan berkomunikasi.
- A memilih suatu bilangan prima p dan a sebagai akar primitif dari p, kemudian mengirimkan nilai a dan p ke B.
- Nilai a dan p boleh diketahui oleh umum.
- Secara rahasia, A memilih bilangan acak x dan B memilih bilangan acak y, $1 \le x, y \le (p-2)$
- A mengirim $\mathbf{(a^x \bmod p)}$ ke B, dan B mengirim $\mathbf{(a^y \bmod p)}$ ke A
- A menghitung $\mathbf{K_A = (a^y \bmod p)^x = (a^{xy} \bmod p)}$ dan B menghitung $\mathbf{K_B = (a^x \bmod p)^y = (a^{xy} \bmod p)}$.

Hasil pertukaran kunci diatas adalah pihak A dan B memperoleh kunci K_A dan K_B yang sama, yang dapat digunakan untuk berkomunikasi dengan sistem kriptografi kunci simetrik.



Pertukaran Kunci Dengan Metode Diffie-Hellman

Gambar 1. Pertukaran Kunci Diffie-Helman.

2.4 Protokol Station-to-Station

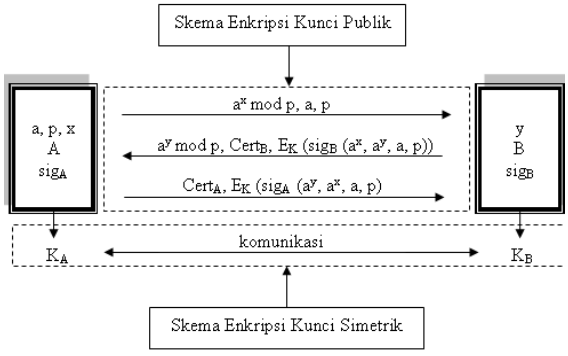
Untuk menghindari serangan aktif *man-in-the-middle attack*, pertukaran kunci dengan metode Diffie-Hellman harus menyediakan proses autentifikasi sehingga kedua pihak yang akan berkomunikasi yakin bahwa mereka bertukar kunci dengan pihak yang diinginkan. Salah satu cara pertukaran kunci yang menyediakan proses autentifikasi adalah protokol Station-to-Station berdasarkan penelitian yang dilakukan oleh Diffie, van Oorschot dan Wiener [2].

Proses autentifikasi pada protokol Station-to-Station dilakukan dengan melibatkan tanda tangan digital (*digital signature*) kedua pihak yang akan melakukan komunikasi.

Bentuk dasar protokol Station-to-Station sebagai berikut :

- Pihak A dan B akan melakukan komunikasi.
- A dan B memilih suatu bilangan prima p dan a sebagai akar primitif dari p, kemudian mengirimkan nilai a dan p ke B.
- Nilai a dan p boleh diketahui oleh umum.
- Secara rahasia, A memilih bilangan acak x dan B memilih bilangan acak y, $1 \leq x,y \leq (p-2)$
- A mengirim $(a^x \bmod p)$ ke B.
- B menghitung $K_B = (a^x \bmod p)^y$.
- B menyusun $(a^y \bmod p, a^x \bmod p, a, p)$ secara berurutan, melakukan tanda tangan digital sig_B, dan mengenkripsi dengan skema enkripsi kunci simetrik dengan kunci K_B, kemudian mengirim ke A bersama $(a^y \bmod p)$.
- A menghitung $K_A = (a^y \bmod p)^x$. $(K = K_A = K_B)$
- A mendekripsi pesan dari B, dan memverifikasi tanda tangan digital dari B.
- A menyusun $(a^x \bmod p, a^y \bmod p, a, p)$ secara berurutan, melakukan tanda tangan digital sig_A , dan mengenkripsi dengan skema enkripsi kunci simetrik dengan kunci K, kemudian mengirim ke B.
- B mendekripsi pesan dari A, dan memverifikasi tanda tangan digital dari A.

Hasil pertukaran kunci diatas adalah pihak A dan B memperoleh kunci K_A dan K_B yang sama, yang dapat digunakan untuk berkomunikasi dengan sistem kriptografi kunci simetrik. Di samping itu, pihak A dan B dapat melakukan proses autentifikasi sehingga yakin mereka bertukar kunci dab berkomunikasi dengan pihak yang diinginkan.



sig_A : tanda tangan digital A
E_K : skema enkripsi kunci simetrik dengan kunci K

Bentuk lengkap protokol Station-to-Station

Gambar 2. Protokol Station-to-Station.

3. Perancangan dan Implementasi

3.1 Penentuan Spesifikasi

Dasar penentuan spesifikasi yang akan digunakan adalah pemilihan algoritma yang akan diimplementasikan telah dikenal dengan baik dan banyak digunakan sehingga telah diketahui kelebihan maupun kekurangannya. Pada penelitian ini, penulis menggunakan standar yang dikeluarkan oleh NIST. Standar tersebut adalah FIPS (*Federal Information Processing Standards*) dengan nomer publikasi SP 800-57 [8] pada Tabel I berikut ini:

Tabel 1. Standar NIST [8].

Algorithm security lifetime	Symmetric key algorithm	FFC (e.g. DSA, D-H)	Digital signatures and hash-only applications
Through 2010 (min. of 80 bits of strength)	2TDEA 3TDEA AES-128 AES-192 AES-256	Min. : L = 1024 N = 160	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min. : L = 2048 N = 224	SHA-224, SHA-256, SHA-384, SHA-512
Through 2060 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min. : L = 3072 N = 256	SHA-256, SHA-384, SHA-512

Perkiraan lifetime beberapa algoritma kriptografi

FFC : Finite Field Cryptography
TDEA : Triple Data Encryption Algorithm
AES : Advanced Encryption Standard
DSA : Digital Signature Algorithm
SHA : Secure Hash Algorithm

Dari Tabel I, penulis menyusun algoritma yang digunakan untuk menyusun protokol Station-to-Station sebagai berikut :

- Besar bilangan prima yang digunakan 2048-bit.
- Algoritma tanda tangan digital : DSA (Digital Signature Algorithm) dengan fungsi hash SHA-256.
- Algoritma kriptografi simetrik : AES (Advanced Encryption Standard) 128-bit.

Algoritma yang dipilih diharapkan belum dipecahkan dan masih bisa dipakai hingga tahun 2030 dengan tingkat keamanan minimum sebesar 112-bit. Tingkat keamanan sebesar X-bit berarti jika T adalah waktu untuk melakukan satu operasi dari suatu algoritma diatas, maka penyerang akan membutuhkan waktu 2^{X-1} T untuk memecahkan algoritma tersebut.

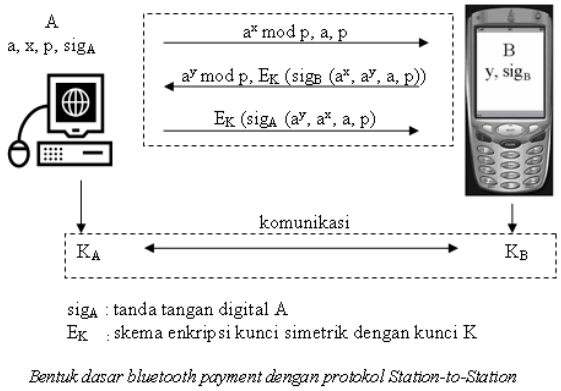
3.2 Perancangan Sistem

Perancangan sistem bluetooth payment dengan protokol Station-to-Station adalah sebagai berikut :

- Pihak A (server/komputer) dan B (client/*handphone*) akan melakukan komunikasi.
- Secara rahasia, A memilih bilangan acak x dan B memilih bilangan acak y, $1 \leq x,y \leq (p-2)$
- A dan B memilih suatu bilangan prima p, a sebagai akar primitif dari p
- A memilih $(a^x \bmod p)$, kemudian mengirimkannya ke B lewat bluetooth.
- B menghitung $K_B = (a^x \bmod p)^y$.
- B menyusun $(a^y \bmod p, a^x \bmod p, a, p)$ secara berurutan, melakukan tanda tangan digital sig_B, dan mengenkripsi dengan skema enkripsi kunci simetrik dengan kunci K_B, kemudian mengirim ke A bersama $(a^y \bmod p)$ lewat bluetooth.
- A menghitung $K_A = (a^y \bmod p)^x$. $(K = K_A = K_B)$

• A mendekripsi pesan dari B, dan memverifikasi tanda tangan digital dari B.
• Jika tanda tangan digital dari B valid, A menyusun (a^x *mod p,* a^y *mod p, a, p*) secara berurutan, melakukan tanda tangan digital sig_A , dan mengenkripsi dengan skema enkripsi kunci simetrik dengan kunci *K*, kemudian mengirim ke B lewat bluetooth.
• B mendekripsi pesan dari A, dan memverifikasi tanda tangan digital dari A.

Hasil pertukaran kunci diatas adalah pihak A dan B memperoleh kunci K_A dan K_B yang sama, yang dapat digunakan untuk berkomunikasi dengan sistem kriptografi kunci simetrik. Di samping itu, pihak A dan B dapat melakukan proses autentifikasi sehingga yakin mereka bertukar kunci dan berkomunikasi dengan pihak yang diinginkan. Untuk lebih jelasnya dapat dilihat pada gambar berikut:



Gambar 3. Bluetooth payment.

3.3 Desain Program

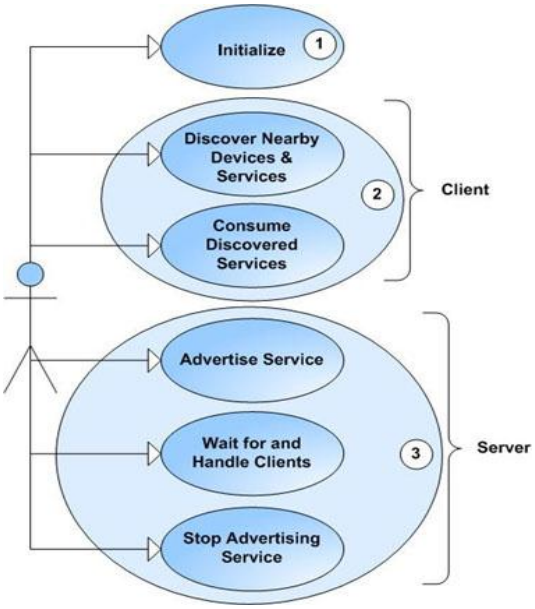
3.3.1 Perancangan Bluetooth Payment

Bluetooth Payment adalah aplikasi pembayaran secara elektronik yang menggunakan bluetooth sebagai media transmisinya. Aplikasi ini bisa berjalan pada mobile phone yang memiliki fitur bluetooth dan Java API untuk bluetooth. Aplikasi ini memungkinkan dua perangkat bluetooth untuk terhubung dan kemudian bertukar paket data antar perangkat tersebut. Salah satu perangkat menjadi server dan perangkat lainnya yang terkoneksi dengan server menjadi client.

Untuk implementasi ini, didesain model client / server. Arsitektur dan komponen utama client / server diperlihatkan oleh Gambar 4 dengan penjelasan sebagai berikut:
• Inisialisasi : semua perangkat yang akan berkomunikasi mulai mengaktifkan bluetooth.
• Client : suatu client menggunakan service yang ditawarkan, sebelumnya client mencari semua perangkat disekitarnya kemudian mencari service yang diinginkan.
• Server : suatu server menyediakan service untuk client, server mendaftarkan service pada SDDB (Service Discovery Database). Kemudian server menunggu koneksi dan melayani client. Jika service tidak diperlukan lagi, server menghilangkannya dari SDDB.

Dimana koneksi antara client dan server dilakukan melalui RFCOMM (komunikasi serial port pada bluetooth).

RFCOMM adalah bagian yang menangani komunikasi data mulai dari pembentukan koneksi, penerimaan data dan pengiriman data pada aplikasi bluetooth payment ini. RFCOMM menyediakan koneksi stream-based yang sesuai dengan komunikasi serial port.



Gambar 4. Arsitektur dan komponen utama client/server.

3.4 Implementasi

Tahap implementasi dimulai dengan membuat algoritma pembangkitan bilangan prima dan pembangkitan parameter tanda tangan digital dalam bahasa C. Untuk melakukan perhitungan dengan bilangan yang relatif besar, penulis menggunakan *library* untuk bilangan besar.

Sedangkan bagian-bagian algoritma kriptografi (tanda tangan digital, fungsi hash, dan kriptografi simetrik) dibuat secara tersendiri sesuai algoritma diatas dengan bahasa Java, khususnya J2ME. Setelah algoritma-algoritma tersebut memberikan hasil yang sesuai, maka algoritma kriptografi tersebut digabungkan untuk menyusun protokol Station-to-Station dan dibagi dalam dua bagian yaitu bagian A (server) dan B (client).

Pada server dan client ditambahkan program untuk berkomunikasi melalui bluetooth. Kemudian baik program server dan client diimplementasikan menggunakan NetBeans IDE versi 6 dan Java Wireless Toolkit pada sistem operasi Windows XP Professional.

Perangkat bluetooth yang digunakan adalah bluetooth USB dongle yang didukung software

BlueSoleil versi 3.2.2.8. Sedangkan perangkat handphone yang digunakan adalah SonyEricsson G502.

4. Pengujian dan Analisis

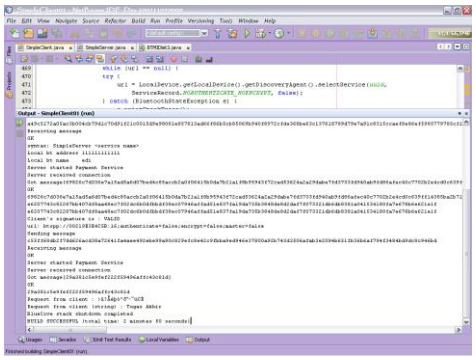
Bagian pertama dari aplikasi Bluetooth Payment menggunakan protokol Station-to-Station adalah server mengirimkan kunci publik berupa a^x mod p, a, dan p ke client.

Untuk bagian kedua, pihak client kemudian membuat kunci pribadi (a^{xy} mod p) dari kunci publik yang diterima dari server, dan membuat kunci enkripsi sebesar 128-bit yang digunakan untuk mengenkripsi tanda tangan digital dengan algoritma AES 128-bit. Kemudian mengirim kunci publik milik client (a^y mod p) bersama dengan tanda tangan digital yang telah dienkripsi ke server.

Pada bagian ketiga, pihak server menerima kunci publik dari client (a^y mod p) kemudian membuat kunci pribadi (a^{xy} mod p) dan kunci enkripsi dari kunci publik. Kunci enkripsi ini digunakan untuk mendekripsi tanda tangan digital pihak client yang diterima oleh server. Tanda tangan pihak client kemudian diverifikasi untuk memeriksa apakah tanda tangan tersebut milik client yang bersangkuan atau bukan. Proses verifikasi tanda tangan oleh server menunjukkan tanda tangan milik client adalah valid.

Bagian selanjutnya adalah server membuat tanda tangan digital, mengenkripsi dengan kunci enkripsi dan mengirimkannya ke client.

Jika proses verifikasi oleh client menunjukkan tanda tangan server adalah valid, maka client akan melanjutkan ke tahap selanjutnya yaitu mengirim pesan ke server, seperti pada Gambar 5.



Gambar 5. Pesan yang dikirim oleh client.

Dari hasil yang telah diperoleh diatas, dapat dilihat bahwa aplikasi tersebut dapat berjalan dengan baik.

Lamanya waktu yang diperlukan untuk seluruh proses, mulai dari bagian pertama, server mengirim kunci publik, hingga proses verifikasi oleh client adalah 2 sampai dengan 3 menit. Panjang waktu 2-3 menit untuk melakukan pembayaran masih merupakan waktu yang lama untuk pengguna menunggu sehingga sistem aplikasi bluetooth payment ini masih memerlukan perbaikan untuk mengurangi waktu transaksi.

5. Kesimpulan

Dari hasil analisis dan pengujian yang telah dilakukan, dapat diambil beberapa kesimpulan sebagai berikut :

1. Algoritma Diffie-Hellman memungkinkan setiap orang mendapatkan kunci rahasia bersama tanpa harus saling bertukar informasi pribadi.
2. Untuk dapat diterapkan dan memenuhi syarat keamanan informasi, algoritma Diffie-Hellman perlu diimplementasikan dalam bentuk protokol Station-to-Station.
3. Aplikasi Bluetooth Payment dengan protokol Station-to-Station telah berjalan dengan baik tetapi waktu yang digunakan untuk proses masih memerlukan 2-3 menit. Sehingga masih diperlukan perbaikan pemrograman untuk menyingkat waktu transaksi.

Pustaka

[1] W. Stallings, *Cryptography and Network Security Principles and Practices, Fourth Edition*, Prentice Hall, 2005.

[2] W. Diffie, P. Van Oorschot, dan Michael J. Wiener, *Authentication and Authenticated Key Exchanges*, Designs, Codes and Cryptography, 2, 107-125, 1992.

[3] Wade Trappe and Lawrence Washington, *Introduction To Cryptography and Coding Theory, Second Edition*, Pearson Prentice Hall, 2006.

[4] A. Menezes, P. van Oorschot, dan S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[5] FIPS 180-3, *Secure Hash Algorithm (SHA)*, *Federal Information Processing Standards Publication* 180, U. S. Dept. of Commerce / National Institute of Standards and Technology, 2007.

[6] FIPS 186-3, *Digital Signature Standard (DSS)*, *Federal Information Processing Standards Publication* 186, U. S. Dept. of Commerce / National Institute of Standards and Technology, 2006.

[7] FIPS 197, *Advanced Encryption Standard (AES)*, *Federal Information Processing Standards Publication* 197, U. S. Dept. of Commerce / National Institute of Standards and Technology, 2001.

[8] SP 800-57, *Recomendation for Key Management*, *Federal Information Processing Standards Publication*, U. S. Dept. of Commerce / National Institute of Standards and Technology, 2007.