UNIVERSITAS INDONESIA

ALGORITMA DIFFIE-HELLMAN DENGAN MENGGUNAKAN POLINOMIAL CHEBYSHEV

SKRIPSI

MERYSA AMANDA

0305010378

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

PROGRAM STUDI SARJANA MATEMATIKA

DEPOK

JULI 2011

UNIVERSITAS INDONESIA

ALGORITMA DIFFIE-HELLMAN DENGAN MENGGUNAKAN POLINOMIAL CHEBYSHEV

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana sains

MERYSA AMANDA
0305010378

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI SARJANA MATEMATIKA
DEPOK
JULI 2011

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama	: Merysa Amanda
NPM	: 0305010378
Tanda Tangan	: 
Tanggal	: 6 Juli 2011

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh

Nama	:	Merysa Amanda
NPM	:	0305010378
Program Studi	:	Sarjana Matematika
Judul Skripsi	:	Algoritma Diffie-Hellman dengan menggunakan polinomial Chebyshev

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Sains pada Program Studi S1 Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Indonesia

DEWAN PENGUJI

Pembimbing	: Dr. Sri Mardiyati, M.Kom	( )
Penguji	: Arie Wibowo, M.Si	( )
Penguji	: Helen Burhan, M.Si	( )
Penguji	: Dr. Hengki Tasman, M.Si	( )

Ditetapkan di	:	Depok
Tanggal	:	9 Juni 2011

KATA PENGANTAR

Alhamdulillah segala puji bagi Allah yang telah mengizinkan penulis untuk bisa merampungkan tugas akhir ini, sebagai salah satu syarat untuk memperoleh gelar Sarjana Sains di Fakultas Matematika dan Ilmu Pengetahuan Alam.

Proses penulisan skripsi ini tidak akan rampung tanpa bantuan, dukungan, serta doa dari orang-orang di sekitar penulis. Oleh karena itu penulis menghaturkan banyak terimakasih kepada

1. Orang tua penulis, Papa dan Mama yang telah merawat dan membesarkan penulis. Terimakasih banyak untuk semua yang telah Papa dan Mama berikan selama ini. Juga doa-doa yang Papa dan Mama panjatkan setiap harinya untuk penulis. Skripsi ini saya hadiahkan buat Mama dan Papa.
2. Adik penulis. Faris. Cepet nyusul dek.
3. Seluruh keluarga, Nenek, Tante, Om dan yang lainnya.
4. Ibu Sri Mardiyati M.Kom selaku pembimbing. Terimakasih atas kesabaran ibu dalam membimbing saya. Terimakasih pula atas saran dan arahan selama masa bimbingan.
5. Ibu Nurrohmah, Ibu Rustina, dan Bapak Suryadi MT, selaku pembimbing Akademik angkatan 2005. Terimakasih atas arahannya selama mengemban ilmu di jurusan ini.
6. Pak Yudi Satria selaku Ketua Jurusan Matematika selama penulis menjalani perkuliahan,
7. Mba Mila selaku Koordinator Kemahasiswaan Departemen, atas kemurahan hatinya sehingga saya bisa menyelesaikan kuliah di jurusan tercinta ini. Juga Ibu Dian Lestari selaku Koordinator Pendidikan Departemen.
8. Seluruh Dosen Matematika UI dan Dosen FMIPA UI
9. Seluruh karyawan Matematika UI. Mba Santi, Pak Saliman, Mas Salman, Mba Rusmi, Mas Anshori, Pak Turino, Mas Suratmin, juga Mas Tatang dan Mas Wawan.

10. Sahabat-sahabat. Fadel Karami, Andri, Mira, Ayu, Icha. Atas dukungan dan doanya.
11. Saudara-saudara. Tante Fina, Tante Mun, Nanta, Melon, Mila, Bang Nanda, Uni Rika, Uni Winda, Tante Leni.
12. Teman-teman seperjuangan dalam menyusun tugas akhir ini. Dhanardi Riansyah, Rendy Ahmad dan M. Try Sutrisno. Terimakasih untuk sharing-sharing dan motivasi dalam skripsi ini.
13. Teman-teman angkatan 2005 Fika, Wicha, Poetri, Inul, Dia, Yanu, Shinta, Akmal, Icha oneng, Riesa, Puji, Ratih, Nisma, Othe, Kumel, Khuri, Ranti, Aya, Gyo, Asep, Trian, Uun, Nasib.
14. Teman-teman 2006 Bara, Aliman, Yono, Dani, Oza, Cimz, Rita, Lee, Syafirah, dan Yuridunis.
15. Teman-teman angkatan 2004, 2005, 2007, 2008, 2009, dan angkatan 2010.
16. Serta orang-orang yang membantu penulisan tugas akhir ini yang namanya tidak bisa penulis sebutkan satu-satu.

Penulis menyadari bahwa masih terdapat banyak kekurangan dalam penulisan skripsi ini. Kritik dan saran sangat diharapkan untuk perbaikan diri penulis. Harapan penulis, semoga skripsi ini dapat bermanfaat bagi kita semua. Amin.

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

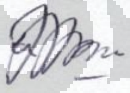
Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	: Merysa Amanda
NPM	: 0305010378
Program Studi	: Sarjana Matematika
Departemen	: Matematika
Fakultas	: Matematika dan Ilmu Pengetahuan Alam
Jenis karya	: Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :
Algoritma Diffie-Hellman dengan menggunakan polinomial Chebyshev beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 6 Juli 2011
Yang menyatakan



(Merysa Amanda)

ABSTRAK

Nama : Merysa Amanda

Program Studi : S1 Matematika

Judul : Algoritma Diffie-Hellman dengan menggunakan polinomial Chebyshev.

Algoritma Diffie-Hellman adalah algoritma yang menggunakan kunci publik dalam proses pembentukkan kunci rahasia. Pada tugas akhir ini akan dipelajari pembentukkan kunci rahasia dengan algoritma Diffie-Hellman berdasarkan fungsi polinomial Chebyshev.

Kata kunci : kunci publik, Diffie-Hellman, polinomial Chebyshev, kunci rahasia.

xi+30 halaman : 5 gambar

Daftar Pustaka : 5 (2003-2007)

ABSTRACT

Name : Merysa Amanda

Study Program : S1 Mathematics

Title : Diffie-Hellman algorithm using Chebyshev polynomial.

Diffie-Hellman algorithm is used to obtain a secret key by using a public key. This final project will study how to obtain a secret key by Diffie-Hellman algorithm based on Chebyshev polynomial.

Key words : public key, Diffie-Hellman, Chebyshev polynomial, secret key.

xii+30 pages : 5 pictures

Bibliography : 5 (2003-2007)

DAFTAR ISI

DAFTAR GAMBAR

BAB 1
PENDAHULUAN

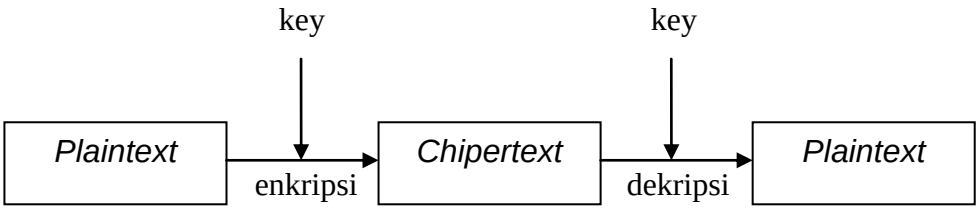
1.1 Latar Belakang

Beberapa puluh tahun yang lalu kita masih bergantung kepada surat sebagai sarana untuk berkomunikasi dengan orang lain yang berada sangat jauh dengan tempat di mana kita tinggal. Dibutuhkan waktu yang cukup lama hingga surat kita dapat diterima. Tetapi saat ini, dengan berkembang pesatnya teknologi maka komunikasi dapat dilakukan dengan cara yang jauh lebih mudah, cepat dan efisien.

Dalam bidang komunikasi, kadang-kadang dibutuhkan juga agar pesan yang kita kirimkan terjaga kerahasiaan dan keamanannya. Agar tidak terjadi kesalahan komunikasi antara pengirim dan penerima, proses pengiriman pesan pada saat dikirim hingga sampai ke penerima isi pesan harus dijamin keamanan dan keasliannya. Untuk menjamin hal tersebut maka kita menggunakan enkripsi dan dekripsi pada setiap proses pengiriman pesan.

Menurut definisi secara umum, enkripsi adalah proses mengubah pesan yang dapat dibaca dan dimengerti maknanya menjadi bentuk pesan yang tersandi dan tidak dapat dimengerti maknanya oleh pihak lain. Sedangkan dekripsi adalah proses mengembalikan pesan tersandi menjadi pesan yang dimengerti maknanya oleh pihak penerima informasi. (Rinaldi Munir, 2004)

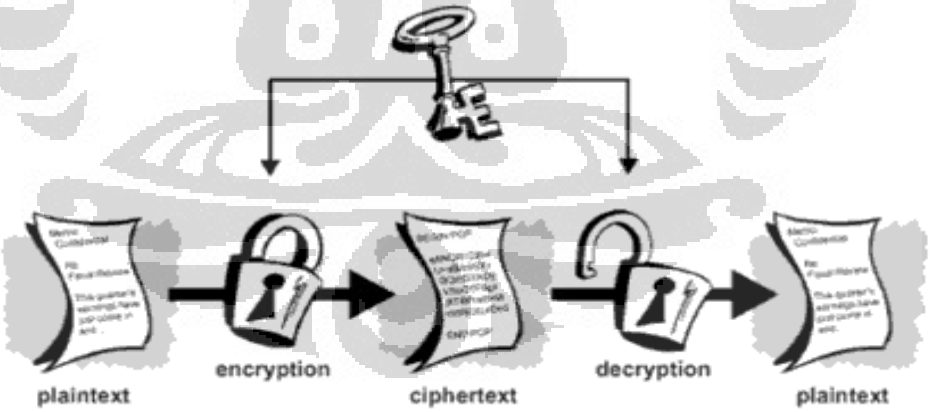
Kriptografi adalah ilmu yang mempelajari tentang kerahasiaan pesan. (Schneier, 2007) Dalam kriptografi, enkripsi adalah suatu proses transformasi pesan/informasi (*plaintext*) dengan menggunakan suatu kunci, agar tidak dapat terbaca oleh siapapun kecuali mereka yang memiliki kunci tersebut. Pesan yang sudah dienkripsi ini disebut sebagai *ciphertext*, sedangkan dekripsi adalah proses mengembalikan *ciphertext* menjadi *plaintext* awal. (Rinaldi Munir, 2004)



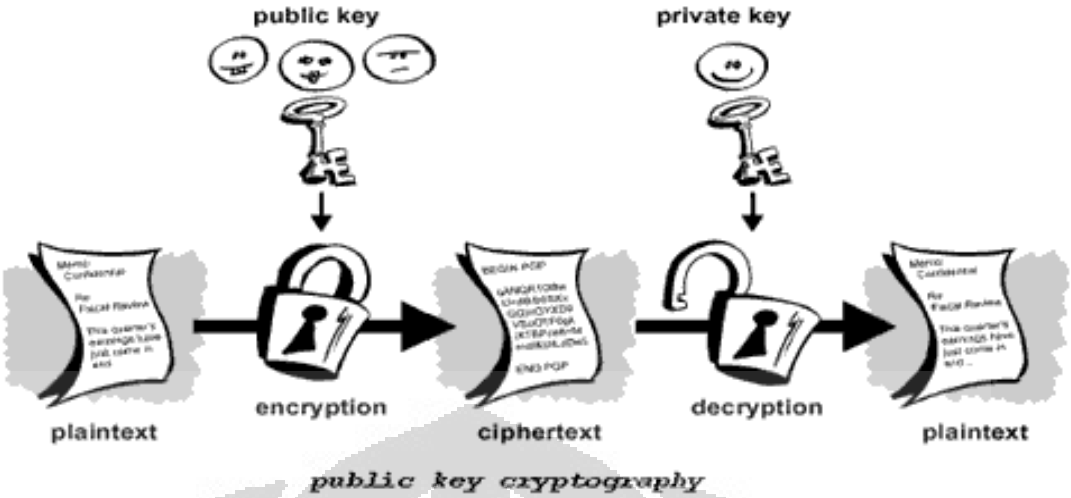
Gambar 1.1 Proses enkripsi dan dekripsi dengan suatu kunci

Penggunaan enkripsi / dekripsi dalam seni komunikasi telah digunakan oleh Bangsa Sparta sejak 400 SM (Thomas Kelly, 1998) dan hingga saat ini, penggunaan enkripsi/dekripsi sudah mengalami perkembangan yang cukup pesat dan digunakan di berbagai macam aspek kehidupan kita sehari-hari seperti transaksi internet banking dan verifikasi akun email. (Schneier, 2007)

Berdasarkan kunci, metode enkripsi/dekripsi dalam kriptografi dibagi menjadi dua tipe yaitu metode dengan kunci simetris dan metode dengan kunci asimetris. Pada metode dengan kunci simetris menggunakan satu kunci rahasia yang sama-sama digunakan untuk proses enkripsi dan dekripsi. Sedangkan metode dengan kunci asimetris menggunakan kunci yang berbeda yaitu satu *public key* yang digunakan oleh pengirim untuk melakukan enkripsi dan satu *private key* yang digunakan untuk melakukan dekripsi. (William Stallings, 2005)



Gambar 1.2 Proses enkripsi/dekripsi dengan kunci simetris



Gambar 1.3 Proses enkripsi/dekripsi dengan kunci asimetris

Ada beberapa contoh proses enkripsi/dekripsi yang menggunakan *private key* yaitu AES, 3DES, dan IDEA. Sedangkan contoh proses enkripsi/dekripsi yang menggunakan *public key* yaitu Diffie-Hellman, ElGamal, Cramer-Shoup, Elliptic Curve dan DSS. (William Stallings, 2005)

Jika pembentukkan kunci rahasia pada buku yang berjudul *Cryptography and Network Security Principles and Practices 4th Edition* oleh William Stallings (2005) menggunakan algoritma Diffie-Hellman berdasarkan fungsi monomial x^n dengan x positif pada proses pembentukkan kunci publik, maka pada tugas akhir ini, akan dilakukan penggantian monomial x^n (x positif) dengan polinomial yang dikenal sebagai polinomial Chebyshev $T_n(x)$. (G. J. Fee & M. B. Monagan, 2004)

1.2 Rumusan Masalah dan Ruang Lingkup

Berdasarkan latar belakang masalah di atas, masalah yang akan di bahas adalah pembentukkan kunci rahasia dengan menggunakan algoritma Diffie-Hellman berdasarkan fungsi polinomial Chebyshev. Pada tugas akhir ini, fungsi polinomial Chebyshev berlaku untuk semua bilangan riil x.

1.3 Jenis dan Metode Penelitian

Jenis penelitian yang dilakukan adalah studi literature. Metode yang digunakan adalah mengimplementasikan fungsi polinomial Chebyshev pada algoritma Diffie-Hellman dalam pembentukkan kunci rahasia.

1.4 Tujuan Penulisan

Sesuai dengan permasalahan yang diangkat dalam penulisan ini, maka tujuan penulisan tugas akhir ini adalah sebagai berikut:

1. Menerapkan algoritma Diffie-Hellman dengan menggunakan polinomial Chebyshev dalam pembentukkan kunci rahasia.
2. Menunjukkan contoh pembentukkan kunci rahasia untuk algoritma Diffie-Hellman.

BAB 2
LANDASAN TEORI

Pada bab ini akan dibahas teori-teori dasar yang berkaitan dengan pembentukkan kunci rahasia menggunakan algoritma Diffie-Hellman berdasarkan polinomial Chebyshev. Pembahasan dimulai dengan teori bilangan pada sub bab 2.1, pada sub bab 2.2 dibahas mengenai algoritma Diffie-Hellman dan pada sub bab 2.3 tentang polinomial Chebyshev.

2.1 Teori Bilangan

Dalam situasi tertentu, seringkali diperlukan sisa pembagian dari dua bilangan yang dikenal dengan kongruen ke suatu bilangan. Untuk menjelaskan pengertian tersebut, digunakan sifat bilangan bulat berikut :

Teorema 2.1.1

Misalkan a adalah bilangan bulat dan m bilangan bulat positif, maka terdapat bilangan bulat q dan r yang tunggal dengan $0 \leq r < m$ sedemikian sehingga $a = mq + r$.

(Kenneth H. Rosen, 2007)

Definisi 2.1.1

Misalkan a dan b adalah bilangan bulat dan m bilangan bulat positif, maka a kongruen ke b modulo m jika m habis membagi $a - b$ atau $m|(a - b)$ dan dinotasikan dengan $a \equiv b \pmod{m}$. Sedangkan jika a dan b tidak kongruen dinotasikan dengan $a \not\equiv b \pmod{m}$.

(Kenneth H. Rosen, 2007)

Setelah mengetahui pengertian kekongruenan, dilanjutkan dengan definisi *gcd* yang akan digunakan dalam definisi relatif prima.

Definisi 2.1.2

Misalkan a dan b adalah dua buah bilangan bulat tidak nol. Bilangan bulat terbesar d sedemikian sehingga $d \mid a$ dan $d \mid b$ disebut pembagi bersama terbesar (*gcd* atau *greatest common divisor*) dari a dan b. Dinotasikan oleh $gcd(a, b)$. (Kenneth H. Rosen, 2007)

Contoh 1

Tentukan *gcd* dari 45 dan 36.

Penyelesaian:

Faktor pembagi 45 : 1, 3, 5, 9, 15, 45

Faktor pembagi 36 : 1, 2, 3, 4, 9, 12, 18, 36

Faktor pembagi bersama dari 45 dan 36 adalah : 1, 3, 9

Sehingga $gcd(45, 36) = 9$

Definisi 2.1.3

Dua buah bilangan bulat a dan b dikatakan *relatif prima* jika $gcd(a, b) = 1$. (Kenneth H. Rosen, 2007)

Contoh 2

20 dan 3 relatif prima karena $gcd(20,3) = 1$.

Begitu juga 7 dan 11 relatif prima karena $gcd(7,11) = 1$.

Tetapi 20 dan 5 tidak relatif prima karena $gcd(20,5) = 5 \neq 1$.

Di bawah ini akan didefinisikan fungsi Euler ϕ dan order dari a modulo m yang akan digunakan untuk menjelaskan akar primitif.

Definisi 2.1.4

Fungsi Euler ϕ dari m dinotasikan dengan $\phi(m)$ untuk $m \geq 1$ adalah banyaknya bilangan bulat positif $< m$ yang relatif prima dengan m.

(David M. Burton, 2007)

Contoh 3

Tentukan $\phi(20)$.

Penyelesaian:

Bilangan bulat positif yang lebih kecil dari 20 adalah 1 sampai 19. Di antara bilangan-bilangan tersebut, terdapat $\phi(20) = 8$ buah yang relatif prima dengan 20, yaitu 1, 3, 7, 9, 11, 13, 17, 19.

Teorema 2.1.2

Jika m bilangan prima, maka banyaknya bilangan bulat yang lebih kecil dari m dan relatif prima terhadap m adalah $\phi(m) = m - 1$.

(David M. Burton, 2007)

Definisi 2.1.5

Misalkan a adalah bilangan bulat dan bilangan bulat $m > 1$ dan $gcd(a, m) = 1$. Order dari a modulo m adalah suatu bilangan bulat positif terkecil t sedemikian sehingga $a^t \equiv 1 \ (mod\ m)$.

(David M. Burton, 2007)

Contoh 4

Carilah order a dari modulo 11 untuk $a = 1, 2, 3, 4, 5, 6, \ldots, 10$

Penyelesaian:

Untuk $a = 1$

Maka $1^t \equiv 1 \ (mod\ 11)$ berlaku dengan $t = 1, 2, 3, 4, \ldots$

Karena 1 adalah bilangan bulat positif terkecil t. Jadi, order 1 (mod 11) adalah 1.

Untuk $a = 2$

Maka $2^t \equiv 1 \ (mod\ 11)$ berlaku dengan $t = 10, 20, 30, 40, \ldots$

Karena 10 adalah bilangan bulat positif terkecil t. Jadi, order 2 (mod 11) adalah 10.

Untuk $a = 3$

Maka $3^t \equiv 1 \ (mod\ 11)$ berlaku dengan $t = 5, 10, 15, 20, \ldots$

Karena 5 adalah bilangan bulat positif terkecil t. Jadi, order 3 (mod 11) adalah 5.

Untuk $a = 4$

Maka $4^{\,t} \equiv 1 \,(\, mod\ 11\,)$ berlaku dengan $t = 5, 10, 15, 20, ...$

Karena 5 adalah bilangan bulat positif terkecil t. Jadi, order 4 (mod 11) adalah 5.

Untuk $a = 5$

Maka $5^{\,t} \equiv 1 \,(\, mod\ 11\,)$ berlaku dengan $t = 5, 10, 15, 20, ...$

Karena 5 adalah bilangan bulat positif terkecil t. Jadi, order 5 (mod 11) adalah 5.

Untuk $a = 6$

Maka $6^{\,t} \equiv 1 \,(\, mod\ 11\,)$ berlaku dengan $t = 10, 20, 30, 40, ...$

Karena 10 adalah bilangan bulat positif terkecil t. Jadi, order 6 (mod 11) adalah 10.

Untuk $a = 7$

Maka $7^{\,t} \equiv 1 \,(\, mod\ 11\,)$ berlaku dengan $t = 10, 20, 30, 40, ...$

Karena 10 adalah bilangan bulat positif terkecil t. Jadi, order 7 (mod 11) adalah 10.

Untuk $a = 8$

Maka $8^{\,t} \equiv 1 \,(\, mod\ 11\,)$ berlaku dengan $t = 10, 20, 30, 40, ...$

Karena 10 adalah bilangan bulat positif terkecil t. Jadi, order 8 (mod 11) adalah 10.

Untuk $a = 9$

Maka $9^{\,t} \equiv 1 \,(\, mod\ 11\,)$ berlaku dengan $t = 5, 10, 15, 20, ...$

Karena 10 adalah bilangan bulat positif terkecil t. Jadi, order 9 (mod 11) adalah 5.

Untuk $a = 10$

Maka $10^{\,t} \equiv 1 \,(\, mod\ 11\,)$ berlaku dengan $t = 2, 4, 6, 8, ...$

Karena 2 adalah bilangan bulat positif terkecil t. Jadi, order 10 (mod 11) adalah 2.

Jadi, order a mod 7 adalah 1, 10, 5, 5, 5, 10, 10, 10, 5, 2.

Pada contoh 4 tampak bahwa order dari bilangan-bilangan bulat positif a modulo 11 masing-masing selalu membagi $\phi(11) = 10$.

Teorema 2.1.3

Jika m adalah bilangan prima dan order a modulo m adalah k dimana $a < m$ sehingga $a^{\phi(m)} \equiv 1 \ (mod\ m)$, maka $k|\phi(m)$ atau order a modulo m selalu membagi $\phi(m)$.

(David M. Burton, 2007)

Setelah mengetahui tentang order a mod m, maka berikut ini akan dijelaskan apa yang dimaksud dengan akar primitif.

Definisi 2.1.6

Jika $gcd(a, m) = 1$ dan order dari a modulo m adalah $\phi(m)$, maka a dinamakan akar primitif dari m. Dengan kata lain, bilangan bulat positif m mempunyai akar primitif a, apabila

$$a^{\phi(m)} \equiv 1 (mod\ m) \text{ asalkan } a^k \not\equiv 1 \ (mod\ m)$$

untuk semua bilangan bulat positif $k < \phi(m)$.

(David M. Burton, 2007)

Contoh 5

Tentukan akar-akar primitif dari 9.

Penyelesaian:

Diketahui dari definisi 2.1.4 bahwa $\phi(9) = 6$.

Untuk $a = 1$

Order 1 (mod 9) adalah 1. Karena $1 \neq \phi(9) = 6$ maka $a = 1$ bukan akar primitif dari m.

Untuk $a = 2$

Order 2 (mod 9) adalah 6. Karena $6 = \phi(9)$ maka $a = 2$ adalah akar primitif dari m.

Untuk $a = 3$

Order 3 (mod 9) adalah 0. Karena $\gcd(3, 9) = 3$ dan $0 \neq \phi(9) = 6$ maka $a = 3$ bukan akar primitif dari m.

Untuk $a = 4$

Order 4 (mod 9) adalah 3. Karena $3 \neq \phi(9) = 6$ maka $a = 4$ bukan akar primitif dari m.

Untuk $a = 5$

Order 5 (mod 9) adalah 6. Karena $6 = \phi(9)$ maka $a = 5$ adalah akar primitif dari m.

Untuk $a = 6$

Order 6 (mod 9) adalah 0. Karena $\gcd(6, 9) = 3$ dan $0 \neq \phi(9) = 6$ maka $a = 6$ bukan akar primitif dari m.

Untuk $a = 7$

Order 7 (mod 9) adalah 3. Karena $3 \neq \phi(9) = 6$ maka $a = 7$ bukan akar primitif dari m.

Untuk $a = 8$

Order 8 (mod 9) adalah 2. Karena $2 \neq \phi(9) = 6$ maka $a = 8$ bukan akar primitif dari m.

Berdasarkan definisi akar primitif, jika gcd (2, 9) = 1, gcd (5, 9) = 1 dan order-order dari 2 dan 5 modulo 9 masing-masing adalah 6, $\phi(9) = 6$, maka akar-akar primitif dari 9 adalah 2 dan 5.

Untuk keamanan maksimal dianjurkan memilih elemen akar primitif dalam algoritma Diffie-Hellman.

2.2 Algoritma Diffie-Hellman

Algoritma Diffie-Hellman adalah algoritma yang menggunakan *public-key* dalam proses pembentukkan kunci rahasia. Untuk mendapatkan kunci rahasia harus melalui beberapa tahap yang di dalamnya terjadi kesepakatan kunci yang dikenal dengan kespakatan kunci Diffie-Hellman. Nama algoritma ini diambil dari Martin E. Hellman dan Bailey W. Diffie yang merupakan penemu dari algoritma Diffie-Hellman pada tahun 1976. Tujuan dari algoritma ini adalah supaya kedua pihak dapat melakukan kesepakatan kunci yang hasilnya nanti dapat digunakan

dalam proses enkripsi / dekripsi pesan yang dikirim maupun diterima. (William Stallings, 2005)

Proses pembentukkan kunci rahasia dimulai dengan mendefinisikan sebuah akar primitif dari sebuah bilangan prima p. Karena p prima, maka bilangan yang relatif prima dengan p adalah $1, 2, \dots, p-1$ dimana order dari bilangan-bilangan ini membagi $\phi(p)$. Pilih bilangan g dengan order $\phi(p)$ yang menurut definisi 2.1.6 disebut sebagai akar primitif dari sebuah bilangan prima p, maka diperoleh barisan

$$g \bmod p,\ g^2 \bmod p,\ \dots,\ g^{p-1} \bmod p$$

yang merupakan barisan bilangan bulat yang berbeda dan terdiri dari 1 sampai $p-1$.

Pada algoritma Diffie-Hellman sendiri terdapat beberapa elemen-elemen dasar yang dibutuhkan dalam menjalankan algoritma tersebut :

- Sebuah bilangan prima p
- Sebuah akar primitif dari p, yaitu g
- Bilangan bulat rahasia yang dimiliki pihak I (m) dan pihak II (n) dan nilainya di antara 0 dan p
- *Public key* yang dimiliki pihak I (a) yang didapatkan dari kalkulasi menggunakan bilangan bulat rahasia milik pihak I yaitu $a = (g^m) \bmod p$
- *Public key* yang dimiliki pihak II (b) yang didapatkan dari kalkulasi menggunakan bilangan bulat rahasia milik pihak II yaitu $b = (g^n) \bmod p$

Elemen-elemen di atas digunakan untuk pembentukkan sebuah kunci rahasia yang akan digunakan dalam proses enkripsi/dekripsi pesan.

Berikut akan dijelaskan pembentukkan kunci rahasia dengan menggunakan algoritma Diffie-Hellman.

Misalkan Alice sebagai pihak I dan Bob sebagai pihak II akan membentuk suatu kunci rahasia. Dimana tahap-tahap yang harus dilalui, yaitu :

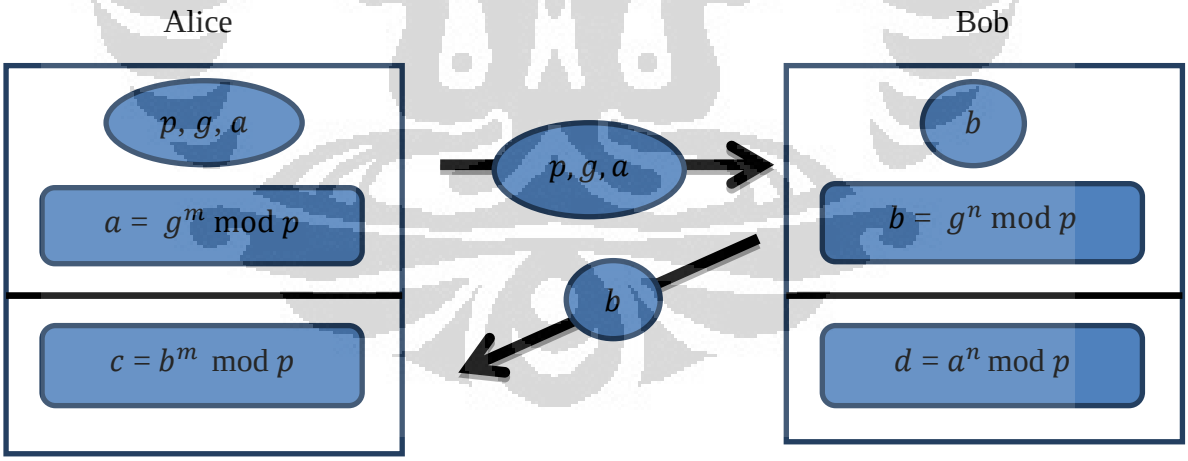
1. Alice memilih bilangan prima p dan bilangan bulat positif g yang merupakan akar primitif dari p.
2. Alice memilih bilangan bulat rahasia m dengan $0 < m < p$
3. Alice menghitung $a = g^m \bmod p$
4. Alice mengirim pesan p, g dan a ke Bob
5. Bob memilih bilangan bulat rahasia n dengan $0 < n < p$
6. Bob menghitung $b = g^n \bmod p$
7. Bob mengirim pesan b ke Alice
8. Alice menghitung kunci rahasia $c = b^m \bmod p$
9. Bob menghitung kunci rahasia $d = a^n \bmod p$

Kunci rahasia adalah c dari Alice dan d dari Bob adalah

$$c = b^m \bmod p = (g^n)^m \bmod p \text{ dan } d = a^n \bmod p = (g^m)^n \bmod p$$

Karena $(g^n)^m = (g^m)^n$ maka $c = d$.

Dari tahap di atas terlihat bahwa kunci rahasia Alice dan Bob yaitu $c = d$. Di bawah ini adalah gambaran dari proses pembentukkan kunci rahasia.



Gambar 2.1 Proses pembentukkan kunci rahasia dengan menggunakan monomial

Berikut ini akan diberikan contoh pembentukkan kunci rahasia (*secret key*) dengan menggunakan algoritma Diffie-Hellman.

Contoh 6

1. Alice memilih bilangan prima $p = 13$ dan bilangan bulat positif $g = 7$ yang merupakan akar primitif dari p.

   Dari definisi 2.1.5 didapat order 7 (mod 13) adalah 12. Karena $12 = \phi(13)$ maka berdasarkan definisi 2.1.6, $g = 7$ adalah akar primitif dari p.
2. Alice memilih sebuah bilangan bulat $m = 4$
3. Alice menghitung $a = 7^4 \ mod \ 13$

   $$a = 2401 \ mod \ 13 = 9$$
4. Alice mengirim pesan $p = 13 , g = 7 \ dan \ a = 9$ ke Bob
5. Bob memilih sebuah bilangan bulat $n = 5$
6. Bob menghitung $b = 7^5 \ mod \ 13$

   $$b = 16807 \ mod \ 13 = 11$$
7. Bob mengirim pesan $b = 11$ ke Alice
8. Alice menghitung kunci rahasia $c = 11^4 \ mod \ 13$

   $c = 14641 \ mod \ 13 = 3$ maka $c = 3$
9. Bob mengitung kunci rahasia $d = 9^5 \ mod \ 13$

   $d = 59049 \ mod \ 13 = 3$ maka $d = 3$

Berdasarkan proses penghitungan di atas kita mendapatkan $c = d = 3$. Maka kunci rahasia Alice dan Bob adalah 3.

Pada tugas akhir ini akan dibahas algoritma Diffie-Hellman dengan menggunakan polinomial Chebyshev. Maka, berikut ini akan ditunjukkan definisi dan sifat dari polinomial Chebyshev.

2.3 Polinomial Chebyshev

Sebelum membahas sifat polinomial Chebyshev, terlebih dahulu akan ditunjukkan definisi dari polinomial Chebyshev.

Definisi 2.3.1

Suatu fungsi T_n dalam variabel $\boldsymbol{x}$ yang memenuhi

$$T_n(x) = \cos\left(n \arccos(x)\right) \tag{2.1}$$

untuk $x \in [-1, 1]$ dan $n = 0, 1, 2, \ldots$.

Untuk $x > 1, n = 0, 1, 2, \ldots$. kita dapat menggunakan formula

$$T_n(x) = cosh\left(n\, cosh^{-1}(x)\right) \tag{2.2}$$

disebut polinomial Chebyshev jenis pertama.

Polinomial Chebyshev jenis pertama untuk $n = 0, 1$ adalah

$$T_0(x) = 1$$
$$T_1(x) = x$$

Untuk $n \geq 1$, polinomial Chebyshev memenuhi teorema berikut.

Teorema polinomial Chebyshev jenis pertama untuk $n \geq 1$ dan x bilangan riil akan memenuhi relasi

$$T_{n+1}(x) = 2x\, T_n(x) - T_{n-1}(x) \tag{2.3}$$

(J.C Mason and D.C Handscom, 2003)

Bukti

Sesuai dengan definisi polinomial Chebyshev untuk $n \geq 0$

$$T_n(x) = cos\left(n\, arccos(x)\right)$$

Kita mempunyai

$$T_0(x) = cos\, 0 = 1$$

dan

$$T_1(x) = cos\left(arccos(x)\right) = x$$

Dari definisi didapatkan

$$T_{n+1}(x) = cos\big((n+1)\, arccos(x)\big) = cos\left(n\, arccos(x) + arccos(x)\right) \tag{2.4}$$

dan

$$T_{n-1}(x) = cos\big((n-1)\, arccos(x)\big) = cos\left(n\, arccos(x) - arccos(x)\right) \tag{2.5}$$

Berdasarkan sifat Trigonometri

$$cos(A + B) = cos\, A\, cos\, B - sin\, A\, sin\, B \tag{2.6}$$

dan

$$cos(A - B) = cos\, A\, cos\, B + sin\, A\, sin\, B \tag{2.7}$$

Untuk $A = n\,arccos(x)$ dan $B = arccos(x)$, maka persamaan (2.4) dan (2.5) menjadi

$$T_{n+1}(x) = cos(n\,arccos\,(x))\,cos(arccos(x)) - sin\,(n\,arccos(x))sin\,(arccos(x)) \quad (2.8)$$

dan

$$T_{n-1}(x) = cos(n\,arccos\,(x))\,cos(arccos(x)) + sin\,(n\,arccos(x))sin\,(arccos(x)) \quad (2.9)$$

Jika persamaan (2.8) dan (2.9) dijumlahkan, akan didapat persamaan berikut :

$$T_{n+1}(x) + T_{n-1}(x) = 2\,cos(n\,arccos\,(x))\,cos(arccos(x)) \quad (2.10)$$

karena

$$T_n(x) = cos\,(n\,arccos(x))$$

dan

$$x = \cos\,(arccos(x))$$

maka persamaan (2.10) dapat ditulis menjadi

$$T_{n+1}(x) + T_{n-1}(x) = 2\,T_n(x)x$$

atau

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$$

Dengan menggunakan persamaan ini didapat

$T_2(x) = 2x^2 - 1$

$T_3(x) = 4x^3 - 3x$

$T_4(x) = 8x^4 - 8x^2 + 1$

$T_5(x) = 16x^5 - 20x^3 + 5x$

$T_6(x) = 32x^6 - 48x^4 + 18x^2 - 1$

$T_7(x) = 64x^7 - 112x^5 + 56x^3 - 7x$

$T_8(x) = 128x^8 - 256x^6 + 160x^4 - 32x^2 + 1$

$T_9(x) = 256x^9 - 576x^7 + 432x^5 - 120x^3 + 9x$

$T_{10}(x) = 512x^{10} - 1280x^8 + 1120x^6 - 400x^4 + 50x^2 - 1$

$T_{11}(x) = 1024x^{11} - 2816x^9 + 2816x^7 + 1232x^5 + 220x^3 - 11x$

$T_{12}(x) = 2048x^{12} - 6144x^{10} + 6912x^8 - 3584x^6 + 840x^4 - 72x^2 + 1$

$T_{13}(x) = 4096x^{13} - 13312x^{11} + 16640x^9 - 9984x^7 + 2912x^5 + 13x^3$

Dengan menggunakan maple juga dapat dicari $T_n(x)$ dengan $n = 0, 1, 2, 3, \ldots$

```
> ChebyshevT(n, x)
```

$$\text{ChebyshevT}(n, x)$$

Untuk $n = 0$

```
> ChebyshevT(0, x)
```

$$\text{ChebyshevT}(0, x)$$

```
> simplify(%,'ChebyshevT')
```

$$1$$

Untuk $n = 1$

```
> ChebyshevT(1, x)
```

$$\text{ChebyshevT}(1, x)$$

```
> simplify(%,'ChebyshevT')
```

$$x$$

Untuk $n = 2$

```
> ChebyshevT(2, x)
```

$$\text{ChebyshevT}(2, x)$$

```
> simplify(%,'ChebyshevT')
```

$$-1 + 2x^2$$

Untuk $n = 3$

```
> ChebyshevT(3, x)
```

$$\text{ChebyshevT}(3, x)$$

```
> simplify(%,'ChebyshevT')
```

$$4x^3 - 3x$$

Untuk $n = 4$

```
> ChebyshevT(4, x)
```

$$\text{ChebyshevT}(4, x)$$

```
> simplify(%,'ChebyshevT')
```

$$1 + 8x^4 - 8x^2$$

BAB 3
PEMBENTUKKAN KUNCI RAHASIA DENGAN POLINOMIAL CHEBYSHEV

Pada bab 2 telah dibahas proses pembentukkan kunci rahasia dengan algoritma Diffie-Hellman menggunakan fungsi monomial x^n dengan x positif. Pada bab ini akan ditunjukkan proses pembentukkan kunci rahasia dengan algoritma Diffie-Hellman yang menggunakan fungsi lain yaitu fungsi Chebsyshev.

3.1 Algoritma Diffie-Hellman Dengan Menggunakan Polinomial Chebyshev

Berikut ini akan ditunjukkan bahwa fungsi Chebyshev dapat digunakan untuk menggantikan monomial x^n untuk pembentukkan kunci rahasia pada algoritma Diffie-Hellman. Sifat persamaan $(x^m)^n = x^{mn} = (x^n)^m$ yang digunakan pada algoritma Diffie-Hellman akan ditunjukkan juga terpenuhi oleh polinomial Chebyshev dari jenis pertama.

Sifat untuk setiap polinomial Chebyshev jenis pertama $T_n(x)$, $x \in Z_p$ berlaku:

$$T_m(T_n(x)) = T_{mn}(x) = T_n(T_m(x)) \tag{3.1}$$

Bukti

Berdasarkan definisi polinomial Chebyshev

$$T_n(x) = \cos(n \arccos(x))$$

yang berlaku untuk semua riil x dalam interval [-1 , 1].

Maka didapat

$$\begin{aligned} T_m(T_n(x)) &= T_m(\cos(n \arccos(x)) \\ &= cos\ (m\ arccos\ (cos\ (n\ arccos\ (x)))) \\ &= \cos(m\ (n \arccos(x))) \\ T_{mn}(x) &= \cos(mn \arccos(x)) \end{aligned}$$

$$= cos\ (nm\ arccos\ (x))$$
$$= \cos\ (n\ (m \arccos\ (x)))$$
$$= cos\ (n\ arccos\ (cos\ (m\ arccos\ (x))))$$
$$= T_n(\cos\ (m \arccos\ (x))$$
$$= T_n\big(T_m(x)\big)$$

Untuk $x > 1$, kita dapat menggunakan formula

$$T_n(x) = cosh\ (n\ cosh^{-1}\ (x))$$

sehingga

$$T_m\big(T_n(x)\big) = T_m(\cosh\ (n\ cosh^{-1}\ (x))$$
$$= cosh\ (m\ cosh^{-1}(cosh\ (n\ cosh^{-1}\ (x))))$$
$$= \cosh\ (m\ (n\ cosh^{-1}\ (x)))$$
$$T_{mn}(x) = \cosh\ (mn\ cosh^{-1}\ (x))$$
$$= cosh\ (nm\ cosh^{-1}\ (x))$$
$$= \cosh\ (n\ cosh^{-1}\ (x)))$$
$$= cosh\ (n\ cosh^{-1}\ (cosh\ (m\ cosh^{-1}\ (x))))$$
$$= T_n(\cosh\ (m\ cosh^{-1}\ (x))$$
$$= T_n\big(T_m(x)\big)$$

Terbukti bahwa setiap polinomial Chebyshev $T_n(x)$, berlaku sifat:

$$T_m(T_n(x)) = T_{mn}(x) = T_n(T_m(x))$$

(G. J. Fee & M. B. Monagan, 2004)

Sifat

$$T_n(x)\ mod\ p = T_n(x\ mod\ p)\ mod\ p\ ,\ x \in Z_p \qquad (3.2)$$

Sifat di atas dapat ditunjukkan dengan cara berikut :

Bukti

Pandang $Z_p = \{0, 1, 2, \dots, p-1\}$ dengan p bilangan prima

Pada Z_p berlaku

$$(a+b)\ mod\ p = a\ mod\ p + b\ mod\ p$$
$$ab\ mod\ p = (a\ mod\ p)(b\ mod\ p) mod\ p$$

Untuk $b = a$

$$a^2 \bmod p = aa \bmod p = (a \bmod p)(a \bmod p) \bmod p = (a \bmod p)^2 \bmod p$$

Untuk $b = a^2$

$$a^3 \bmod p = aa^2 \bmod p = (a \bmod p)(a^2 \bmod p) \bmod p = (a \bmod p)^3 \bmod p$$

Untuk $b = a^{n-1}$

$$a^n \bmod p = (a \bmod p)^n \bmod p$$

Jika $x \in Z_p$, maka

$$x^n \bmod p = (x \bmod p)^n \bmod p$$

Jika $T_n(x)$ dengan $x \in Z_p$ dan $a_i \in Z_p$, $i = 0, 1, 2, \dots, n$ maka $T_n(x) \bmod p$ akan diperoleh dengan cara berikut :

Untuk koefisien $a_i \in Z_p$, $i = 0, 1, 2, \dots, n$ maka

$$a_i \, x^i \bmod p = a_i \, (x \bmod p)^i \bmod p \tag{3.3}$$

Karena $T_n(x)$ berbentuk polinomial dan dapat dinyatakan sebagai berikut

$$T_n(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0 \tag{3.4}$$

maka

$$T_n(x) \bmod p = (a_n x^n + a_{n-1} \, x^{n-1} + a_{n-2} \, x^{n-2} + \dots + a_1 x + a_0) \bmod p \tag{3.5}$$

dan

$$T_n(x \bmod p) \bmod p =$$
$$(a_n \, (x \bmod p)^n + a_{n-1} \, (x \bmod p)^{n-1} + a_{n-2} \, (x \bmod p)^{n-2} + \dots +$$
$$a_1 (x \bmod p) + a_0) \bmod p \tag{3.6}$$

Berdasarkan persamaan (3.3) maka

$$T_n(x) \bmod p = (a_n x^n + a_{n-1} \, x^{n-1} + a_{n-2} \, x^{n-2} + \dots + a_1 x + a_0) \bmod p =$$
$$(a_n \, (x \bmod p)^n + a_{n-1} \, (x \bmod p)^{n-1} + a_{n-2} \, (x \bmod p)^{n-2} + \dots +$$
$$a_1 (x \bmod p) + a_0) \bmod p = T_n(x \bmod p) \bmod p \tag{3.7}$$

Sehingga

$$T_n(x) \bmod p = T_n(x \bmod p) \bmod p$$

Dengan menggunakan polinomial Chebyshev yang bekerja pada Z_p , maka elemen-elemen dasar yang dibutuhkan dalam menjalankan algoritma Diffie-Hellman dengan menggunakan polinomial Chebyshev adalah

- Sebuah bilangan prima p
- Sebuah akar primitif dari p, yaitu g
- Bilangan bulat rahasia yang dimiliki pihak I (m) dan pihak II (n) dan nilainya di antara 0 dan p
- *Public key* yang dimiliki pihak I (c) yang didapatkan dari kalkulasi menggunakan bilangan bulat rahasia milik pihak I yaitu

$$c = T_m(g) \bmod p$$

- *Public key* yang dimiliki pihak II (d) yang didapatkan dari kalkulasi menggunakan bilangan bulat rahasia milik pihak II yaitu

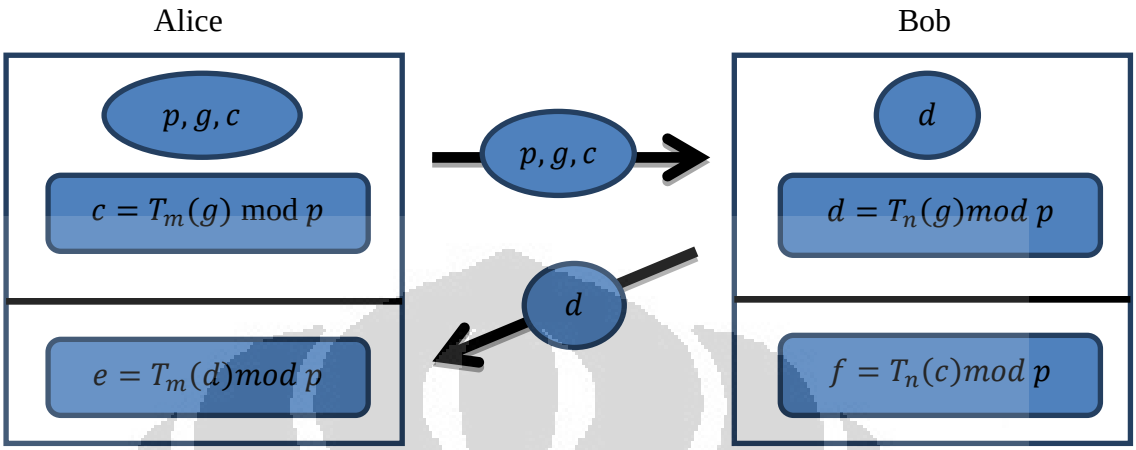
$$d = T_n(g) \bmod p$$

Jadi, algoritma Diffie-Hellman menggunakan polinomial Chebyshev dengan Alice sebagai pihak I dan Bob sebagai pihak II sebagai berikut :

1. Alice memilih bilangan prima p dan bilangan bulat positif g yang merupakan akar primitif dari p.
2. Alice memilih bilangan bulat rahasia m dengan $0 < m < p$
3. Alice menghitung $c = T_m(g) \bmod p$
4. Alice mengirim pesan p, g dan c ke Bob
5. Bob memilih bilangan bulat rahasia n dengan $0 < n < p$
6. Bob menghitung $d = T_n(g) mod\ p$
7. Bob mengirim pesan d ke Alice
8. Alice menghitung kunci rahasia $e = T_m(d) mod\ p$
9. Bob menghitung kunci rahasia $f = T_n(c) mod\ p$

Bilangan bulat e untuk Alice dan bilangan bulat f untuk Bob merupakan kunci rahasia dari hasil perhitungan $T_{mn}(g) \bmod p$.

Di bawah ini adalah gambaran sederhana proses pembentukan kunci rahasia Alice dan Bob dengan menggunakan polynomial Chebyshev.



Gambar 3.1 Proses pembentukkan kunci rahasia dengan polinomial Chebyshev

Berikut ini akan ditunjukkan bahwa kunci rahasia yang dihasilkan Alice dan Bob adalah sama.

Secret key yang dihasilkan Alice e

$e = T_m(d)\ mod\ p$

$= T_m(T_n(g)\ mod\ p)\ mod\ p$ Berdasarkan persamaan (3.2) maka didapat

$= T_m\big(T_n(g)\big)\ mod\ p$

$= T_{mn}(g)\ mod\ p$

Secret key yang dihasilkan Bob f

$f = T_n(c)\ mod\ p$

$= T_n(T_m(g)\ mod\ p)\ mod\ p$ Sesuai persamaan (3.2) maka didapat

$= T_n\big(T_m(g)\big)\ mod\ p$

$= T_{nm}(g)\ mod\ p$

Karena $T_{mn} = T_{nm}$ maka didapat $e = f$.

3.2 Contoh Algoritma Diffie-Hellman Dengan Menggunakan Polinomial Chebyshev

Pada bagian ini akan diberikan contoh pembentukkan kunci rahasia dengan menggunakan polinomial Chebyshev. Alice dan Bob akan melakukan kesepakatan kunci untuk membentuk kunci rahasia dengan menggunakan algoritma Diffie-Hellman berdasarkan polinomial Chebyshev.

Contoh 7

Alice dan Bob memilih masing-masing bilangan bulat rahasia $m = 2$ dan $n = 5$.

Maka tahap yang harus dilalui untuk membentuk kunci rahasia adalah

1. Alice memilih bilangan prima $p = 13$ dan bilangan bulat positif $g = 7$ yang merupakan akar primitif dari p.

   Dari definisi 2.1.5 didapat order 7 (mod 13) adalah 12 sedemikian sehingga $7^{12} \equiv 1 \ (mod\ 13)$. Karena $12 = \phi(13)$ maka berdasarkan definisi 2.1.6, $g = 7$ adalah akar primitif dari p.

2. Alice memilih sebuah bilangan bulat rahasia $m = 2$
3. Alice menghitung $c = T_m(g) \bmod p$

   $$c = T_2(7)\ mod\ p = (2(7)^2 - 1) \bmod 13 = 97 \bmod 13 = 6$$

4. Alice mengirim pesan nilai $p = 13,\ g = 7,\ dan\ c = 6$ ke Bob
5. Bob memilih sebuah bilangan bulat rahasia $n = 5$
6. Bob menghitung $d = T_n(g) mod\ p$

   $$d = T_5(7)\ mod\ p = (16(7)^5 - 20(7)^3 + 5(7)) \bmod 13$$
   $$= 262087 \bmod 13 = 7$$

7. Bob mengirim pesan $d = 7$ ke Alice
8. Alice menghitung kunci rahasia $e = T_m(d) mod\ p$

   $$e = T_2(7)\ mod\ p = (2(7)^2 - 1) \bmod 13 = 97 \bmod 13 = 6$$

9. Bob menghitung kunci rahasia $f = T_n(c) mod\ p$

$f = T_5(6)\ mod\ p = (16(6)^5 - 20(6)^3 + 5(6)) \bmod 13$

$= 120126 \bmod 13 = 6$

Bob dan Alice mendapatkan kunci rahasia yang sama-sama bernilai 6 yang mana $T_{10}(7) \bmod 13 = (512(7)^{10} - 1280(7)^8 + 1120(7)^6 - 400(7)^4 + 50(7)^2 - 1) \bmod 13 = 137379191137 \bmod 13 = 6.$

Contoh 8

Jika $m = 4$ dan $n = 3$ maka

$T_4(x) = 8x^4 - 8x^2 + 1$

$T_3(x) = 4x^3 - 3x$

dan

$T_{4\ .3}(x) = T_{12}(x)$

$= 2048x^{12} - 6144x^{10} + 6912x^8 - 3584x^6 + 840x^4 - 72x^2 + 1$

Maka tahap yang harus dilalui untuk membentuk kunci rahasia adalah

1. Alice memilih bilangan prima $p = 29$ dan bilangan bulat positif $g = 8$ yang merupakan akar primitif dari p.

   Dari definisi 2.1.5 didapat order 8 (mod 29) adalah 28 sedemikian sehingga $8^{28} \equiv 1\ (mod\ 29)$. Karena $28 = \phi(29)$ maka berdasarkan definisi 2.1.6, $g = 8$ adalah akar primitif dari p.

2. Alice memilih sebuah bilangan bulat rahasia $m = 4$
3. Alice menghitung $c = T_m(g) \bmod p$

   $c = T_4(8)\ mod\ p = (8(8)^4 - 8(8)^2 + 1) \bmod 29 = 32257 \bmod 29$

   $= 9$
4. Alice mengirim pesan nilai $p = 29,\ g = 8,\ dan\ c = 9$ ke Bob
5. Bob memilih sebuah bilangan bulat rahasia $n = 3$
6. Bob menghitung $d = T_n(g) mod\ p$

   $d = T_3(8)\ mod\ p = (4(8)^3 - 3(8)) \bmod 29 = 2024 \bmod 29 = 23$

7. Bob mengirim pesan $d = 23$ ke Alice
8. Alice menghitung kunci rahasia $e = T_m(d) mod\ p$

$$e = T_4(5)\ mod\ p = (8(23)^4 - 8(23)^2 + 1) \bmod 29$$
$$= 2234497 \bmod 29 = 18$$

9. Bob menghitung kunci rahasia $f = T_n(c) mod\ p$

$$f = T_3(9)\ mod\ p = (4(9)^3 - 3(9)) \bmod 29 = 2889 \bmod 29 = 18$$

Bob dan Alice mendapatkan kunci rahasia yang sama-sama bernilai 18 sama dengan

$$T_{12}(8)\ mod\ p = 2048(8)^{12} - 6144(8)^{10} + 6912(8)^8 - 3584(8)^6$$
$$+ 840(8)^4 - 72(8)^2 + 1\ mod\ 29$$
$$= 134255446617601\ mod\ 29 = 18$$

Kunci rahasia inilah yang akan digunakan pada proses enkripsi dan dekripsi.

BAB 4
KESIMPULAN

Sesuai dengan pembahasan pada bab 3, dapat disimpulkan bahwa algoritma Diffie-Hellman dapat diterapkan dengan menggunakan fungsi polinomial Chebyshev $T_n(x)$ untuk menggantikan fungsi monomial x^n dengan x bilangan bulat positif dalam pembentukkan kunci rahasia karena sifat persamaan $(x^m)^n = x^{mn} = (x^n)^m$ pada fungsi monomial juga terpenuhi pada fungsi polinomial Chebyshev jenis pertama yaitu $T_m(T_n(x)) = T_{mn}(x) = T_n(T_m(x))$ dengan $x \in Z_p$.

DAFTAR PUSTAKA

Burton, D. M. (2007). *Elementary Number Theory* (6th ed.). Singapore : McGraw-Hill.

Fee, G. J. & Monagan, M. B. (2004). *Cryptography using Chebyshev polynomial*. Canada.

Mason, J. C. & Handscom, D. C. (2003). *Chebyshev Polynomial*. Florida : Chapman & Hall/ CRC, Boca Raton.

Rosen, K. H. (2007). *Discrete Mathematics and Its Applications*. Singapore : McGraw-Hill.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices* (4th ed.). Prentice Hall.