Analisis Algoritma Pertukaran Kunci Diffie-Hellman

Sejarah

Pertukaran Kunci Diffie-Hellman (selanjutnya disebut D-H) merupakan sebuah metode untuk bertukar kunci yang akan digunakan untuk proses enskripsi pesan atau data. Metode D-H merupakan salah satu pelopor metode pertukaran kunci di bidang kriptografi. Metode ini pertama kali dipublikasikan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976. Metode D-H memungkinkan dilakukannya pertukaran kunci antara dua atau lebih pihak tanpa pihak-pihak tersebut harus bertemu atau berkomunikasi terlebih dahulu. Sampai saat ini metode D-H masih digunakan untuk menenskripsi data dan informasi, khususnya data dan informasi di internet. Contohnya, metode D-H digunakan di The Secure Shell (SSH) Transfer Layer Protocol.

Metode

Metode yang digunakan D-H pada dasarnya adalah sebuah prinsip aritmatika modular. Tahap terpenting dari metode D-H adalah ketika dua pihak bertukar *public key* masing-masing dan mengkalkulasikan *public key* temannya dengan bilangan rahasia miliknya dan bilangan *p* dan *g*, p adalah prima dan g adalah primitive root modulo dari p. Bilangan *p* yang biasa digunakan dalam aplikasi enskripsi data merupakan bilangan bulat besar yang terdiri dari 100-300 digit. Mengapa? Dengan memakai bilangan bulat yang sangat besar maka metode D-H akan sulit untuk dipecahkan dengan metode *discrete logarithm,* baca bagian permasalahan discrete logarithm*.*

Teori

Ada beberapa teori yang dipakai dalam pengaplikasian metode D-H ini. Teori tersebut antara lain:

1. Aritmatka Modular
2. Primitive Root Modulo
3. Discrete Logarithm Problem

Teori-teori tersebut dimanfaatkan sebagai prinsip dasar berfungsinya metode D-H.

Aplikasi

Alice dan Bob sepakat untuk menggunakan bilangan prima p = 23 dan g = 5 (g adalah primitive root modulo dari 23).

Alice memilih bilangan rahasia a = 6, dan mengirimkan Bob bilangan A = g^a mod p

A = 56 mod 23 = 8

Bob memilih bilangan rahasia b = 15, dan mengirimkan Alice bilangan B = g^b mod p

B = 515 mod 23 = 19

Alice menghitung s = B^a mod p

s = 196 mod 23 = 2

Bob menghitung s = A^b mod p

s = 815 mod 23 = 2

Alice dan Bob kini memiliki *shared key* yang sama.

Link

Link program web tertera di <http://mahasiswa.cs.ui.ac.id/~jundi.ahmad/DiffieHellman>