Diffie-Hellman Key Exchange

Tri Ahmad Irfan (1306398983)
Kelas MD2 - E
Asisten: Rayhan Anandya

Pada tugas pemrograman matematika diskret 2 ini, saya mengimplementasikan algoritma Diffie-Hellman Key Exchange dengan bahasa pemrograman Javascript.

Tentang Algoritma Diffie-Hellman

Algoritma Diffie-Hellman Key Exchange adalah sebuah algoritma untuk mengirim data rahasia melalui jalur komunikasi yang tidak aman. Inti dari algoritma ini adalah kedua belah pihak (pengirim dan penerima) telah setuju untuk menggunakan sebuah kunci bersama (shared key) sedemikian sehingga tidak ada pihak lain yang dapat mendapatkan kunci ini.

Langkah Algoritma Diffie-Hellman

1. A dan B menyetujui sebuah bilangan prima **p** dan sebuah angka **q**
2. A memilih sebuah bilangan rahasia **a**, dan mengirim sebuah kode publik kepada B. Kode publik tersebut adalah $\mathbf{P_A = (q \hat{} a) \bmod p}$
3. B memilih sebuah bilangan rahasia **b**, dan mengirim sebuah kode publik kepada A. Kode publik tersebut adalah $\mathbf{P_B = (q \hat{} b) \bmod p}$
4. A menghitung shared key $\mathbf{S = (P_B \hat{} a) \bmod p}$
5. B menghitung shared key $\mathbf{S = (P_A \hat{} b) \bmod p}$
6. Perhatikan bahwa A dan B mendapatkan shared key yang sama tanpa harus langsung mengirimkan angkanya
7. A dan B kemudian dapat berkomunikasi dengan memanfaatkan shared key tersebut

Contoh Langkah Algoritma Diffie-Hellman

1. A dan B menyetujui **p = 23** dan **q = 5**
2. A memilih **a = 6** dan mengirimkan $\mathbf{P_A = 5 \hat{} 6 \bmod 23 = 8}$
3. B memilih **b = 15** dan mengirimkan $\mathbf{P_B = 5 \hat{} 15 \bmod 23 = 19}$
4. A menghitung shared key $\mathbf{S = 19 \hat{} 6 \bmod 23 = 2}$
5. B menghitung shared key $\mathbf{S = 8 \hat{} 15 \bmod 23 = 2}$
6. A dan B mendapatkan shared key yang sama

Penjelasan Algoritma Diffie-Hellman

1. A menghitung shared key S dengan cara 19^6 mod 23
2. 19 didapatkan dari 5^15 mod 23
3. Berarti A menghitung S = 5^15^6 mod 23
4. B menghitung shared key S dengan cara 8^15 mod 23
5. 8 didapatkan dari 5^6 mod 23
6. Berarti B menghitung S = 5^6^15 mod 23
7. Perhatikan bahwa sesuai dengan sifat komutatif perpangkatan, 5^6^15 = 5^15^6

Cara Menjalankan Program

Saya mengimplementasikan algoritma ini dalam bahasa pemrograman JavaScript.

Berikut struktur direktori project saya

```
-  diffie-hellman              (folder utama)
      -  css                   (folder css)
            -  styles.css      (file css utama)
      -  js
            -  jquery.min.js   (file plugin jQuery)
            -  algorithm.js          (source code diffie-hellman)
      -  index.html            (main html file)
```

Program dapat dijalankan dengan membuka file index.html dengan web browser yang anda miliki. Begitu terbuka, akan muncul program yang saya buat dalam bentuk web app.

Informasi Website

Website untuk program ini dapat diakses di
http://irfan-.github.io/diffie-hellman/

Referensi

1. Rouse, Margaret. Diffie-Hellman key exchange (exponential key exchange). Search Security - Tech Target. <http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange>
2. Khan Academy. Diffie-Hellman key exchange. Journey into Cryptography - Khan Academy. <https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-2>
3. Young, Bill. Diffie-Hellman key exchange. Foundations of Computer Security - University of Texas at Austin. <https://www.cs.utexas.edu/users/byoung/cs361/lecture52.pdf>