Facultatea de Electronică, Telecomunicații
și Tehnologia Informației

Proiect validare

Diffie Hellman

Andrei Mihăescu
TSAC II, ianuarie 2016

Capitolul 1
Prezentare protocol

Metoda schimbului de chei Diffie-Hellman, cunoscută şi ca metoda de distribuţie a cheilor publice, poartă numele a doi specialişti de la Standford University, Whitfield Diffie şi Martin Hellman. În anul 1976, ei au inventat o metodă prin care două părţi pot cădea de comun acord să comunice prin mesaje secrete fără să fie nevoie de o terţă parte, de un schimb off-line sau de transmiterea vreunei valori secrete între ele.

Independent, Ralph Merkle a venit cu o soluţie de distribuţie a cheilor publice, numai că metoda propusă implica substanţiale cheltuieli pentru efectuarea calculelor şi a transmisiei. Varianta realizată de Diffie şi Hellman a fost numită sistemul distribuţiei cheilor publice sau al schimburilor de chei publice.

Metoda Diffie-Hellman se bazează pe conceptul perechii de chei publică privată. Protocolul începe cu fiecare parte care generează independent câte o cheie privată. În pasul următor, fiecare calculează câte o cheie publică, aceasta fiind o funcţie matematică a cheilor private respective. Urmează schimbul de chei publice.

În final, fiecare dintre cele două persoane calculează o funcţie a propriei chei private şi a cheii publice a celeilalte persoane. Matematica este cea care va face să se ajungă la aceeaşi valoare, care este derivată din cheile lor private. Ele vor folosi valoarea ca pe cheie a mesajului.

Diffie şi Hellman folosesc exponenţierea în aritmetica modulară pentru a calcula cheile publice şi cheia mesajului. Aritmetica modulară este ca şi aritmetica standard, cu excepţia faptului că foloseşte numere numai în intervalul 0 la N, numit modulo. Atunci când o operaţie produce un rezultat care este mai mare sau egal cu N, N este scăzut repetat din rezultat până când valoarea se încadrează în intervalul 0 la N-1 (ca şi cum s-ar împărţi la N şi se ia în seamă restul). De exemplu, 3+4 mod 5 = 2. Dacă rezultatul este negativ, N se adaugă acestuia până când se va încadra în intervalul 0 la N-1. De exemplu, 3-8 mod 7 = -5 mod 7 = 2.

În aritmetica modulară, exponenţierea este o funcţie într-un singur sens. Aceasta înseamnă că este uşor de calculat un număr y = gx mod N pentru o valoare secretă x, însă este mult mai dificil să se calculeze x din y, dacă numerele sunt suficient de mari, ca de exemplu o lungime de câteva sute de cifre (noi presupunem că g şi N sunt cunoscute). Aceasta este referită ca şi problema logaritmului discret pentru că x este logaritm din y în baza g (mod N), iar numerele sunt finite şi întregi. Cu metoda Diffie-Hellman a schimbului de chei publice, Alice şi Bob stabilesc cheia mesajului secret după cum urmează. Alice generează o cheie secretă xa şi Bob o cheie secretă xb. După aceasta, Alice calculează o cheie publică ya, care este g ridicat la puterea xa modulo p, unde p este un număr prim (adică nu poate fi descompus în produsul a două numere), g fiind mai mic decât p. Identic, Bob calculează o cheie publică yb, prin ridicarea lui g la puterea xb modulo p. Ei vor schimba valorile publice ale acestora. Apoi, Alice ridică cheia publică a lui Bob la puterea exponentului său, xa modulo p, în timp ce Bob ridică cheia publică a lui Alice la exponentul său, xb modulo p. Amândoi vor obţine acelaşi rezultat, g ridicat la puterea xa şi xb, iar rezultatul obţinut va fi folosit de amândoi drept cheia K a mesajului. Matematic, totul se va exprima astfel:

Deşi în practică se folosesc numere foarte lungi, de câteva sute de cifre, pentru a ajuta la înţelegerea modului de funcţionare, vom folosi numere mici.

Diffie-Hellman Key Exchange

Step	Alice	Bob
1	Parameters: p, g	
2	$A = \text{random}()$ $a = g^A \pmod p$	$\text{random}() = B$ $g^B \pmod p = b$
3	$a \longrightarrow$ $\longleftarrow b$	
4	$K = g^{BA} \pmod p = b^A \pmod p$	$a^B \pmod p = g^{AB} \pmod p = K$
5	$\longleftarrow E_K(data) \longrightarrow$	

Figura 1.1: Functionarea protocolului Diffie Hellman

Exemplul 1
Să presupunem că p = 7, g = 3, cheia lui Alice xa = 1 şi a lui Bob xb = 2 Vom avea:

- Alice calculează cheia sa publică: ya = gxa mod p = 31 mod 7 = 3
- Bob calculează cheia sa publică: yb = gxb mod p = 32 mod 7 = 2
- Alice calculează K = ybxa mod p = 21 mod 7 = 2
- Bob calculează K = yaxb mod p = 32 mod 7 = 2

sau K = gxa*xb mod p = 32×1 mod 7 = 9 mod 7 = 2.

Exemplul 2
Să presupunem că p = 5, g = 4, cheia lui Alice xa = 3 şi a lui Bob xb = 2

- Alice calculează cheia sa publică: ya = gxa mod p = 43 mod 5 = 4
- Bob calculează cheia sa publică: yb = gxb mod p = 42 mod 5 = 1
- Alice calculează K = ybxa mod p = 13 mod 5 = 1
- Bob calculează K = yaxb mod p = 42 mod 5 = 1

sau K = gxa*xb mod p = 43×2 mod 5 = 4096 mod 5 = 1. Se observă că în ambele cazuri K ia valori identice, 2, respectiv 1.

Metoda Diffie-Hellamn, precum şi variantele ei sunt utilizate în câteva protocoale de securitate a reţelelor şi în produse comerciale, inclusiv la AT&T 3600 Telephone Security Device, la Fortezza card – o variantă de carduri criptate, şi la Pretty Good Privacy pentru criptarea e-mail-urilor şi a unor fişiere.

Capitolul 2
Atacuri asupra protocolului

Acest tip de protocol este vulnerabil la atacurile de tip "Man-in-the-middle" care functioneaza dupa principiul ilustrat mai jos.

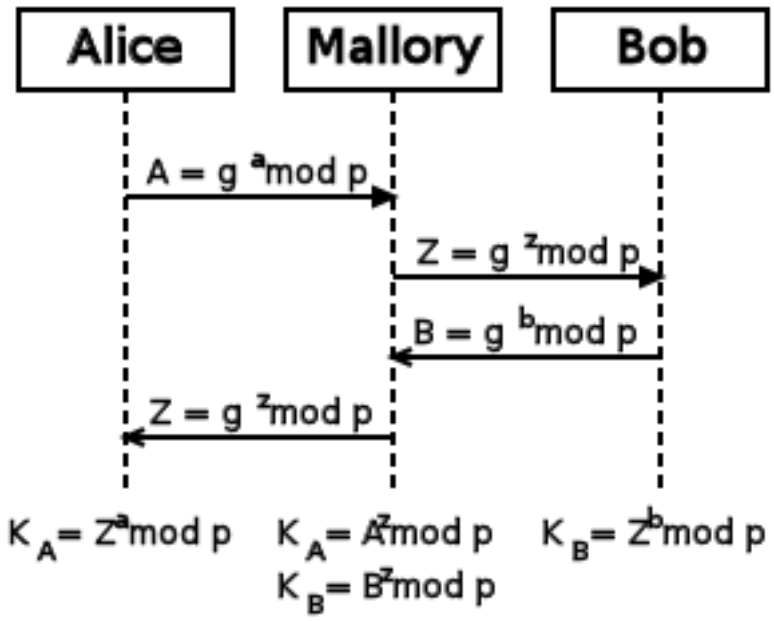

Figura 2.1: Atac de tip Man-in-the-Middle asupra protocolului Diffie-Hellman