



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 și ca metoda de distribuție a cheilor publice, poartă numele a doi specialiști de la Stanford University, Whitfield Diffie și Martin Hellman. În anul 1976, ei au inventat o metodă prin care două părți pot cădea de comun acord să comunice prin mesaje secrete fără să fie nevoie de o terță parte, de un schimb off-line sau de transmiterea vreunei valori secrete între ele.

Independent, Ralph Merkle a venit cu o soluție de distribuție a cheilor publice, numai că metoda propusă implica substanțiale cheltuieli pentru efectuarea calculelor și a transmisiei. Varianta realizată de Diffie și Hellman a fost numită sistemul distribuției 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 funcție matematică a cheilor private respective. Urmează schimbul de chei publice.

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

Diffie și Hellman folosesc exponențierea în aritmetica modulară pentru a calcula cheile publice și cheia mesajului. Aritmetica modulară este ca și aritmetica standard, cu excepția faptului că folosește numere numai în intervalul 0 la N , numit modulo. Atunci când o operație 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 și cum s-ar împărți la N și se ia în seamă restul). De exemplu, $3+4 \bmod 5 = 2$. Dacă rezultatul este negativ, N se adaugă acestuia până când se va încadra în intervalul 0 la $N-1$. De exemplu, $3-8 \bmod 7 = -5 \bmod 7 = 2$.

În aritmetica modulară, exponențierea este o funcție într-un singur sens. Aceasta înseamnă că este ușor de calculat un număr $y = gx \bmod N$ 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 și N sunt cunoscute). Aceasta este referită ca și problema logaritmului discret pentru că x este logaritm din y în baza $g \pmod{N}$, iar numerele sunt finite și întregi. Cu metoda Diffie-Hellman a schimbului de chei publice, Alice și Bob stabilesc cheia mesajului secret după cum urmează. Alice generează o cheie secretă x_a și Bob o cheie secretă x_b . După aceasta, Alice calculează o cheie publică y_a , care este g ridicat la puterea x_a 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 y_b , prin ridicarea lui g la puterea x_b modulo p . Ei vor schimba valorile publice ale acestora. Apoi, Alice ridică cheia publică a lui Bob la puterea exponentului său, x_a modulo p , în timp ce Bob ridică cheia publică a lui Alice la exponentul său, x_b modulo p . Amândoi vor obține același rezultat, g ridicat la puterea x_a și x_b , iar rezultatul obținut va fi folosit de amândoi drept cheia K a mesajului. Matematic, totul se va exprima astfel:

Deși în practică se folosesc numere foarte lungi, de câteva sute de cifre, pentru a ajuta la înțelegerea modului de funcționare, 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 $x_a = 1$ și a lui Bob $x_b = 2$ Vom avea:

- Alice calculează cheia sa publică: $y_a = g^{x_a} \pmod{p} = 3^1 \pmod{7} = 3$
- Bob calculează cheia sa publică: $y_b = g^{x_b} \pmod{p} = 3^2 \pmod{7} = 2$
- Alice calculează $K = y_b^{x_a} \pmod{p} = 2^1 \pmod{7} = 2$
- Bob calculează $K = y_a^{x_b} \pmod{p} = 3^2 \pmod{7} = 2$

sau $K = g^{x_a x_b} \pmod{p} = 3^{2 \times 1} \pmod{7} = 9 \pmod{7} = 2$.

Exemplul 2

Să presupunem că $p = 5$, $g = 4$, cheia lui Alice $x_a = 3$ și a lui Bob $x_b = 2$

- Alice calculează cheia sa publică: $y_a = g^{x_a} \pmod{p} = 4^3 \pmod{5} = 4$
- Bob calculează cheia sa publică: $y_b = g^{x_b} \pmod{p} = 4^2 \pmod{5} = 1$
- Alice calculează $K = y_b^{x_a} \pmod{p} = 1^3 \pmod{5} = 1$
- Bob calculează $K = y_a^{x_b} \pmod{p} = 4^2 \pmod{5} = 1$

sau $K = g^{x_a x_b} \pmod{p} = 4^{3 \times 2} \pmod{5} = 4096 \pmod{5} = 1$. Se observă că în ambele cazuri K ia valori identice, 2, respectiv 1.

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

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.

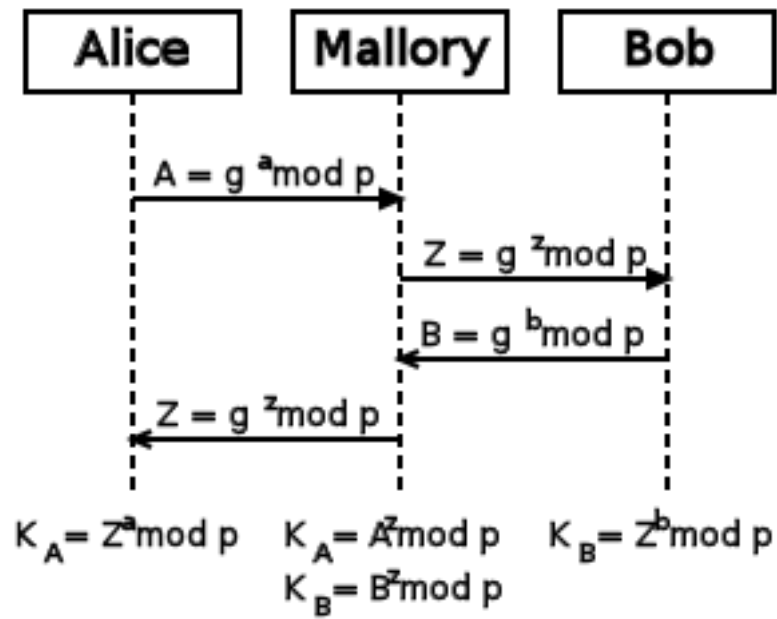


Figura 2.1: Atac de tip Man-in-the-Middle asupra protocolului Diffie-Hellman