Biztonságos kulcscsere

Hogyan egyezhet meg **Anna** és **Berci** a közös titkos kulcs használatában, ha egyáltalán nem találkozhatnak (elsősorban a nagy távolságok miatt)? Lehetséges egy ilyen megoldás nyilvános hálózatokon? Az interneten?

Diffie – Hellman kulccsere algoritmus

Anna és Berci véletlenszám generátor segítségével készít egy-egy véletlen számot (**a** és **b**), amit titokban tartanak. Korábban megegyeznek **N** és **g** egész számokban, amit mindketten ismernek, ezért a két értéket nyilvánosnak is tekinthetjük.

Anna kiszámolja a $A = g^a \mod{N}$. míg Berci kiszámolja $B = g^b \mod{N}$ értékeket felhasználva saját véletlen számaikat.

A és B eredményt visszaküldik egymásnak a kommunikációs csatornán.

Ekkor mindketten végrehajtják ugyanazt a művelet: Anna $M = B ^a \mod{N} = (g^b)^a \mod{N}$ és Berci a másik oldalon $M = A ^b \mod{N} = (g^a)^b \mod{N}$ azonos értéket kapnak, amit kulcsként használhatnak a további kommunikációjukban.

M - értéket nevezzük **mesterkulcs**-nak

From:
https://edu.iit.uni-miskolc.hu/ - **Institute of Information Science - University of Miskolc**

Permanent link:
https://edu.iit.uni-miskolc.hu/tanszek:oktatas:infrendalapjai_architekturak:informacio_titkositas_es_hitelesites:biztonsagos_kulcscsere?rev=1731519044

Last update: **2024/11/13 17:30**