

# 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 kulcscsere 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  $(A = g^a \pmod{N})$ . míg Berci kiszámolja  $(B = g^b \pmod{N})$  értékeket felhasználva saját véletlen számaikat.

A és B eredményt visszaküldik egymásnak a kommunikációs csatornán.

Ekkor mindketten végrehajtják ugyanazt a művelet: Anna  $(M = B^a \pmod{N} = g^{BA} \pmod{N})$  és Berci a másik oldalon  $(M = A^b \pmod{N} = g^{AB} \pmod{N})$  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=1731518734](https://edu.iit.uni-miskolc.hu/tanszek:oktatas:infrendalapjai_architekturak:informacio_titkositas_es_hitelesites:biztonsagos_kulcscsere?rev=1731518734)

Last update: 2024/11/13 17:25

