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

Példa

Legyen $N = 997$ és $g = 3$. Anna $a = 8$ és Berci $b = 12$ véletlen számokat választotta.

$$ A = g^a \mod{N}= 38 \mod{997} = 579. $$ $$ B = g^b \mod{N} = 312 \mod{997} = 40. $$

A és B átküldése után:

$$ M = B ^a \mod{N} = g^{BA} \mod{N} = 887 $$ $$ M = A ^b \mod{N} = g^{AB} \mod{N} = 887 $$

A közös mesterkulcs a 887 lesz. Ezt a számot használhatják kulcsként a kommunikációs algoritmusban.