Tema 5

Alice şi Bob folosesc protocolul Diffie-Hellman pentru a genera o cheie comună secretă. Ei se înţeleg asupra unui număr prim p şi a unei rădăcini primitive modulo p.

1. Presupunem că $p = 761$. Bob propune $g = 6$. Alice spune că valoarea propusă de Bob nu este rădăcină primitivă modulo 761. Cine are dreptate? Justificare.

2. Dacă $p = 23$, ştiind că $g = 5$ este rădăcină primitivă modulo 23, ajutaţi-l pe Bob să găsească celelalte rădăcini primitive modulo 23.

3. Presupunem că $p = 47$, şi $g = 5$, Oscar a reuşit să intercepteze valorile $u = 20$ şi $v = 45$. Folosind algoritmul lui Shanks, ajutaţi-l acum pe Oscar să găsească cheia comună secretă.

Calculele se pot face (de exemplu) cu https://www.dcode.fr/modular-exponentiation dar nu cu "mâna".