Výměna klíčů Diffie-Hellman (1976)

- Problém: Dvě entity (Alice a Bob) chtějí vzájemně bezpečně komunikovat přes otevřenou síť, aniž by sdílely nějaké tajemství
- Základní myšlenka spočívá ve faktu, že vypočítat g^a je rychlé, zatímco vypočítat a z g^a je mnohem těžší
- Alice najde veliké prvočíslo n, generátor g a náhodné číslo x, kde
    - prvočíslo n je 512 bitů dlouhé nebo delší
    - generátor g << n je také prvočíslo
    - pro každé $i < n$ existuje a takové, že platí $g^a = i \ mod \ n$
- Alice vygeneruje náhodné číslo x, vypočte $X = g^x \ mod \ n$
- pošle X, g, n Bobovi
- Bob vygeneruje náhodné číslo y, vypočte $Y = g^y \ mod \ n$
- Bob pošle Y Alici
- Alice vypočte $K_{AB} = Y^x \ mod \ n$
- Bob vypočte $K_{AB} = X^y \ mod \ n$
- Obě hodnoty jsou stejné
    - Bez znalosti x nebo y není možné jednoduše vypočítat K_{AB}
    - Diskrétní logaritmus $mod \ n$ je příliš složitý
- Vypočtenou hodnotu K_{AB} použijí jako tajný klíč
- Nevýhoda metody spočívá v tom, že Alice i Bob musí spolupracovat v reálném čase. Nehodí se např. pro dohodu na klíčí pro elektronickou poštu.