

5. cvičení z MIN401 – šifrování

Příklad 1: Veřejný klíč Honzy pro RSA šifru je $(91, 23)$. Zachytili jste jemu určenou zprávu 3. Dekódujte ji.

Příklad 2: [10.32, 10.33] Najděte primitivní kořeny modulo 8, 11, 20, 26, 41 a 41^2 .

Příklad 3: V ElGamalově šifrovacím systému si Alice zvolila veřejný klíč sestávající z prvočísla $p = 997$, primitivního kořene $g = 11$ a jeho mocniny g^x (kde exponent $x = 23$ je soukromý). Bob si pro komunikaci s Alicí zvolil soukromý klíč $y = 25$ a poslal jí svůj veřejný klíč g^y . Pomocí společného soukromého klíče g^{xy} pak zašifroval zprávu m a výslednou zprávu $c = 20$ poslal Alici. Jak ji bude Alice dešifrovat?

[*Řešení:* Při počítání mod 997 je $g^x \equiv 11^{23} \equiv 659$, $g^y \equiv 11^{25} \equiv 976$, $g^{xy} \equiv (g^y)^x \equiv 976^{23} \equiv 950$, inverze k němu je -297 , $m \equiv c \cdot (-297) \equiv 42$.]

Příklad 4: Martin a Honza chtějí komunikovat šifrou ElGamal. Martin si zvolil prvočísla 41 s primitivním kořenem 11 a tajný klíč 10, tj. zveřejnil $(41, 11, A)$, kde $A \equiv 11^{10} \pmod{41}$. Honza mu poslal veřejným kanálem dvojici $(22, 6)$. Jakou zprávu Honza poslal?

Příklad 5: V Rabinově šifrovacím systému s veřejným klíčem $3149 = n = p \cdot q = 47 \cdot 67$ dešifrujte zprávu $c = 158$. Uveďte všechny čtyři možnosti.

[*Řešení:* 149, 1355, 1794, 3000.]

Příklad 6: Ukažte, jak pomocí Rabinova kryptosystému s veřejným klíčem $n = 437$ zašifrovat a pak dešifrovat zprávu $M = 321$.