Zadání cvičení pro 6. týden: 26.3.-30.3.

V tomto týdnu se věnujte aplikacím elementární teorie čísel v šifrování – RSA, Diffie-Hellman, El Gamal, Rabin.

Příklad. *(10.87)*
Šifrou RSA s veřejným klíčem (7,33) byly poslány zprávy 29, 7, 21. Prolomte šifru a zprávy dešifrujte.

Poznámka. Velmi přímočaré, lze zkoušet pro jiná malá čísla dle potřeby.

Příklad. *Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.*

Poznámka. $n = pq = 667$ a např. $e = 487$ a $m = 25$ dá zprávu $c = 25^{487} \pmod{667} = 169$, soukromý klíč je $d = e^{-1} \pmod{616} = 191$. Vskutku $25 = 169^{191} \pmod{667}$.

Příklad. *Demonstrujte protokol výměny klíčů Diffie-Hellman pro zvolené prvočíslo* 61 *a primitivní kořen* 7 *s různými volbami a a b.*

Poznámka. zmiňte problém "diskrétního logaritmu".

Příklad. *(10.91)*
Martin a Honza chtějí komunikovat šifrou ElGamal navrženou egyptským matematikem Taherem Elgamalem podle protokolu Diffieho a Hellmana na výměnu klíčů. Martin si zvolil prvočíslo 41 *a jemu příslušný primitivní kořen $g = 11$ a dále si zvolil číslo* 10*. Následně zveřejnil trojici $(41, 11, A)$, kde $A \equiv 11^{10} \pmod{41}$; číslo 10 přitom utajil – je to jeho soukromý klíč. Honza mu poslal veřejným kanálem dvojici $(22, 6)$. Jakou zprávu Honza poslal?*

Příklad. *V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 23, q = 31$, veřejným klíčem je pak $n = pq = 713$. Zašifrujte pro Alici zprávu $M = 327$ a ukažte, jak bude Alice tuto zprávu dešifrovat.*