Keliška a Cecilka, informátorky
Pracovný list - RSA

- **Keliškin verejný a súkromný kľúč**
- Kelišová zvolí dve "veľké" prvočísla: $p_K = 17, q_K = 19$
  (dolný index je odvodeny od "Kelišky")
- vyrobí svoj verejný kľúč: (n_K, e_K)
  - $n_K = p_K.q_K = 17.19 = 323$
  - Pre určenie e_K musíme najskôr určiť

    $$\varphi(n_K) = \varphi(323) = \varphi(17.19) = (17-1).(19-1) = 288$$

  - Potom pre e_K platí

    $$1 < e_K < \varphi(n_K), \text{NSD}(e_K, \varphi(n_K)) = 1,$$

    napr. $e_K = 37$.
  - verejný kľúč je $(323, 37)$
- vyrobí svoj súkromný kľúč: (n_K, d_K)
  - nájdeme d_K tak, aby $e_K.d_K \equiv 1(mod\ \varphi(n_K))$
  - Ako budeme hľadať d_K? *Toto si premyslite a skúste ho určiť.*
  - d_K =????

- **Cecilkin verejný a súkromný kľúč**
- Cecilka zvolí dve prvočísla: $p_C = 7, q_C = 11$
  (dolný index je odvodeny od "Cecilky")
- vyrobí svoj verejný kľúč (princíp je taký istý ako u Kelišky):
  - $n_C = p_C.q_C = 7.11 = 77$
  - $\varphi(n_C) = \varphi(77) = \varphi(7.11) = (7-1).(11-1) = 60$
  - $1 < e_C < \varphi(n_C)$, $\text{NSD}(e_C, \varphi(n_C)) = 1$, napr. $e_C = 23$
  - verejný kľúč je $(77, 23)$
- vyrobí svoj súkromný kľúč (*ak ste zistili, ako ho vyrobila Keliška, tak teraz rovnako určíte aj Cecilkin*)
  Vyšlo Vám to takto (77,47)?
  Ak nie, tak sa musíte ešte potrápiť.

- **Komunikácia:**
  - Cecilka chce poslať správu, napr. číslo 15.
  - Použije Keliškin verejný kľúč:

$$x \equiv 15^{37} (mod\ 323)$$

$$x = 53$$

    Premyslite si efektívny spôsob určenia x.
  - zašifrovanú správu pošle Keliške a tá použije svoj súkromný kľúč

$$x \equiv 53^{d_K} (mod\ 323)$$

$$x = 15$$

Skúste odhaliť princíp tohto šifrovania a stručne ho popísať.