Cryptography, winter 2015/16

MICHAEL NÜSKEN, SIMON SCHNEIDER

10. Exercise sheet
Hand in solutions until Saturday, 23 January 2016, 12:00

Exercise 10.1 (EEA, examples). (18 points)

In each run of the algorithm, use the table to document it. Think of the cross-check. State the result.

- ○ Run the Extended Euclidean Algorithm on 42, 235. (Do NOT swap the inputs!) $\boxed{3}$
- ○ Compute the inverse of $42 \in \mathbb{Z}_{1009}$. $\boxed{3}$
- ○ Say $L = 28 \cdot 30$ and you choose $e = 26$. Is e invertible? If so determine its inverse d. $\boxed{3}$
- ○ Say $L = 28 \cdot 30$ and you choose $e = 17$. Is e invertible? If so determine its inverse d. $\boxed{3}$
- ○ Determine $x \in \mathbb{Z}_{899}$ with $x \bmod 29 = 7$ and $x \bmod 31 = 13$. $\boxed{6}$

Exercise 10.2 (RSA, example). (6 points)

Run RSA for $\kappa = 40$. Document your procedure. $\boxed{6}$