Technische Universität München (I7)
Dr. M. Luttenberger / S. Jaax

Winter term 2017/2018
2019/01/29

Solution

Cryptography – Questionnaire 5

Name: _____

Matr.: _____

Questions – 1P each = 4P

	true	false
$\mathbb{Z}_{35}^*$ is cyclic.	☐	☒
There exists a prime p such that $\lambda(2 \cdot p^k) < \varphi(2 \cdot p^k)$ for some $k > 0$.	☒	☐
Every cyclic group is commutative.	☒	☐
Let G be cyclic and $H \leq G$ be a subgroup of G. Then H is cyclic as well.	☒	☐

"One-liners" – 2P each = 6P

Exercise 5.1

- When is a prime p a "safe prime"?
- Let p be a safe prime. Compute $\varphi(p-1)$.

Answer: p is called a safe prime if $p = 2q+1$ for some (odd) prime q. Let $p = 2q+1$, then $\varphi(p-1) = \varphi(2q) = 1 \cdot \varphi(q) = q-1$.

Exercise 5.2

Compute 3^{158} in Z_{53}^*.
Answer: $3^{158} \equiv_{53} 3^2 \equiv_{53} 9$

Exercise 5.3

How many generators does $\mathbb{Z}_{47}^*$ have? (*Hint*: 47 is prime)
Answer: $\varphi(\varphi(47)) = \varphi(46) = \varphi(2) \cdot \varphi(23) = 22$