# Exercise for Exam
## *VU Network Security Advanced*

Note: It is **not allowed** to use any material (slides, notes, etc.) in the exam.

This document provides example questions as exercise for the final exam.

**A. Cryptographic Methods**

1. Extended Euclidean algorithm: For an RSA cryptosystem the sender Alice has chosen p=5, q=11 and therefore n is calculated as n=pq=55.

   a) Calculate $\varphi(n)$

   b) Alice wants to use e=7 as her public key. Show that e is co-prime to $\varphi(n)$ by calculating the greatest common divisor (gcd) using the Extended Euclidean algorithm (table form).

   c) Could Alice use e=7 as her public key if it is not co-prime to phi(n)? Explain your answer.

   d) Find the inverse d for e by using the Extended Euclidean algorithm (table form)

   $$e \cdot d \equiv 1 \; mod \; \varphi(n)$$

2. What can you do to reduce the computational effort for calculating an RSA signature?

3. What is a homomorphic encryption?

4. Describe the Elgamal Digital Signature calculation (simple form without hash).

**B. IPv6 Security**

5. Duplicate Address Detection: What can happen if a malicious node is on the local network?

6. Explain how the IPv6 privacy extension works.

7. Name the 4 building blocks used in SEND to secure the IPv6 neighbor discovery protocol.

8. Which parameters are used to calculate a Cryptographically Generated Addresses (CGA)?

9. What is the purpose of the hash2 calculation in the CGA generation?

**C. Routing Security**

10. What are the two major objectives of the IETF SIDR group for securing BGP?

11. Explain the structure of the Resource Public Key Infrastructure (RPKI).

12. How does Route Origin Authorization (ROA) work?

**D. Smart Grid Security**

13. Is it allowed that a smart meter gateway that conforms to the BSI smart meter gateway protection profile reacts to a connection attempt from an external device in the wide area network (WAN)?

14. Why do clocks on Phasor Measurement Units (PMU) need to be synchronized?

15. Why is it useful to encrypt IEEE C37.118 frames that are sent by a PMU?

**E. Hidden Communication**

16. Is the type of service (ToS) field in the IPv4 header suitable to be used as covert channel? Explain your answer.

17. Why should one not transmit plaintext in covert channels?

18. What is a subliminal channel?

19. How can the Elgamal Signature be used to transmit hidden information