Repetition

Disclaimer 1: This is an *incomplete* list. Use it to test your knowledge. In the exam, you need to *apply* your knowledge.
Disclaimer 2: Topics which are part of the lecture/exercise but are not in this list may yet appear in the exam!
If you are well-prepared for the exam, you should have no problems answering these questions. The other direction may not hold!

- Give the five technical security goals
- What's the difference: active vs. passive attacker?
- What are the three security components (Chap. Security Policies and Firewalls)?
- What's the difference: block vs. stream cipher?
- Draw all modes of encryption (we discussed) and state their important properties.
- What is authenticated encryption?
- What is Kerckhoff's principle?
- Define: cryptographic hash function
- Define: Message Authentication Code (MAC)
- Give possibilities how to construct a MAC.
  - Give the HMAC formula
  - What is essential about CBC-MAC?
- What properties should a secure channel have?
- How can replay protection be realized? How is it done in the secure channel of TLS?
- What are the mathematical principles for public key cryptography?
- Write down the DH key exchange
- How does RSA encryption/decryption work?
- Public Key Infrastructures: How is trust in keys established? What is a certificate, what is in it? How are certificates checked/created/signed? What signing power does a single CA have? Revocation? What are the problems? What was proposed to improve our PKIs and how do the solutions work?
- Why do we need randomness and how can we measure it?
- What are the goals of an authentication and key establishment protocol?
- Building blocks of key exchange protocols.
- Write down the following protocols
  - TCP 3-way handshake (basic knowledge)
  - Needham-Schroeder (symmetric and asymmetric)
  - Kerberos (define: KDC, AS, TGS)
  - IKEv2
  - TLS
- How does DOS protection with cookies work?
- What is (P)FS?
- IPSec: Architecture of IPSec (components and how they work together); SPD; SA; Transport and Tunnel Mode; ESP and AH; IPSec processing; header stacking layout
- What is a VPN? How could it be built with IPsec?
- Firewalls
  - Stateful vs. Stateless
  - Generate firewall rules for a given policy
  - Firewall architectures
- Link Layer Security
  - Compare: PAP, CHAP, EAP, and 802.1x
  - AAA architecture (entities and protocol layering)
- Attacks and Attack Detection: Types; Knowledge-based vs. Anomaly Detection; False Positive, False Negative, True Positive, True Negative
- Web Security: JS and same origin, SQL Injection, CSS, CSRF, . . . , counter measures, HTTPS