Kryptographie **Stoffumfang**

1. Du kannst die Hauptaufgaben der Kryptographie aufzählen.
2. Du kannst die Situation, in der die (klassische) Kryptographie stattfindet, mit den entsprechenden Fachbegriffen (Geheimtext, Klartext, Verschlüsselungsfunktion $c = E_k(m)$, Entschlüsselungsfunktion $m = D_k(c)$) graphisch oder sprachlich beschreiben.
3. Du kannst das Prinzip von Kerckhoffs beschreiben.
4. Du kannst beschreiben, worum es bei der Kryptoanalyse und bei den einzelnen Angriffszenarien geht.
5. Du kannst eine Antwort auf die Frage geben, was symmetrische Verschlüsselungsverfahren sind.
6. Du kannst die folgenden symmetrischen Verschlüsselungsverfahren an einfachen Beispielen durchführen und ihre Vor- und Nachteile aufzählen.
   - Cäsar-Chiffre
   - Monalphabetische Verschlüsselung
   - Verschlüsselung nach DE VIGENÈRE
   - One Time Pad
7. Du kannst die Funktionsweise von Stromchiffren beschreiben und ihre Vor- und Nachteile nennen.
8. Du kannst den Output eines lineare Schieberegisters (maximal 4 Zellen) berechnen.
9. Du kannst die Funktionsweise von Blockchiffren beschreiben und kannst die (*Code Book Mode* und *Cipher Block Chaining Mode*)
10. Du kannst die Multiplikatonstabelle der primen Restklassengruppen $\mathbb{Z}_n^*$ für kleine $n \in \mathbb{N}$ tabellarisch darstellen und rechnerisch interpretieren:
    - Multiplikationen durchführen
    - zu $a \in \mathbb{Z}_n^*$ das inverse Element a^{-1} finden
11. Du kannst untersuchen, ob ein Element $a \in \mathbb{Z}_n^*$ erzeugend, d.h. eine Primitivwurzel modulo n ist.
12. Du kannst angeben, wie viele Primitivwurzeln es in $\mathbb{Z}_p^*$ gibt, wenn p eine Primzahl ist.
13. Du kannst die Werte der Eulerschen φ-Funktion $\varphi(n)$ für grössere n mit Hilfe der Rechenregeln bestimmen.
14. Du kannst den Square-and-Multiply-Algorithmus (mit Hilfe von Multiplikationstabellen) anwenden.

15. Du kannst die Anzahl der Schlüssel berechnen, die bei einem symmetrischen Verschlüsselungsverfahren und n Kommunikationspartnern nötig sind.

16. Du kannst die Funktionsweise und den Vorteil des Diffie-Hellman-Merkle-Schlüsselaustauschs (DHMS) beschreiben und (ohne Details) erklären, worauf seine Sicherheit beruht.

17. Du kannst einen DHMS für konkret gegebene Werte für g, a und b durchrechnen. Dazu wird der Square-and-Multiply-Algorithms vorausgesetzt.

18. Du kannst das Szenario des Man-in-the-Middle-Angriff beschreiben.

19. Du kannst den Satz von Euler-Fermat (mit der Voraussetzung) formulieren.

20. Du kannst die Funktionsweise des RSA-Verfahrens und seine zentralen Eigenschaften beschreiben (Public-Key-Eigenschaft, Entschlüsselungseigenschaft, Signatureigenschaft) beschreiben.

21. Du kannst beschreiben, auf welchem Prinzip die Sicherheit des RSA-Verfahrens beruht.

22. Du kannst erklären, wie sich mit Hilfe des RSA-Verfahrens, die Authentizität einer Nachricht m überprüfen lässt.

23. Du kannst für vorgegebene (kleine) Primzahlen p, q und einem vorgegebenen öffentlichen Schlüssel e den privaten Schlüssel d mit Hilfe des erweiterten euklidschen Algorithmus berechnen.

24. Du kannst eine Klartextnachricht m (aus einem Zeichen) mit Hilfe des öffentlichen Schlüssels d verschlüsseln bzw. eine Geheimtextnachricht c mit Hilfe des privaten Schlüssels e entschlüsseln. Auch hier wird die Verwendung des Square-and-Multiply-Algorithmus vorausgesetzt.