Kryptographie (Teil 2) **Stoffumfang**

1. 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
2. Du kannst untersuchen, ob ein Element $a \in \mathbb{Z}_n^*$ erzeugend, d.h. eine Primitivwurzel modulo n ist.
3. Du kannst angeben, wie viele Primitivwurzeln es in $\mathbb{Z}_p^*$ gibt, wenn p eine Primzahl ist.
4. Du kannst die Werte der Eulerschen φ-Funktion $\varphi(n)$ für grössere n mit Hilfe der Rechenregeln bestimmen.
5. Du kannst den Square-and-Multiply-Algorithmus (mit Hilfe von Multiplikationstabellen) anwenden.
6. Du kannst die Anzahl der Schlüssel berechnen, die bei einem symmetrischen Verschlüsselungsverfahren und n Kommunikationspartnern nötig sind.
7. Du kannst die Funktionsweise und den Vorteil des Diffie-Hellman-Merkle-Schlüsselaustauschs (DHMS) beschreiben und (ohne Details) erklären, worauf seine Sicherheit beruht.
8. Du kannst einen DHMS für konkret gegebene Werte für g, a und b durchrechnen. Dazu wird der Square-and-Multiply-Algorithms vorausgesetzt.
9. Du kannst das Szenario des Man-in-the-Middle-Angriff beschreiben.
10. Du kannst den Satz von Euler-Fermat (mit der Voraussetzung) formulieren.
11. Du kannst die Funktionsweise des RSA-Verfahrens und seine zentralen Eigenschaften beschreiben (Public-Key-Eigenschaft, Entschlüsselungseigenschaft, Signatureigenschaft) beschreiben.
12. Du kannst beschreiben, auf welchem Prinzip die Sicherheit des RSA-Verfahrens beruht.
13. Du kannst erklären, wie sich mit Hilfe des RSA-Verfahrens, die Authentizität einer Nachricht m überprüfen lässt.
14. 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.
15. 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.