1. (2 Punkte) Verschlüssele den Klartext *Morgenstunde* mit der Cäsar-Chiffre und Schlüssel 4.

2. (3 Punkte) a. Verschlüssele nach dem Vigenere-Verfahren: Klartext = 'WAHLURNE', key = 'ABI'
   b. Erkläre, wie man einen mit der Vigenere-Chiffre verschlüsselten Text bei bekannter Schlüssellänge vollständig entschlüsseln kann.

3. (3 Punkte) Erläutere den Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung.

4. (2 Punkte) Du willst zur Sicherheit die Daten deiner Festplatte verschlüsseln. Gib an, ob du ein symmetrisches oder asymmetrisches Verschlüsselungsverfahren wählen würdest. Begründe deine Wahl.

5. (3 Punkte) Ein Verein möchte Nachrichten nur noch mit asymmetrischer Verschlüsselung per email empfangen. Deshalb soll der Webmaster, der Zugriff auf den Mailserver hat, den öffentlichen Schlüssel auf der Homepage des Vereins veröffentlichen. Erläutere, wie der Webmaster mit Hilfe eines sogenannten *Man-in-the-Middle-Angriffs* die Nachrichten manipulieren kann.

6. (4 Punkte) Jemand macht folgenden Verbesserungsvorschlag für das Vigenere-Verfahren. Der Klartext wird erst mit dem Schlüssel *GEHEIM* verschlüsselt, der verschlüsselte Text dann nochmal mit dem Schlüssel *ABI* verschlüsselt. Erhöht dieser Vorschlag die Sicherheit des Verfahrens? Begründe deine Antwort.

7. (4 Punkte) Für den Diffie-Hellman Schlüsselaustausch vereinbaren Alice und Bob die Primzahl p und die Primitivwurzel g. Alice wählt als geheime Zahl a, Bob wählt als geheime Zahl b. Die Werte sind: p = 11, g = 7, a = 3, b = 5.
a. Welche Zahlen sind öffentlich und wie werden diese berechnet?
b. Wie heißt der gemeinsame Schlüssel und wie wird er berechnet?

8. (4 Punkte) Für das RSA-Verfahren wählt Bob p und q als Primzahlen und den Verschlüsselungsexponent e.
Die Werte sind: p = 7, q = 13, e = 11.
Warum ist e ein zulässiger Verschlüsselungsexponent?
Wie heißen der öffentliche, wie der private Schlüssel von Bob? Wie werden diese Werte berechnet?

9. (4 Punkte) Bob hat den öffentlichen RSA-Schlüssel (143,23). Alice will Bob die Nachricht 56 schicken. Wie wird die verschlüsselte Nachricht berechnet?