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

Lösung:
QSVKIRWXYRHI

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.

Lösung:
a. WBPLVZNF
b. Nachdem die Schlüssellänge n bekannt ist, müssen nur noch n Cäsar-Verschlüsselungen analysiert werden. Diese können mit einer Häufigkeitsanalyse oder mit der Brut-Force-Methode entschlüsselt werden, da es nur 26 Möglichkeiten der Verschlüsselung gibt.

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

Lösung:
Bei der symmetrischen Verschlüsselung wird für das Ver- und Entschlüsseln nur ein Schlüssel verwendet. Der Schlüssel muss entweder persönlich oder mit Hilfe eines abhörsicheren Kanals vom Sender zum Empfänger übertragen werden. Bei der asymmetrischen Verschlüsselung gibt es zwei Schlüssel, einen privaten und einen öffentlichen Schlüssel, der letztere ist allen möglichen Kommunikationspartnern bekannt. Der private Schlüssel wird nie veröffentlicht, der öffentliche Schlüssel kann über alle zur Verfügung stehenden Publikationsmöglichkeiten veröffentlicht werden (E-Mail, WWW-Seiten, Public-Key-Server, ...). Um die Echtheit eines öffentlichen Schlüssels zu überprüfen, muss es ein Verfahren zur Herstellung von Schlüsselvertrauen geben. Das kann eine (zentrale) Zertifizierungsstelle sein oder ein dezentraler Web-of-Trust-Ansatz.

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.

Lösung: Bei der Verschlüsselung einer Festplatte ist es wichtig, dass die verschlüsselten Daten schnell ausgelesen werden können, um die Arbeitsgeschwindigkeit nicht zu beeinträchtigen. Der Schlüsselaustausch ist nicht relevant, da sowohl der Empfänger als auch der Sender ein und dieselbe Person sind. Deshalb ist ein symmetrisches Verfahren vorzuziehen.

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.

Lösung: Der Webmaster veröffentlicht seinen eigenen öffentlichen Schlüssel an Stelle des öffentlichen Schlüssels des Vereins auf deren Homepage. Wenn ein Kunde mit Hilfe dieses Schlüssels eine Nachricht an den Verein schickt, fängt der Webmaster die Mail auf dem Mailserver ab, entschlüsselt sie mit Hilfe seines privaten Schlüssels, manipuliert die Nachricht und schickt sie dann mit Hilfe des öffentlichen Schlüssels des Vereins an den Verein weiter.

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.

Lösung:

Der erste Schlüssel *GEHEIM* ist 6 Buchstaben lang und damit ein Vielfaches der Länge des zweiten Schlüsselworts (3). Weil das zweite Schlüsselwort genau in das erste passt, ist es so, als hätte man nur mit einem einzelnen Schlüsselwort der Länge 6 *GFPEJU* verschlüsselt. Da die Sicherheit in erster Linie von der Schlüssellänge abhängt, gewinnt man damit nichts. Anders sähe es aus, wenn die Längen der Schlüssel teilerfremd wären, also z.B. ein Schlüsselwort der Länge 3 und eines der Länge 7. Dadurch entstünde ein neuer Schlüssel der Länge 21.

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?

Lösung: Öffentlich: A=2, B=10, p=11, g=7, Gemeinsamer Schlüssel: K=10
Berechnung: A = 7^3 in $\mathbb{Z}_{11}$, B = 7^5 in $\mathbb{Z}_{11}$ K = $2^5 = 10^3$ in $\mathbb{Z}_{11}$

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?

Lösung:

p=7,q=13,e=11
m=p∗q=91
$\tilde{m} = (p-1)*(q-1) = 72$
e zulässig, da ggT(11,72) = 1
d = 1/e = 59 **in** $\mathbb{Z}_{72}$
oeffentlicher Schlüssel: (91,11)
privater Schlüssel: (91,59)
Berechnung von d mit dem erweiterten Euklidschen Algorithmus:

a	b	q	r	x	y
72	11	6	6	2	−13
11	6	1	5	−1	2
6	5	1	1	1	−1
5	1	5	0	0	1

$d = y = -13 = 59$ **in** $\mathbb{Z}_{72}$

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

Lösung:

Alice muss $56^{23} \bmod 143$ berechnen.
Berechnung mit dem Powermod–Verfahren:
Binärdarstellung von 23 = 10111
Potenzen von 56 werden für Potenzen von 2 berechnet:
In $\mathbb{Z}_{143}$:
$56^1 = 56$
$56^2 = -10$
$56^4 = -43$
$56^8 = -10$
$56^{16} = -43$

$56 * -10 * -43 * -43 = 23$ **in** $\mathbb{Z}_{143}$, 23 ist die verschlüsselte Nachricht.