Aufgabe 1 (7 Punkte)
Bewerten Sie die Richtigkeit der folgenden Aussagen. Für jede richtige Antwort erhalten Sie einen Punkt. Fehlende oder falsche Antworten geben keinen Abzug.

Aussage	**wahr**	**falsch**
43 ist eine sichere Primzahl.	◯	◯
Man muss den Miller-Rabin-Primzahltest nur fünfmal erfolgreich durchführen, um sicherzustellen, dass die Fehlerwahrscheinlichkeit unter ein Promille liegt.	◯	◯
Es wurde bewiesen, dass es Einwegfunktionen gibt.	◯	◯
Wenn der Entschlüsselungsexponenten d im RSA-Kryptosystem zu klein gewählt wird, kann das System gebrochen werden.	◯	◯
Die Sicherheit des Diffie-Hellman-Schlüsselaustausches beruht darauf, dass es zurzeit keine effizienten Verfahren zur Faktorisierung großer ganzer Zahlen gibt.	◯	◯
Wenn man eine Nachricht m mit dem RSA-Kryptosystem verschlüsselt, so ist die resultierende Chiffre kürzer als diejenige, die man mit dem ElGamal-Verfahren (ebenfalls angewandt auf m) erhält.	◯	◯
Sei $n = 5911 = 23 \cdot 257$. Pollards $(p-1)$-Algorithmus wird den Primfaktor 23 zuerst finden.	◯	◯

Aufgabe 2 (4 Punkte)
Gegeben sei eine affine Chiffrierung durch $E(x) = c = 25x + 4 \mod 26$. Finden Sie die affine Dechiffrierfunktion $D(c) = x = ac + b \mod 26$, wobei $a, b \in \{0, ..., 25\}$ gilt (mit Begründung).

Aufgabe 3 (2+3 Punkte)

(a) Bestimmen Sie eine erwartungstreue Schätzung des Koinzidenzindexes von

`ABRAKADABRA`

(b) Welchem Angriff will man mit einer homophonen Chiffrierung entgehen? Beschreiben Sie das Prinzip einer homophonen Chiffrierung.

Aufgabe 4 (2+1+4+1+1 Punkte)
In dieser Aufgabe soll das RSA-System mit sehr kleinen Zahlen durchgerechnet werden. Sei $n = 39$. Es soll also modulo n ver- und entschlüsselt werden.

(a) Berechnen Sie $\varphi(n)$.

(b) Geben Sie die zwei kleinstmöglichen, erlaubten Verschlüsselungsexponenten e mit $e > 1$ an (mit Begründung).

(c) Angenommen, der Verschlüsselungsexponent ist $e = 17$. Mit welchem Algorithmus wird der dazugehörige Entschlüsselungsexponent d berechnet? Berechnen Sie d mit dem Algorithmus.

(d) Wenn dieses RSA-System für eine digitale Signatur benutzt wird, wie erfolgt die Unterschrift für ein Dokument m?

(e) Wie kann man mithilfe des öffentlichen Schlüssels (geben Sie diesen an) die Unterschrift verifizieren?

Aufgabe 5 (1+3 Punkte)

(a) Geben Sie die Binärdarstellung von 25 an.

(b) Berechnen Sie $3^{25} \mod 19$ mittels modularer Exponentiation.

Aufgabe 6 (1+5+2+2+1+2 Punkte)

(a) In welchen Krypto-Verfahren benötigt man Primitivwurzeln?

(b) Zeigen Sie mit dem Primitivwurzel-Kriterium, dass 2 eine Primitivwurzel modulo 11 ist. Begründen Sie, dass das Primitivwurzel-Kriterium hier anwendbar ist.

(c) Wie viele Primitivwurzeln (Erzeuger) hat $\mathbb{Z}_{11}^*$?

(d) Welche Ordnung kann ein Element $a \in \mathbb{Z}_{11}^*$ haben?

(e) Bestimmen Sie den diskreten Logarithmus von 5 (zur Basis 2, modulo 11).

(f) Gilt $2^{115} \equiv 2^{525} \pmod{11}$?
Hinweis: Sie können dieses ausrechnen oder mit einem zahlentheoretischen Argument begründen.

Aufgabe 7 (2+8 Punkte)

(a) Wie viele Quadratwurzeln der 1 gibt es in $\mathbb{Z}_{15}^*$? Geben Sie diese an.

(b) Im Folgenden soll mittels des Rabin-Verfahrens ver- und entschlüsselt werden. Beschreiben Sie das Verfahren, indem Sie die folgenden Fragen beantworten.

(i) Wie wird der öffentliche Schlüssel n gewählt?

(ii) Woraus besteht der geheime Schlüssel?

(iii) Wie verschlüsselt Alice eine Nachricht m?

(iv) Wie entschlüsselt Bob den Geheimtext c?

Aufgabe 8 (4 Punkte)
Wenden Sie den Fermatschen Faktorisierungsalgorithmus auf die Zahl $n = 1763$ an. Welche Faktoren findet der Algorithmus? Geben Sie den Rechenweg an.

Hinweis: Es gilt $\lceil \sqrt{1763} \rceil = 42$.

Aufgabe 9 (4 Punkte)
Man betrachte die folgende Vereinfachung des Shamirschen No-Key-Protokolls. Das Ziel des Protokolls ist es, eine Nachricht $m \in \mathbb{Z}_n^*$ von Alice an Bob zu senden, wobei n eine natürliche Zahl ist und als bekannt vorausgesetzt wird.

(i) Alice wählt $a_1 \in \mathbb{Z}_n^*$ zufällig. Sie berechnet $c_1 \coloneqq m \cdot a_1 \mod n$ und sendet c_1 an Bob.

(ii) Bob wählt $a_2 \in \mathbb{Z}_n^*$ zufällig. Er berechnet $c_2 \coloneqq c_1 \cdot a_2 \mod n$ und sendet c_2 an Alice.

(iii) Sei b_1 das multiplikativ inverse Element zu a_1 modulo n. Alice berechnet $c_3 \coloneqq c_2 \cdot b_1 \mod n$ und sendet c_3 an Bob.

(iv) Sei b_2 das multiplikativ inverse Element zu a_2 modulo n. Bob berechnet nun $m = c_3 \cdot b_2 \mod n$

Beschreiben Sie, wie ein Angreifer, der n kennt und die Chiffren c_1, c_2 und c_3 abfangen konnte, die Verschlüsselung brechen kann.