**Aufgabe 1.** (20 Punkte)
Betrachten Sie die One-Time-Pad (OTP) Verschlüsselung, bei der zu einem Klartext ein zufälliger Schlüssel gleicher Länge addiert wird. Das Ergebnis ist ein gleichverteilter Chiffretext. Für eine Nachricht der Länge $n$ und ein Alphabet der Kardinalität $m$ ergibt sich

$$e(m_1, \ldots, m_n) = c_1, \ldots, c_n \text{ mit } c_i \equiv m_i + k_i (\text{mod } m)$$

und

$$d(c_1, \ldots, c_n) = m_1, \ldots, m_n \text{ mit } m_i \equiv c_i - k_i (\text{mod } m).$$

(a) Eine der folgenden Nachrichten wurde mit einer einfachen Substitutions-Chiffrierung verschlüsselt und die andere mit OTP. Ordnen Sie mit Hilfe des Koinzidenzindex die Nachrichten der Verschlüsselung zu und erklären Sie Ihre Antwort. Das römische Alphabet der Länge 26 und englische Sprache wird betrachtet.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $s_1 =$ | rczbw | bfhsl | pscpi | lhbgz | jtgbi | bjgly | ijibf | hcqqf | zbyfp |
| $s_2 =$ | khqwg | izmgk | poyrk | huitd | uxlxc | wzotw | pahfo | hmgfe | vuejj |

Im Folgenden wird ein binäres Alphabet ($m = 2$) betrachtet. OTP ist gleich

$$c_i = m_i \oplus k_i \text{ and } m_i = c_i \oplus k_i$$

wobei $\oplus$ der binäre XOR-Operator ist. $\{0,1\}^n$ ist die Menge der binären Zeichenfolgen der Länge $n$. Bekanntlich ist OTP-Verschlüsselung perfekt sicher, wenn $\mathcal{M} = \mathcal{K} = \{0,1\}^n$ und der Schlüssel $k = k_1, \ldots, k_n$ gemäß einer Gleichverteilung gewählt wird. Nun werden Varianten des OTP mit Einschränkungen auf dem Klartext und dem Schlüssel betrachtet. $S = \{00, 01, 10\}$ bezeichne eine Menge mit drei 2-bit Zeichenfolgen.
Beachten Sie die folgenden drei OTP Varianten, wobei die Schlüssel zufällig gleichverteilt gewählt werden:

1. Gegeben sei $\mathcal{M} = S^n$ und $\mathcal{K} = \{0,1\}^{2n}$. Der Klartext und die Schlüssel sind $2n$-bit lange Zeichenfolgen, aber nicht jede $2n$-bit Zeichenfolge ist eine gültige Nachricht (z.B. für $n = 3$, $m = 000100$ ist gültig, aber $m = 110011$ ist ungültig weil $11 \notin S$).
2. Gegeben sei $\mathcal{M} = \{0,1\}^{2n}$ und $\mathcal{K} = S^n$.
3. Gegeben sei $\mathcal{M} = \mathcal{K} = S^n$.

Beantworten Sie die folgenden Fragen für die einzelnen OTP Varianten:

(b) Wie groß sind der Nachrichtenraum $\mathcal{M}$ und der Schlüsselraum $\mathcal{K}$?

(c) Was ist die Menge $\mathcal{C}$ der Chiffretexte?

(d) Ist die Chiffrierung perfekt sicher? Erklären Sie Ihre Antwort.

(e) Hängt perfekte Sicherheit mit der Grösse des Schlüsselraums und des Nachrichtenraums zusammen? Begründen Sie Ihre Antwort.

**Aufgabe 2.** (20 Punkte)
Alice und Bob wollen die Zahl $p = 1373$ und das primitive Element $a = 2$ für einen Diffie-Hellman Schlüsselaustauch nutzen.

(a) Es soll geprüft werden, ob $p$ eine Primzahl ist. Nutzen Sie den Miller-Rabin Test um zu zeigen, dass 2 kein starker Zeuge für die Zusammengesetztheit von $p$ ist.

(b) Welche Bedingungen muss $a$ für den Diffie-Hellman Schlüsselaustausch erfüllen? Prüfen Sie, ob $a$ diese Bedingung erfüllt (Tipp: $2^{196} \equiv 333 \pmod{1373}$).

Alice sendet $u = 974$ zu Bob.

(c) Gegeben sei Bobs Geheimnis 871. Berechnen Sie den gemeinsamen Schlüssel.

Der Diffie-Hellman Schlüsselaustausch basiert auf dem Diffie-Hellman Problem. Eine Variante von diesem Problem ist das Diffie-Hellman Entscheidungsproblem. Mit den drei Zahlen $u$, $v$ und $w$ ist es wie folgt definiert:

$$\text{Entscheide für } u \equiv a^x \pmod{p} \text{ und } v \equiv a^y \pmod{p} \text{ ob}$$

$$w \equiv a^{xy} \pmod{p}.$$

(d) Zeigen Sie, dass ein Algorithmus, der das Diffie-Hellman Problem löst, genutzt werden kann, um das Diffie-Hellman Entscheidungsproblem zu lösen.

**Aufgabe 3.** (20 Punkte)
Alice nutzt den RSA Algorithmus und verschlüsselt eine Nachricht $m$ mit dem öffentlichen Schlüssel von Bob $(n, e) = (91, 59)$.

(a) Finden Sie den Klartext zu dem Chiffretext $c = 23$.

Nehmen Sie an, dass Alice eine Nachricht $x$ zu drei unterschiedlichen Leuten Bob, Bart und Barney senden will. Alle nutzen denselben öffentlichen Exponenten $e = 3$ und die öffentlichen Moduln $n_1$, $n_2$ und $n_3$. Alice sendet $c_i \equiv x^3 (\text{mod } n_i)$ zum Empfänger $i$.

(b) Nehmen Sie zunächst an, dass mindestens zwei öffentliche Moduln $n_i$ **nicht** relativ prim sind (zum Beispiel $\gcd(n_1, n_2) \neq 1$). Wie kann man $x$ finden, wenn alle $c_i$ gegeben sind?

(c) Nun seien $n_1 = 46$, $n_2 = 51$, $n_3 = 77$ und $c_1 = 31$, $c_2 = 19$, $c_3 = 71$. Es ergibt sich:

$$\begin{aligned} 31 &\equiv x^3 (\text{mod } 46) \\ 19 &\equiv x^3 (\text{mod } 51) \\ 71 &\equiv x^3 (\text{mod } 77) \end{aligned}$$

Berechnen Sie $x$ bei gegebenen $c_i$ (und bekannten öffentlichen Schlüsseln), ohne die $n_i$ zu faktorisieren.

(d) Oskar kann nur die ersten beiden Kryptogramme abfangen. Kann Oskar aus den beiden Kongruenzen

$$\begin{aligned} 31 &\equiv x^3 (\text{mod } 46) \\ 19 &\equiv x^3 (\text{mod } 51) \end{aligned}$$

das Kryptogramm entschlüsseln (ohne die $n_i$ zu faktorisieren)?