Kryptologie
Übungsblatt 1

Aufgabe 1.1

(a) Bei einer affinen Chiffrierung haben Sie herausgefunden, dass `M` auf `P` und `B` auf `K` abgebildet wird. Bestimmen Sie den Schlüssel $k = (a, b)$.

(b) Jemand kommt auf die Idee, die affine Verschlüsselung durch doppelte Verschlüsselung zu verbessern. Nachdem also eine Nachricht m mit geeignetem Schlüssel $k_1 = (a_1, b_1)$ zu $c_1 = (a_1 m + b_1) \mod 26$ verschlüsselt wurde, wird mit einem weiteren Schlüssel $k_2 = (a_2, b_2)$ zu $c_2 = (a_2 c_1 + b_2) \mod 26$ verschlüsselt.
Was halten Sie davon?

Aufgabe 1.2

Verschlüsseln Sie den Klartext `SAMSTAGNACHMITTAGDIESTADTANGREIFEN` mit dem Schlüssel `KRYPTO`.

(a) mit Hilfe der Playfair-Chiffre.

(b) mit Hilfe der Vigenère-Chiffre.

Aufgabe 1.3

Die Verschlüsselung bei der ENIGMA-Maschine geschieht mit Hilfe von Walzen (runde Scheiben), auf denen auf Vorder- und Rückseite kreisförmig 26 Metallstifte angeordnet sind (die die Buchstaben repräsentieren). Im Inneren der Walze sind die Stifte auf der Vorderseite gemäß einer festen Permutation aus S_{26} mit den Stiften auf der Rückseite elektrisch verbunden. Allerdings darf die in einer solchen Walze verdrahtete Permutation keinen Fixpunkt enthalten.
Eine Permutation $\pi \in S_n$ heißt *fixpunktfrei*, falls $\pi(i) \neq i$ für alle $i \in \{1, ..., n\}$ gilt. Für $n \in \mathbb{N}$ bezeichne d_n als die Anzahl der fixpunktfreien Permutationen in S_n.

(a) Bestimmen Sie d_1 und d_2.

(b) Zeigen Sie für $n \geq 3$ die Rekursionsformel $d_n = (n-1) \cdot (d_{n-1} + d_{n-2})$.

Aufgabe 1.4

Betrachten Sie das Wort `ERDBEERE`.

(a) Geben Sie die relativen Häufigkeiten der Buchstaben in `ERDBEERE` an.

(b) Berechnen Sie für `ERDBEERE` den erwartungstreuen Schätzwert des Koinzidenzindex.

(c) Hat `ERDBEEREERDBEERE` den gleichen erwartungstreuen geschätzten Koinzidenzindex?

Aufgabe 1.5

(a) Ein Kryptoanalytiker versucht, eine Vigenère-verschlüsselte Chiffre zu knacken. Ihm fallen die Buchstabenwiederholungen `XSD` mit Abstand 12 und `AWER` mit Abstand 18 auf.
Welche Vermutung über die verwendete Schlüsselwortlänge stellt er auf?

(b) Wir haben es mit einer Sprache zu tun, in der es nur die 3 Buchstaben A, B, C gibt, welche mit den Wahrscheinlichkeiten 0.7, 0.2 und 0.1 auftreten. Das Folgende ist ein Vigenère-verschlüsselter Text in dieser Sprache (wobei nun modulo 3 statt modulo 26 gerechnet wird):

`ABCBABBBAC`

Wir wissen, dass die verwendete Schlüssellänge 1, 2 oder 3 ist. Zeigen Sie, dass die Schlüssellänge höchstwahrscheinlich 2 ist und bestimmen Sie den plausibelsten Schlüssel und Klartext.

Aufgabe 1.6

Man erzeuge Pseudozufallszahlen mit dem Blum-Blum-Shub-Generator

$$z_{i+1} = (z_i)^2 \mod n,$$

wobei $n = 11 \cdot 23$ und $z_0 = 2$.

(a) Wie lang ist die Periode, die sich ergibt?

(b) Wie in der Vorlesung wird der Schlüssel k aus den letzten Bits der erzeugten Pseudozufallszahlen gebildet. Verschlüsseln Sie die Nachricht $m = (m_1, ..., m_8) = 10110101$ durch XOR-Verknüpfung mit k.