

7. März 2026

3. Übungsblatt Mathematik und Information

Aufgabe 1:

Die deutsche Wehrmacht verwendete in der Zeit bis zum ersten Weltkrieg Chiffren, die sogenannte Permutationschiffren enthalten. Bei einer Permutationschiffre wird die Nachricht in Blöcke einer festen Länge r zerlegt, wobei r typischerweise etwa zwischen zwanzig und dreißig liegt. Auf jeden dieser Blöcke wird dann eine Permutation aus der symmetrischen Gruppe $\mathfrak{S}_r$ angewendet.

- Welche Entropie hat der Schlüssel eines solchen Verfahrens?
- Welche Informationen kann ein Kryptanalytiker aus der Häufigkeitsverteilung der Buchstaben im Chiffretext ziehen?
- Wie kann er vorgehen, um bei bekanntem r schneller als durch Ausprobieren aller Permutationen den Klartext zu einem Kryptogramm zu finden?
- Welche Möglichkeiten hat er, um die Blocklänge r zu bestimmen?

Aufgabe 2:

Bei einer allgemeinen monoalphabetischen Substitution wird ein Text verschlüsselt, indem die Buchstaben des Alphabets untereinander permutiert werden.

- Welche Entropie hat der Schlüssel eines solchen Verfahrens?
- Wie kann ein Kryptanalytiker erkennen, daß ein solches Verfahren angewandt wurde?

Aufgabe 3:

Im zweiten Weltkrieg verwendete die deutsche Wehrmacht sogenannte Rotormaschinen zur Verschlüsselung. Ein Rotor war ein Zylinder mit je 26 Kontakten auf beiden Seitenflächen, der eine feste Permutation aus $\mathfrak{S}_{26}$ realisierte. Auf dem Zylindermantel saß ein Ring, der mit den Buchstaben des Alphabets beschriftet war und gegenüber dem Zylinder gedreht werden konnte, so daß frei festgelegt werden konnte, welcher der 26 Kontakte dem Buchstaben A entsprach. Für eine spezielle solche Enigma-Maschine gab es fünf verschiedene Rotoren, von denen jeweils drei in einer beliebig wählbaren Reihenfolge eingesetzt werden konnten. Da sich nach der Verschlüsselung eines Buchstabens stets mindestens ein Rotor weiterbewegte, hing die Verschlüsselung schließlich auch noch ab von den Anfangsstellungen der drei Rotoren. Wie groß war die Schlüsselentropie?

Aufgabe 4:

Das Alphabet $A = \{a, b\}$ enthalte zwei Elemente, und $X_1, X_2, \dots$ sei eine Folge von unabhängigen Zufallsvariablen, die a mit Wahrscheinlichkeit $2/3$ und b mit Wahrscheinlichkeit $1/3$ annehmen. Bestimmen Sie für $\eta = \frac{1}{2}$ und $\eta = \frac{1}{4}$, wieviel Prozent der Elemente $W \in A^{10}$ die Bedingung $\left| \frac{-\log_2 p(W)}{10} - H \right| < \eta$ erfüllen!

Abgabe bis zum Mittwoch, dem 10. März 2026, um 15.30 Uhr