Wolfgang K. Seiler
Tel. 2515

A5, C201

11. April 2016

5. Übungsblatt Mathematik und Information

Aufgabe 1: *(10 Punkte)*

a) Die Buchstaben des Alphabets haben in Jean Pauls Roman *Dr. Katzenbeisers Badereise* sind auf dem vorigen Übungsblatt zu finden. Welche Entropie pro Buchstabe hat ein aus diesen Buchstaben zusammengesetzter Text, wenn man nur von den Buchstabenhäufigkeiten ausgeht?

b) Um wie viele Bit pro Buchstabe unterscheidet sich das von der Entropie einer Quelle, bei der alle 26 Buchstaben gleichwahrscheinlich sind?

c) Der Zwischenraum hat in deutschen Texten eine Häufigkeit von etwa 18%. Was ändert sich bei *a)* und *b)*, wenn man von einem Alphabet ausgeht, das auch noch diesen enthält?

d) Wäre die Arbeit eines Kryptanalytikers einfacher oder schwerer, wenn man von einem Alphabet mit Groß- und Kleinbuchstaben sowie Satzzeichen ausginge?

Aufgabe 2: *(3 Punkte)*

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, und auf jeden dieser Blöcke wird eine Permutation aus der symmetrischen Gruppe $\mathfrak{S}_r$ angewendet.

a) Welche Entropie hat der Schlüssel eines solchen Verfahrens?

b) Welche Informationen kann ein Kryptanalytiker aus der Häufigkeitsverteilung der Buchstaben im Chiffretext ziehen?

Aufgabe 3: *(3 Punkte)*

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

a) Welche Entropie hat der Schlüssel eines solchen Verfahrens?

b) Wie kann ein Kryptanalytiker erkennen, daß ein solches Verfahren angewandt wurde?

Aufgabe 4: *(4 Punkte)*

Im zweiten Weltkrieg verwendete die deutsche Wehrmacht sogenannte Rotormaschinen zur Verschlüsselung, Ein Rotor war eine 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?

Abgabe bis zum Freitag, dem 15. April 2016, um 11.55 Uhr