# Diskrete Mathematik ICE

6. Übungsblatt

8. Mai 2018

In allen verschlüsselten Texten wurde die Konvention von Seite A.27 aus dem Skript verwendet. Die Buchstaben werden dabei paarweise in Zahlen übersetzt wie im Folgenden am Beispiel `XL` gezeigt. `X` ist der 24. Buchstabe im Alphabet und `L` der 12. Buchstabe. Das Paar `XL` wird in die Zahl

$$(24 - 1) \cdot 26 + (12 - 1) = 609$$

übersetzt.

**26.** Alice hat für den RSA-Algorithmus den öffentlichen Schlüssel $m = 697$ und $r = 199$ bekannt gegeben. Sie schickt nun die Nachricht `SIGNATUR` im Klartext und dazu die verschlüsselte Zahlenfolge $(187, 33, 587, 277)$. Entschlüsseln Sie diese Zahlenfolge mit Hilfe des öffentlichen Schlüssels. Mit welchem Schlüssel hat Alice die Zahlenfolge verschlüsselt? Rechnen Sie beim Entschlüsseln wie gewohnt modulo $m$ (und nicht modulo $p$ und $q$ wie in Aufgabe 27).

**27.** Die Entschlüsselung beim RSA-Algorithmus kann effizienter gestaltet werden, wenn man anstatt $g(y) = y^s \bmod m$ zunächst $g_p(y) = y^s \bmod p$ und $g_q(y) = y^s \bmod q$ berechnet und dann $g(y)$ mit Hilfe des chinesischen Restsatzes aus $g_p(y)$ und $g_q(y)$ bestimmt.

Für den RSA-Algorithmus wurde der öffentliche Schlüssel $m = 899$ und $r = 143$ bekannt gegeben. Berechnen Sie den Geheimschlüssel $s$ und führen Sie obiges Prinzip aus um die Nachricht $(229, 725, 847, 754, 473)$ zu entschlüsseln.

**28.** Verwenden Sie für diese Aufgabe *keine* elektronischen Hilfsmittel – die Lösung muss entsprechend samt allen Rechenschritten an der Tafel präsentiert werden können.

Für den RSA-Algorithmus wurde der öffentliche Schlüssel $m = 91$ und $r = 29$ bekannt gegeben.

(a) Verschlüsseln Sie die Nachricht $(31, 41)$.

(b) Berechnen Sie den Geheimschlüssel $s$.

(c) Entschlüsseln Sie die Nachricht $(89, 52)$.

**29.** Gegeben seien aussagenlogische Formeln $X$ und $Y$. Außerdem sei $T$ eine Tautologie und $K$ eine Kontradiktion.

(a) Zeigen Sie anhand einer Wahrheitstafel, dass

$$X \vee T \iff T, \qquad X \wedge T \iff X, \qquad X \vee K \iff X \qquad \text{und} \qquad X \wedge K \iff K.$$

(b) Erstellen Sie eine Wahrheitstafel für die Formeln $X \to Y$ und $X \leftrightarrow Y$ und begründen Sie anhand dieser Tafel, dass diese Formeln genau dann Tautologien sind, falls $X \Rightarrow Y$ beziehungsweise $X \Leftrightarrow Y$ gilt.

**30.** Bestimmen Sie mit Hilfe einer Wahrheitstafel für welche Belegungen von $A$, $B$ und $C$ die folgenden logischen Ausdrücke wahr sind.

(a)
$$(A \vee (B \to (C \wedge (A \wedge (\neg(A \leftrightarrow (B \vee C)))))))$$

(b)
$$((((((A \vee B) \to C) \wedge A) \wedge (\neg A)) \leftrightarrow B) \vee C)$$