LV Algorithmen und Komplexität **WS 2014/15**

Aufgaben: P-NP-Problem

Dozenten: Stefanie Feuerriegel, Damaris Soldan

SAT-Problem

1. Gesucht sei eine Belegung der booleschen Variablen x_i mit je einem Wert aus {0,1}, sodass das unten genannte Beispiel 1 ergibt.
   (a) $(\neg x_1 \vee x_3) \wedge (x_2 \vee x_1 \vee x_3) \wedge (\neg x_3 \vee x_2 \vee x_1)$
   (b) $(x_2 \vee x_1 \vee \neg x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3 \vee \neg x_1)$

Party-Problem

1. Geben Sie einen vollständigen Graphen für eine Party mit 8 Leuten an. Davon sollen sich mindestens 4 Personen kennen.

Cliquen-Problem

1. Zeichnen Sie einen vollständigen Graphen mit 6 Knoten und geben Sie jeweils eine mögliche 5er-, 4er, 3er-, und 2er-Clique an.

Euler-Kreis

1. Zeichnen Sie alle möglichen Graphen mit 5 Ecken, die einen Euler-Kreis beinhalten.

RSA-Verfahren

Zur Erinnerung wie das Euklidische Verfahren funktioniert, ist hier nochmal die Anwendung auf das Beispiel aus der Vorlesung gegeben.

Reste	**q**	**s**	**t**
288		1	0
5	57	0	1
3	1	1	-57
2	1	-1	58
1	2	2	**-115**

Die Koeffizienten s und t der aktuellen Zeile berechnen sich wie folgt:

aktuelle Zeile = vorletzte Zeile $-\ q *$ letzte Zeile

Also zum Beispiel: $58 = 1 - 1 * (-57)$
Weiterhin gilt $ggT(a, b) = s * a + t * b$.
In unserem Fall bedeutet das $ggT(a, b) = ggT(288, 5) = 1$, folglich ist $1 = 2 * 288 + (-115) * 5$.
Unser gesuchtes d ist $-155 \equiv 173 \bmod 288$.

1. Gegeben sei ein RSA-Schlüssel mit den Parametern $p = 11$, $q = 19$ und $e = 7$.
   (a) Bestimmen Sie den geheimen Schlüssel (m, d) mit Hilfe des erweiteren Euklidischen Verfahrens.
   (b) Verschlüsseln Sie den Klartext $x = 14$.
2. Gegeben sei ein RSA-Schlüssel mit $m = 143$. Der zweite Parameter des öffentlichen Schlüssels $e > 1$ sei kleinsmöglich gewählt.
   (a) Bestimmen Sie p und q.
   (b) Wie lautet e?
   (c) Bestimmen Sie den geheimen Schlüssel (m, d) mit Hilfe des Euklidischen Verfahrens.
   (d) Verschlüsseln Sie den Klartext $x = 7$.