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

Lösung: P-NP-Problem

Dozenten: Stefanie Feuerriegel, Damaris Soldan

SAT-Problem

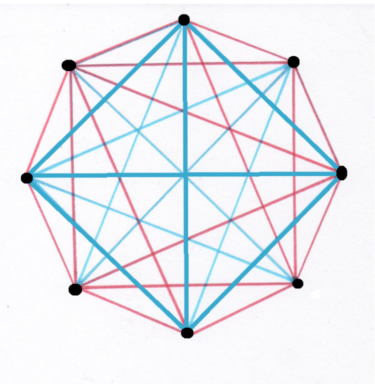
x_1	x_2	x_3	
0	0	0	$(1 \vee 0) \wedge (0 \vee 0 \vee 0) \wedge (1 \vee 0 \vee 0) = 1 \wedge 0 \wedge 1 = \text{false}$
0	0	1	$(1 \vee 1) \wedge (0 \vee 0 \vee 1) \wedge (0 \vee 0 \vee 0) = 1 \wedge 1 \wedge 0 = \text{false}$
0	1	0	$(1 \vee 0) \wedge (1 \vee 0 \vee 0) \wedge (1 \vee 1 \vee 0) = 1 \wedge 1 \wedge 1 = \text{true}$
0	1	1	$(1 \vee 1) \wedge (1 \vee 0 \vee 1) \wedge (0 \vee 1 \vee 0) = 1 \wedge 1 \wedge 1 = \text{true}$
1	0	0	$(0 \vee 0) \wedge (0 \vee 1 \vee 0) \wedge (1 \vee 0 \vee 1) = 0 \wedge 1 \wedge 1 = \text{false}$
1	0	1	$(0 \vee 1) \wedge (0 \vee 1 \vee 1) \wedge (0 \vee 0 \vee 1) = 1 \wedge 1 \wedge 1 = \text{true}$
1	1	0	$(0 \vee 0) \wedge (1 \vee 1 \vee 0) \wedge (1 \vee 1 \vee 1) = 0 \wedge 1 \wedge 1 = \text{false}$
1	1	1	$(0 \vee 1) \wedge (1 \vee 1 \vee 1) \wedge (0 \vee 1 \vee 1) = 1 \wedge 1 \wedge 1 = \text{true}$

1. (a)

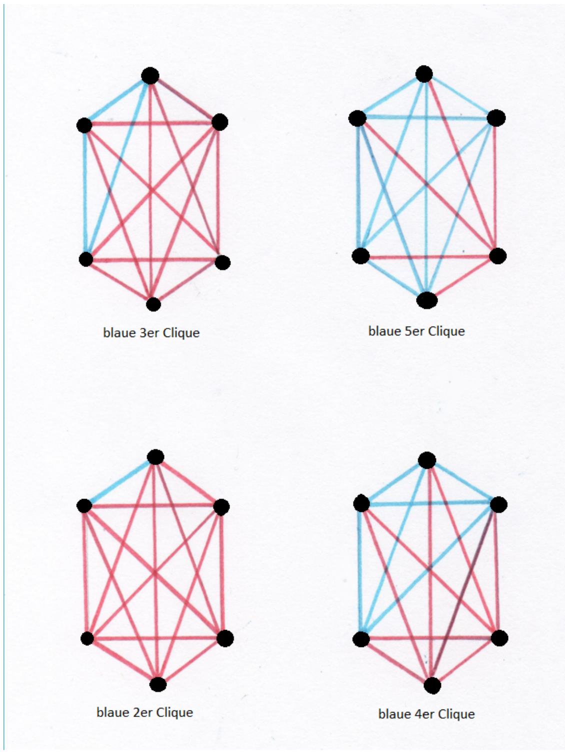
x_1	x_2	x_3	
0	0	0	$(0 \vee 0 \vee 1) \wedge (1 \vee 0 \vee 1) \wedge (1 \vee 0 \vee 1) = 1 \wedge 1 \wedge 1 = \text{true}$
0	0	1	$(0 \vee 0 \vee 0) \wedge (1 \vee 0 \vee 0) \wedge (1 \vee 1 \vee 1) = 0 \wedge 1 \wedge 1 = \text{false}$
0	1	0	$(1 \vee 0 \vee 1) \wedge (1 \vee 1 \vee 1) \wedge (0 \vee 0 \vee 1) = 1 \wedge 1 \wedge 1 = \text{true}$
0	1	1	$(1 \vee 0 \vee 0) \wedge (1 \vee 1 \vee 0) \wedge (0 \vee 1 \vee 1) = 1 \wedge 1 \wedge 1 = \text{true}$
1	0	0	$(0 \vee 1 \vee 1) \wedge (0 \vee 0 \vee 1) \wedge (1 \vee 0 \vee 0) = 1 \wedge 1 \wedge 1 = \text{true}$
1	0	1	$(0 \vee 1 \vee 0) \wedge (0 \vee 0 \vee 0) \wedge (1 \vee 1 \vee 0) = 1 \wedge 0 \wedge 1 = \text{false}$
1	1	0	$(1 \vee 1 \vee 1) \wedge (0 \vee 1 \vee 1) \wedge (0 \vee 0 \vee 0) = 1 \wedge 1 \wedge 0 = \text{false}$
1	1	1	$(1 \vee 1 \vee 0) \wedge (0 \vee 1 \vee 0) \wedge (0 \vee 1 \vee 0) = 1 \wedge 1 \wedge 1 = \text{true}$

(b)

Party-Problem



Cliquen-Problem



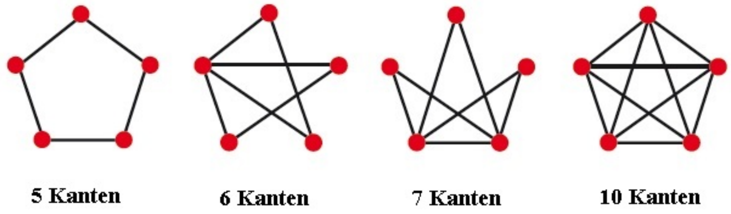
blaue 3er Clique

blaue 5er Clique

blaue 2er Clique

blaue 4er Clique

Euler-Kreis



RSA-Verfahren

1. (a)
   - $m = p * q = 11 * 19 = 209$
   - $\varphi(m) = (p-1)*(q-1) = 10 * 18 = 180$
   - $ggT(\varphi(m), e) = 1 \rightarrow \; ggT(180, 7) = 1$
   - $d = e^{-1} \mod \varphi(m) \rightarrow \; d = 7^{-1} \mod 180$

Reste	q	s	t
180		1	0
7	25	0	1
5	1	1	-25
2	2	-1	26
1	2	3	**-77**

   - $ggT(a,b) = s*a + t*b \rightarrow \;\; 1 = 3 * 180 + (-77) * 7$
   - **d=-77** $\equiv$ **103** mod 180

   (b)
   - $y = x^e \mod m$
   - $= 14^7 \mod 209$
   - **y=174**

2. (a)
   - $p = 11 \; q = 13$

   (b)
   - $\varphi(m) = (p-1)*(q-1) = 10 * 12 = 120$
   - $ggT(\varphi(m), e) = 1 \rightarrow \; ggT(120, e) = 1 \rightarrow \; e = 7$

   (c)
   - $d = e^{-1} \mod \varphi(m) \rightarrow \; d = 7^{-1} \mod 120$

Reste	q	s	t
120		1	0
7	17	0	1
1	7	1	**-17**

   - $ggT(a,b) = s*a + t*b \rightarrow \;\; 1 = 1 * 120 + (-17) * 7$
   - **d=-17** $\equiv$ **103** mod 120

   (d)
   - $y = x^e \mod m$
   - $= 7^7 \mod 143$
   - **y=6**