Logik und diskrete Stukturen

Felix (2807144) & Philipp (2583572) Müller

WS 14/15

Blatt 11

Aufgabe 1

Wähle $p = 5$ und $q = 7$. Daher $n = 5 \cdot 7 = 35$. Wir haben

$$\phi(n) = \phi(35) = \phi(5 \cdot 7) = \phi(5) \cdot \phi(7) = 6 \cdot 4 = 24$$

Verschlüssele $n \in \{0, \ldots, 34\}$. Wähle $e = 5$ ($1 < e < \phi(35)$ und $\text{ggT}(5, 24) = 1$).
Suche $d \in \mathbb{N}$ so, dass $ed = 1 \mod \phi(n)$.

d	de	$de \bmod 24$
1	5	5
2	10	10
3	15	15
4	20	20
5	25	1
6	30	6
7	35	11
	$\vdots$	
28	140	20
29 (=: d)	145	1
30	150	6

Öffentlicher Schlüssel $(n, e) = (35, 5)$
Privater Schlüssel $(n, d) = (35, 29)$

Nachricht `FELIX` = { 6 5 12 9 24 } (Nummer im Alphabet).

	x	x^5 mod 35
F	6	6
E	5	10
L	12	17
I	9	4
X	24	19

Geheimtext: { 6 10 17 4 19 }

Aufgabe 2

$$\phi = ((x_1 \implies \neg x_2) \wedge \neg(x_3 \iff x_1))$$

b)

$$\phi = ((x_1 \implies x_2) \wedge \neg((x_3 \implies x_1) \wedge (x_1 \implies x_3)))$$ Elimination der Äquivalenz

$$\phi = ((\neg x_1 \vee \neg x_2) \wedge \underbrace{\neg((\neg x_3 \vee x_1) \wedge (\neg x_1 \vee x_3))}$$ Elimination der Implikation

$$= \neg(\neg x_3 \vee x_1) \vee \neg(\neg x_1 \vee x_3)$$ De Morgan

$$= (\neg\neg x_3 \wedge \neg x_1) \vee (\neg\neg x_1 \wedge \neg x_3)$$ De Morgan

$$= (x_3 \wedge x_1) \vee (x_1 \wedge \neg x_3)$$ Elimination der doppelten N

$$\phi = ((\neg x_1 \wedge \geq x_2) \wedge \underbrace{((x_3 \wedge \neg x_1) \vee (x_1 \wedge \neg x_3)))}$$ (*)

$$= ((x_3 \wedge x_1) \vee x_1) \wedge ((x_3 \wedge \neg x_1) \vee \neg x_3)$$

$$= ((x_3 \vee x_1) \wedge (\neg x_1 \vee x_1)) \wedge ((x_2 \vee \neq x_3) \wedge (\neg x_1 \vee \neg x_3))$$

$$\phi = ((\neg x_1 \vee \neg x2) \wedge ((x_3 \vee x_1) \wedge (\neg x_1 \vee x_1) \wedge ((x_3 \vee \neg x_3) \wedge (\neg x_1 \vee \neg x_3))))$$

Mit Abkürzungen aus Roeglin 12/13, S.84 folgt

$$\phi = (\neg x_1 \vee \neg x_2) \wedge (x_3 \vee x_1) \wedge \underbrace{(\neg x_1 \vee x_1)}_{\text{immer wahr}} \wedge \underbrace{(x_3 \vee \neg x_3)}_{\text{immer wahr}} \wedge (\neg x_1 \vee \neg x_2)$$

$$\phi = (\neg x_1 \vee \neg x_2) \wedge (x_3 \vee x_1) \wedge (\neg x_1 \vee \neg x_3)$$

a) Benutze $(*)$ für Wahrheitstabelle:

x_1	x_2	x_3	$A = (\neg x_1 \vee \neg x_2)$	$B = (x_3 \wedge \neg x_1)$	$C = (x_1 \wedge \neg x_3)$	$D = (B \vee C)$	$\phi = (A \wedge D)$
0	0	0	1	0	0	0	0
1	0	0	1	0	1	1	1
0	1	0	1	0	0	0	0
1	1	0	0	0	1	1	0
0	0	1	1	1	0	1	1
1	0	1	1	0	0	0	0
0	1	1	1	1	0	1	1
1	1	1	0	0	0	0	0

DNF:

$$(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3)$$