LIDS Blatt 11

Aufgabe 1. RSA.

$p = 5 \quad q = 7 \Rightarrow n = p \cdot q = 35 \quad \varphi(n) = (5-1)(7-1) = 24$

sei $e = 11 \qquad ggT(e, \varphi(n)) = ggT(11, 24) = 1$

$24 = 2 \cdot 11 + 2$

$11 = 5 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 11 - 5 \cdot 2$

$= 11 - 5 \cdot (24 - 2 \cdot 11)$

$= 11 \cdot 11 - 5 \cdot 24$

$\Rightarrow d = 11$

Probe $e \cdot d = 121 \equiv 1 \mod 24$ ✓

Öffentlicher Schlüssel (35, 11)

Privater Schlüssel (35, 11)

Verschlüsselung für NESSA

Berechnungsbeispiel für Buchstabe E; $m = 5$

$E(m) = m^{11} \mod 35 \qquad z = 5^{11} \mod 35 = 48828125 \mod 35 = 10$

$D(z) = z^{11} \mod 35 \qquad m = 10^{11} \mod 35 = 100000000000 \mod 35 = 5$

Buchstabe	m	$z = m^{11} \mod 35$	$m = z^{11} \mod 35$
N	14	14	14
E	5	10	5
S	19	24	19
S	19	24	19
A	1	1	1

LuDS Blatt 11

Aufgabe 2 a

x_1	x_2	x_3	$x_1 \to \neg x_2$	$x_3 \leftrightarrow x_1$	$\neg(x_3 \leftrightarrow x_1)$	$(x_1 \to \neg x_2) \wedge \neg(x_3 \leftrightarrow x_1)$
0	0	0	1	1	0	0
0	0	1	1	0	1	1
0	1	0	1	1	0	0
0	1	1	1	0	1	1
1	0	0	1	0	1	1
1	0	1	1	1	0	0
1	1	0	0	0	1	0
1	1	1	0	1	0	0

DNF: $\varphi_{DNF} = (\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3)$

Aufgabe 2b) mit Erzeuge KNF-Algorithmus

$\varphi = (x_1 \to \neg x_2) \wedge \neg(x_3 \leftrightarrow x_1)$ Schritte (1+2)

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

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

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

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

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

$= (\neg x_1 \vee \neg x_2) \wedge (x_3 \vee x_1) \wedge (\neg x_1 \vee x_3) = \varphi_{KNF}$