Lösungen vom 14.5.2018

40.) Es ergibt sich folgende Zahlenfolge:

2, 4, (16), 256, 170, 219, 604, 634, 422, 662, 25, 625, 430, 141, 538, 633, 489, 335, 169, 547, 393, 372, 315, 509, 285, 518, 190, 82, 54, 248, 140, 257, (16)

Die Periodenlänge ist 30.

41.) Wir berechnen zunächst die Randverteilungen:

	X_1	X_2	
Y_1	1/6	1/3	1/2
Y_2	1/8	1/4	3/8
Y_3	1/24	1/12	1/8
	1/3	2/3	1

Also z.B.
$P(Y=y_1) = 1/2$

Wir überprüfen nun die 6 Gleichungen:

$$P(X=x_i, Y=y_j) \stackrel{?}{=} P(X=x_i) \cdot P(Y=y_j)$$

z.B: $P(X=x_1, Y=y_1) = \frac{1}{6} = P(X=x_1) \cdot P(Y=y_1) = \frac{1}{2} \cdot \frac{1}{3}$

Alle 6 Gleichungen treffen zu. Also sind X und Y unabhängig.

42.) $H(X,Y) = 4 \cdot \left(-\frac{1}{4} \log_2 \frac{1}{4}\right) = 2$

$$H(X) = -\frac{3}{4} \log_2 \frac{3}{4} - \frac{1}{4} \log_2 \frac{1}{4} = 0{,}811$$

$$H(Y) = -\frac{1}{2} \log_2 \frac{1}{2} - 2 \cdot \frac{1}{4} \log_2 \frac{1}{4} = 1{,}5$$

$$H(X|Y) = H(X,Y) - H(Y) = 2 - 1,5 = 0,5$$

$$H(Y|X) = H(X,Y) - H(X) = 2 - 0,811 = 1,189$$

$$I(X,Y) = H(X) + H(Y) - H(X,Y) = 0,811 + 1,5 - 2 = 0,311$$

43.) Der Abhörer erfährt

$$m' = m \oplus z$$
$$m'' = m' \oplus z' = m \oplus z \oplus z'$$
$$m''' = m'' \oplus z = m \oplus z'$$

Er berechnet $m' \oplus m'' = z'$

und schließlich: $m''' \oplus z' = m$

44.) Übertragung von 10^6 Bit in moderner Weise; dies sind 10^3 Blöcke. Die Anzahl der Rechenoperationen ist also $10^3 \cdot (1000)^3 = 10^{12}$ (pro Teilnehmer).

Bei hybrider Übertragungsweise:

$(1000)^3$ zur Übertragung des Schlüssels,

ausschließend: $10^3 \cdot (1000 + 1000)$

Insgesamt: $10^9 + 2 \cdot 10^6$ Rechenoperationen.

45.) Die Anzahl der 500 Bit-Primzahlen ist

$$\approx \pi(2^{500}) - \pi(2^{499})$$

$$\approx \frac{2^{500}}{\ln(2^{500})} - \frac{2^{499}}{\ln(2^{499})} \approx 4{,}7 \cdot 10^{147}$$

Anzahl der ungeraden 500 Bit-Zahlen:

$$(2^{500} - 2^{499})/2 \approx 8{,}18 \cdot 10^{149}$$

$$\frac{\text{Anzahl Primzahlen}}{\text{Anzahl unger. Zahlen}} \approx 1:174$$

46.) Man muss nach n auflösen:

$$n^{\ln n} = 2^{80}$$

und erhält: $n = 1714$

47.) Additionstafel:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Neutrales Element ist 0

Additive Inverse:

0 — 0
1 — 5
2 — 4
3 — 3
4 — 2
5 — 1

Multiplikationstafel:

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Neutrales Element: 1

Multiplikative Inverse besitzen nur die 1 und die 5:

$1^{-1} = 1$, $5^{-1} = 5$

48.) $24 = 0 \cdot 129 + 24$

$129 = 5 \cdot 24 + 9$

$24 = 2 \cdot 9 + 6$

$9 = 1 \cdot 6 + 3$ $\Rightarrow$ der ggT ist 3

$6 = 2 \cdot 3 + 0$

49.) Es gelte $a \cdot b \equiv 1 \pmod{n}$. Also ist $a \cdot b - 1$ durch n teilbar: $a \cdot b - 1 = k \cdot n$, somit:

$a \cdot b - k \cdot n = 1$. Sei $d := ggT(a, n)$. Dann ist $a = d \cdot a'$ und $n = d \cdot n'$. Eingesetzt:

$a \cdot b - k \cdot n = d \cdot a' b - k \cdot d \cdot n' = d(a'b - kn') = 1$

Somit ist d Teiler von 1; d.h. $d = 1$.