Lösungen, 4.6.2018

61.) Euklid-Algorithmus auf 9 und $n-1=22$ anwenden:

$$22 = 2 \cdot 9 + 4$$

$$9 = 2 \cdot 4 + 1 \Leftarrow ggT$$

Rückwärts einsetzen:

$$1 = 9 - 2 \cdot 4$$
$$= 9 - 2 \cdot (22 - 2 \cdot 9)$$
$$= -2 \cdot 22 + \underline{\underline{5}} \cdot 9$$

Also ist 5 multiplikatives Inverses von 9 mod 22.

Also $e = 9$ und $d = 5$.

Verschlüsseln: $c = m^e \bmod n = 16^9 \bmod 23$

16^9 mittels „square + multiply" berechnen:

$$16^9 = (((16)^2)^2)^2 \cdot 16$$

$16^2 = 256 \equiv 3 \pmod{23}$,

$16^4 \equiv 3^2 \equiv 9 \pmod{23}$,

$16^8 \equiv 9^2 \equiv 81 \equiv 12 \pmod{23}$

$16^9 \equiv 12 \cdot 16 \equiv 192 \equiv \underline{\underline{8}} \pmod{23}$

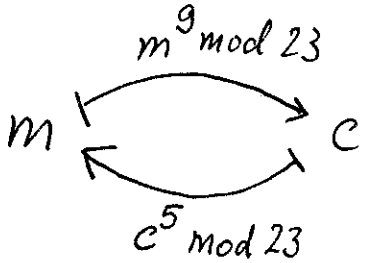
Also $c = 8$

Entschlüsseln: $c^d \bmod n = 8^5 \bmod 23 = \underline{\underline{16}} = m$

Wenn man (nicht nur $m=16$, sondern) alle Nachrichten $m \in \{1,2,\dots,22\}$ analysiert, auf welchen Wert $c = m^9 \bmod 23$ sie abgebildet werden, so erhält man:

m	1	2	3	4	5	6	7	8	9	10	11
c	1	6	18	13	11	16	15	9	2	20	19

m	12	13	14	15	16	17	18	19	20	21	22
c	4	3	21	14	8	7	12	10	5	17	22



Es entsteht also durch Wahl von $d \in \mathbb{Z}_{22}^*$ eine (pseudo-) zufällige Permutation der Zahlen $1,2,\dots,22$.
Insgesamt stehen $\varphi(22) = 10$ solche Permutationen zur Verfügung.

62.) Der Beweis ist nicht ganz einfach.

Falls n Primzahl, so ist $\mathbb{Z}_n^* = \{1, 2, \dots, n-1\}$, also $\varphi(n) = n-1$. Die Ordnung von jedem $a \in \mathbb{Z}_n^*$, also die Größe der Untergruppe $\langle a \rangle$, muss ein Teiler von $n-1$ sein. Sei $\mathcal{U}(t)$ die Menge diejenigen $a \in \Sigma_n^*$ mit Ordnung t. Somit gilt, dass $\mathbb{Z}_n^*$ sich als disjunkte Vereinigung aller $\mathcal{U}(t)$ schreiben lässt, wobei t alle Teiler von $n-1$ durchläuft. Somit gilt:

$$n-1 = \sum_{\substack{\text{alle Teiler} \\ t \text{ von } n-1}} |\mathcal{U}(t)|$$

Falls $\mathcal{U}(t)$ nicht die leere Menge ist, so gilt $|\mathcal{U}(t)| = \varphi(t)$, denn aus einem $a \in \mathcal{U}(t)$ lassen sich $\varphi(t)$ viele $b \in \mathcal{U}(t)$ gewinnen, indem man $b = a^i$, $i \leq t$, teilerfremd zu t, wählt.

Sollte also auch nur ein $\mathcal{U}(t) = \emptyset$ sein (für einen Teiler t von $n-1$), so folgt

$$n-1 = \sum_{\substack{t \text{ Teiler} \\ \text{von } n-1}} |\mathcal{U}(t)| < \sum_{\substack{t \text{ Teiler} \\ \text{von } n-1}} \varphi(t)$$

Andererseits gilt $\sum_{\substack{t \text{ Teiler} \\ \text{von } n-1}} \varphi(t) = n-1$.

Somit ist dies ein Widerspruch; kein solches $U(t)$ ist die leere Menge, sondern $|U(t)| = \varphi(t) > 0$

Insbesondere ist $|U(n-1)| = \varphi(n-1) > 0$.

<u>Es gibt</u> also mindestens ein Element mit Ordnung $n-1$ (eine Primitivwurzel); sogar $\varphi(n-1)$ viele. □

63.)

n_i	$\varphi(n_i)$	$\varphi(n_i)/n_i$
$2 \cdot 3 = 6$	2	0,333
$2 \cdot 3 \cdot 5 = 30$	$2 \cdot 4 = 8$	0,267
$2 \cdot 3 \cdot 5 \cdot 7 = 210$	$2 \cdot 4 \cdot 6 = 48$	0,229
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$	$2 \cdot 4 \cdot 6 \cdot 10 = 480$	0,208
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$	$2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 = 5760$	0,192
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = 510510$	$2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 \cdot 16 = 92160$	0,181

64.)

$n = 5$	100 %		$n = 15$	$2/12 = 16{,}7\%$	
6	0 %		16	0 %	
7	100 %		17	100 %	
8	0 %		18	0 %	
9	0 %		19	100 %	
10	0 %		20	0 %	
11	100 %		21	$2/18 = 11{,}1\%$	
12	0 %		22	0 %	
13	100 %		23	100 %	
14	0 %		24	0 %	
			25	$2/22 = 9{,}1\%$	

65.) $\varphi(561) = \varphi(3) \cdot \varphi(11) \cdot \varphi(17) = 2 \cdot 10 \cdot 16 = 320$

Die gesuchte W'heit ist $\frac{320-2}{561-3} = 0{,}57 = 57\%$

$\varphi(1105) = \varphi(5) \cdot \varphi(13) \cdot \varphi(19) = 4 \cdot 12 \cdot 18 = 864$

Die gesuchte W'heit ist $\frac{864-2}{1105-3} = 0{,}78 = 78\%$

Für große Carmichael-Zahlen ist damit zu rechnen, dass diese W'heit gegen 1 strebt.

66.) Alice sendet zuerst und sendet $\tilde{\tilde{x}}$, also $\tilde{x}$, ein zweites Mal verschlüsselt. Nachdem Bob $\tilde{y}$ gesendet hat, sendet Alice ausschließend $\tilde{x}$. Bob überprüft, dass $\tilde{\tilde{x}} = a^{\tilde{x}}$ mod n. Beide berechnen nun z.

Bemerkung: Man spricht von einem Commitment-Protokoll. Alice sendet zuerst $\tilde{\tilde{x}}$ und ist damit auf das darin verschlüsselte $\tilde{x}$ festgelegt. Andererseits kann Bob diese Information $\tilde{x}$ vorläufig nicht sehen.

67.) Bei PH ist $\varphi(n) = n-1$, da n Primzahl ist. Insofern kann $\varphi(n)$ unmittelbar aus n berechnet werden. Ebenso ist es effizient möglich mittels ExtEuklid$(e, n-1)$ d zu berechnen (also kein geheimer Dechiffrierschlüssel!)

Anders bei RSA: Ohne Kenntnis der Faktorisierung von n in p und q lässt sich $\varphi(n) = (p-1)\cdot(q-1)$ nicht berechnen (zumindest ist nicht klar, wie). Und damit lässt sich ebensowenig d berechnen.

68.) $\frac{3n^3+5n}{2n+1} = O(n^2)$, $42 = O(1)$,

$5n^2+7\log n = O(n^2)$, $7n^2\log n = O(n^2 \log n)$,

$3n^3\sqrt{2n} = O(n^{4/3})$, $(\log n)^{\log n} = 2^{\log((\log n)^{\log n})}$

$= 2^{\log n \cdot \log(\log n)} = n^{\log(\log n)}$, $(\sqrt{2})^{n/3} = 2^{n/6} = 1{,}12^n$

$\log(n!) = \log\left(\sqrt{2\pi n}\cdot\left(\frac{n}{e}\right)^n\right) = O\left(\frac{1}{2}\log n\right) + O\left(n\cdot\log\left(\frac{n}{e}\right)\right)$

(Stirling)

$= O(\log n) + O(n\log n) - O(n) = O(n\log n)$