Lösungen, 11.6.2018

69.) Man muss $\frac{\varphi(n)}{n}$ abschätzen.

$$\frac{\varphi(n)}{n} = \frac{n \cdot (1-\frac{1}{p}) \cdot (1-\frac{1}{q}) \cdot (1-\frac{1}{r})}{n}$$

$$\approx (1-2^{-100}) \cdot (1-2^{-200}) \cdot (1-2^{-200}) \approx 1-2^{-100}$$

Die W'heit, dass $a^{n-1} \not\equiv 1 \pmod n$, liegt also bei 2^{-100}.

70.) Da $\varphi(n) = \underbrace{(p-1)}_{\text{gerade}} \cdot \underbrace{(q-1)}_{\text{gerade}}$ durch 4 teilbar ist, kann e nicht durch 4 (auch nicht durch 2) teilbar sein.

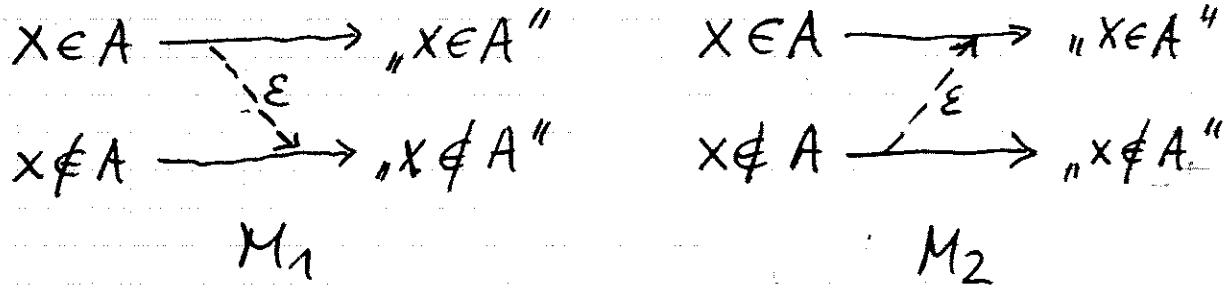
17 und 65537 sind Primzahlen, daher liegen diese Zahlen immer in $\mathbb{Z}^*_{\varphi(n)}$, auch ohne vorher n zu kennen. Ein weiterer Vorteil ist, dass die Exponentiation, z.B. mit 17 nur 4 Quadrierungen und eine Multiplikation erfordert. Daher ist die Laufzeit für das Verschlüsseln (also das Berechnen von $m^e \bmod n$) $O(k^2)$, wobei k die Bitlänge von m, e, n ist.

71.) Wir zeigen $ZPP \subseteq RP$. Sei $p(n)$ die erwartete polynomiale Laufzeit des gegebenen ZPP-Algorithmus. Mit der Markov-Ungleichung kann eine Laufzeit von mehr als $2 \cdot p(n)$ Schritten höchstens mit W'keit $\frac{1}{2}$ auftreten.
Man kann den ZPP-Algorithmus in einen RP-Algorithmus umformen: Der Berechnungsvorgang, sofern er nach $2 \cdot p(n)$ Schritten zu keinem Ergebnis geführt hat, wird abgebrochen und 0 ausgegeben.

Aus Symmetriegründen gilt entsprechend auch $ZPP \subseteq co\text{-}RP$.

Wir zeigen nun $RP \cap co\text{-}RP \subseteq ZPP$.
Sei M_1 ein RP-Algorithmus für Problem A und M_2 ein RP-Algorithmus für $\bar{A}$.

Skizze:



Ein ZPP-Algorithmus entsteht dadurch, dass man wiederholt beide Algorithmen laufen lässt, bis beide einheitlich „$x \in A$“ oder „$x \notin A$“ ausgeben. Die entsprechende Ausgabe ist dann korrekt.

72.) Sei $d := ggT(x-y, n)$.

Nehmen wir zunächst an, dass $d = n$. Aber dann folgt $x \equiv y \pmod{n}$, was in der Aufgabenstellung aber ausgeschlossen ist.

Nehmen wir nun an, $d = 1$. Ein einfaches Resultat über Teilbarkeit besagt:

> Wenn a Teiler von $b \cdot c$ ist,
> und wenn $ggT(a,b) = 1$, so
> folgt, dass a Teiler von c ist.

In unserem Fall heißt das, da n Teiler ist von $x^2 - y^2 = (x-y) \cdot (x+y)$ und $d = 1$, dass n Teiler von $x+y$ sein muss. Aber dies

widerspricht der Voraussetzung $x \not\equiv -y \pmod n$.
Daher ist d weder gleich n, noch gleich 1.
Insofern ist d ein nicht-trivialer Teiler von n.

Bemerkung: Beim Miller-Rabin-Primzahltest gibt es 2 mögliche Ausgänge mit dem Ergebnis „keine Primzahl". Der „Hauptausgang" ist das Nicht-Bestehen des Fermat-Tests. Die weitere Möglichkeit ist der „Nebenausgang" Nicht-Bestehen der Quadratwurzel der 1-Tests.
In diesem Fall haben wir die Situation, dass für ein x gilt $x^2 \equiv 1^2 \pmod n$, sowie $x \not\equiv \pm 1 \pmod n$.
Somit ergibt sich, wie bei dieser Aufgabe, in diesem Fall das Seitenergebnis einer Faktorierung von n, nämlich $ggT(n, x-1)$ bzw. $ggT(n, x+1)$.

73.) $n = 77 = 7 \cdot 11$ und $e = 17$.

Daraus folgt: $\varphi(n) = (7-1) \cdot (11-1) = 60$

Euklid: $60 = 3 \cdot 17 + 9$

$17 = 1 \cdot 9 + 8$

$9 = 1 \cdot 8 + \textcircled{1} \leftarrow ggT$

Somit: $1 = 9 - 8$

$= 9 - (17 - 9) = -17 + 2 \cdot 9$

$= -17 + 2 \cdot (60 - 3 \cdot 17)$

$= 2 \cdot 60 - 7 \cdot 17$

Inverses von $e = 17$ ist also $-7 \equiv 60 - 7 = \widetilde{53} = d \pmod{60}$

Chiffre $c = 42$. Der dazu gehörige Klartext ist $c^d \bmod n = 42^{53} \bmod 77 = 14$.

74.) Da 9, 8, 7 paarweise teilerfremd sind, kann man den Chinesischen Restsatz anwenden. Gesucht ist die Lösung x der 3 Kongruenzgleichungen:

$$x \equiv 4 \pmod 9$$
$$x \equiv 3 \pmod 8$$
$$x \equiv 0 \pmod 7$$

Es gilt $n = 9 \cdot 8 \cdot 7 = 504$.
$m_1 = 504/9 = 56$, $m_2 = 504/8 = 63$, $m_3 = 504/7 = 72$

Mittels ExtEuklid erhalten wir:

$y_1 = m_1^{-1} \pmod 9 = 5$, $y_2 = m_2^{-1} \pmod 8 = 7$,

$y_3 = m_3^{-1} \pmod 7 = 4$. Damit ergibt sich

$$x = \left(\sum_{j=1}^{3} a_j \cdot y_j \cdot m_j\right) \bmod n$$
$$= (4 \cdot 5 \cdot 56 + 3 \cdot 7 \cdot 63 + 0 \cdot 4 \cdot 72) \bmod 504$$
$$= 427$$

Es sind 427 Goldmünzen.

(PS: Wenn die Aufgabe eine Zahl zwischen 500 und 1000 verlangt hätte, so wäre die Lösung $427 + 504 = 931$.)

75.) Der Sinn der Aufgabe ist nur der, auf einen Nachteil von RSA hinzuweisen: die Verschlüsselung ist deterministisch. Das heißt, jeder, der „Kandidat A" chiffriert an den Wahlleiter schickt, schickt ein und dieselbe Chiffre.

Darüber hinaus ist das gesamte Protokoll (also schlicht RSA zu verwenden) noch unausgegoren: es fehlt jedwede Form der Anonymisierung. Der Wahlleiter darf zwar wissen, wer seine Stimme abgegeben hat, nicht aber, was er gewählt hat.