Kryptologie: Übungsblatt 8, Besprechung ab dem 18.6.2018, 10:15, H20

76.) Man zeige, dass die auf der Menge der algorithmischen Problemstellungen definierte Relation $\preceq_{eff}$ reflexiv und transitiv ist.

77.) [Faktorisieren $\preceq_{eff}$ starkes Brechen von RSA]
Gegeben sei $n = 77$. (Wir stellen uns vor, dies sei eine sehr große Zahl, so dass die Faktorisierung von n, hier 7 und 11, sowie $\varphi(n) = 60$, uns zunächst nicht bekannt sind.)
Wir wählen (per Zufall, oder grundsätzlich immer) den Verschlüsselungsexponenten $e = 17$. Nun wird das Orakel befragt, das uns den zugehörigen Entschlüsselungsexponenten, nämlich $d = 53$ verrät (vgl. Aufgabe 73) – dies entspricht dem Brechen von RSA im starken Sinne.
Nun wählen wir "zufällig" einige Basiszahlen (Nachrichten), etwa $m = 4$, $m = 2$ und $m = 3$.
Mit etwas Glück kann man auf diese Weise die Faktorisierung von n berechnen. Wie? Führen Sie dies mit den angegebenen Zahlen durch!

78.) [Chinesischer Restsatz mit Tabelle, ohne Rechnung]
Die Aufgabe besteht darin, die Quadratwurzeln der 1 modulo 35 zu bestimmen. Es ist $35 = 5 \cdot 7$. Durch systematisches Ausfüllen der folgenden Tabelle (und Ablesen der entsprechenden Einträge) lässt sich die Aufgabe ohne Rechnung lösen.

	0	1	2	3	4	5	6
0							
1							
2							
3							
4							

79.) Wir betrachten einen BPP-Algorithmus mit Fehlerwahrscheinlichkeit $\varepsilon = 1/3$.
Wie oft muss man den Algorithmus mit unabhängigen Zufallszahlen wiederholen, um per Mehrheitsentscheid die Fehlerwahrscheinlichkeit unter 0.01 zu drücken?
Man rechne einmal exakt (was sehr aufwändig ist und ggf. ein Computer Algebra-System benötigt) und einmal mit der in der Vorlesung hergeleiteten Abschätzung.

80.) Gegeben eine Zahl n und $a \in \mathbb{Z}_n^*$. In der folgenden Tabelle, in der ersten Spalte sei n eine Primzahl, in der zweiten Spalte sei $n = p \cdot q$ für zwei unbekannte Primzahlen p, q. Tragen Sie ein, welche Rechenoperationen einfach (E) und welche nur sehr schwer (S) auszuführen sind, sofern n eine Zahl mit (zum Beispiel) 1000 Binärstellen ist.

	n Primzahl	$n = p \cdot q$
Berechnen von $\varphi(n)$		
Berechnen von a^{n-1} mod n		
Feststellen ob a Primitivwurzel mod n		
Feststellen ob $a \in QR_n$		
Berechnen von a^{-1} mod n		

81.) [El Gamal]
Teilnehmer Bob hat den öffentlichen El Gamal-Schlüssel 13, wobei initial die Primzahl $n = 23$ und die Primitivwurzel $a = 5$ festgelegt wurde.
Teilnehmer Alice möchte an Bob die Nachricht 10 schicken. Geben Sie 3 verschiedene Chiffren an, die Alice senden könnte und die dazu führen, dass Bob am Ende korrekt 10 entschlüsseln kann.

82.) Man zeige, dass die folgenden beiden algorithmischen Probleme gegenseitig mittels $\preceq_{eff}$ reduzierbar sind:

Diffie-Hellman-Problem: Gegeben n (Primzahl), a (Primitivwurzel mod n), $\tilde{x}\,(= a^x \bmod n)$, $\tilde{y}\,(= a^y \bmod n)$. Finde: $z = a^{xy} \bmod n$.

El Gamal-System brechen: Gegeben n (Primzahl), a (Primitivwurzel mod n), $\tilde{x}\,(= a^x \bmod n)$, $\tilde{y}\,(= a^y \bmod n)$, $\tilde{m}\,(= a^{xy} \cdot m \bmod n)$. Finde: m.