Kryptologie: Übungsblatt 7, Besprechung ab dem 11.6.2018, 10:15, H20

69.) Sei $n = p \cdot q \cdot r$ eine Carmichael-Zahl mit Bitlänge 500. Die drei Primfaktoren p, q, r haben Bitlänge 100, 200, 200. Schätzen Sie ab, wie groß die Wahrscheinlichkeit ist, dass n durch den Fermat-Test als Nicht-Primzahl entlarvt wird (mit anderen Worten, wie groß ist die Wahrscheinlichkeit, dass $a^{n-1} \not\equiv 1 \pmod{n}$, bei zufällig gewähltem a).

Man darf hier verschiedentliche Vernachlässigungen verwenden. Es geht hier nur darum, die Größenordnung der betreffenden Wahrscheinlichkeit herauszubekommen. Eine n-Bitzahl identifizieren wir schlicht mit 2^n. Bei der Addition oder Subtraktion einer 200-Bitzahl mit einer 100-Bitzahl entsteht wieder eine 200-Bitzahl, usw.

70.) Beim RSA-Verfahren wird eine Zahl e gesucht in $\mathbb{Z}^*_{\varphi(n)}$, wobei n das Produkt zweier verschiedener, großer Primzahlen p und q ist.
Kann e durch 4 teilbar sein?

Bei manchen Implementierungen von RSA wird e fest mit $17 = 2^4 + 1$ oder $65537 = 2^{16} + 1$ festgelegt. Ist ein solches e immer (bei noch unbekanntem n und damit auch $\varphi(n)$) möglich? Welchen Vorteil könnte eine solche Wahl haben?

71.) Die probabilistischen Komplexitätsklassen RP und ZPP wurden in der Vorlesung formal definiert.
Nochmals in Kürze: bei ZPP gibt es keine fehlerhaften Ausgaben, jedoch ist die Algorithmen-Laufzeit eine Zufallsvariable; diese hat polynomialen Erwartungswert.
Bei RP haben wir eine einseitige Fehlermöglichkeit: mit Wahrscheinlichkeit ε kann eine Eingabe $x \in L$ zur Ausgabe 0 führen (ansonsten zur Ausgabe 1). Eine Eingabe $x \notin L$ führt immer auf die Ausgabe 0. Die Laufzeit eines RP-Algorithmus ist immer polynomial.

Zeige, dass ZPP $=$ RP $\cap$ co-RP, dabei ist co-RP die Menge der Komplemente der RP-Entscheidungsprobleme.

72.) Für eine gegebene Zahl n haben wir zwei Zahlen x, y gefunden mit $x^2 \equiv y^2 \pmod{n}$, wobei $x \not\equiv \pm y \pmod{n}$. Man zeige, dass daraus folgt, dass n keine Primzahl sein kann, und dass darüber hinaus $ggT(x - y, n)$ einen nicht-trivialen Faktor von n ergibt.

73.) Angenommen Bob verwendet den öffentlichen RSA-Schlüssel $(n = 77, e = 17)$ und empfängt von Alice die Chiffre 42. Sie sind in der Lage, mit einem neuen, raffinierten Faktorisierungsalgorithmus die Faktorisierung von 77 zu knacken, nämlich $77 = 7 \cdot 11$. Was ist der Klartext von Alice?

74.) Neun Piraten haben einen Schatz von Goldmünzen erobert. Es sind weniger als 500 Münzen. Da die Piraten nicht rechnen bzw. zählen können, verteilen sie den Schatz Münze für Münze reihum. Es geht aber leider nicht auf: 4 Münzen bleiben übrig. Darüber geraten sie so in Streit, dass am Ende einer der Piraten sein Leben verliert. Nun wird erneut der Schatz Münze für Münze zwischen 8 Piraten aufgeteilt. Erneut bleiben diesmal 3 Münzen übrig. Erneuter Streit endet mit 7 überlebenden Piraten. Beim diesmaligen Aufteilungsvorgang geht es auf. Jeder Pirat erhält $1/7$ des Goldschatzes.

Wieviele Münzen sind es?

75.) Sie sind der Wahlleiter bei einer geheimen RSA-basierten Wahl in Ihrem Sportverein, bei der Sie selber nicht mitstimmen dürfen. Jeder Wahlberechtigte sendet Ihnen in RSA-verschlüsselter Form entweder ”Kandidat A” oder ”Kandidat B” oder ”Kandidat C” oder ”Enthaltung” zu. Am Ende wird Kandidat B gewählt, und zwar mit 102 zu 154 zu 87 Stimmen, bei 23 Enthaltungen.
Können Sie – auch ohne die Nachrichten zu entschlüsseln – feststellen, wer für welchen Kandidaten gestimmt hat?