Kryptologie: Übungsblatt 6, Besprechung ab dem 4.6.2018, 10:15, H20

61.) [Pohlig-Hellman-Chiffrierung]
Es ist $n = 23$ eine Primzahl. Sei $e = 9$. Es gilt $ggT(9, n-1) = 1$. Bestimme d so dass $e \cdot d \equiv 1 \pmod{n-1}$. Verschlüssle (mittels Pohlig-Hellman-Verfahren) die Nachricht $m = 16$ mittels e und entschlüssle wieder mittels d.

62.) In der Vorlesung wurde der Satz von Gauß (ohne Beweis) angegeben, der diejenigen n charakterisiert, so dass die multiplikative Gruppe $\mathbb{Z}_n^*$ zyklisch ist. Für kryptographische Anwendungen (in dieser Vorlesung) ist nur der Fall, dass n eine Primzahl ist, von Interesse. Beweise für diesen Fall, dass $\mathbb{Z}_n^*$ zyklisch ist.

63.) Gib eine Folge $n_1 < n_2 < n_3 < \ldots$ natürlicher Zahlen an, bei denen der relative Unterschied zwischen $\varphi(n_i)$ und n_i besonders groß ist.

64.) [Fermat-Test als Primzahl-Test]
Für eine gegebene, zu testende Zahl n und eine Zufallszahl $a \in_R \{2, \ldots, n-2\}$ soll bestimmt werden, wie groß der Prozentsatz der a's ist mit

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{(sog. Fermat-Test)}$$

(Bemerkung: wir haben hier $a = 1$ und $a = n-1$ außen vor gelassen, da diese *immer* die Eigenschaft $a^{n-1} \equiv 1 \pmod{n}$ haben – zumindest für ungerades n.)
Bestimmen Sie diesen Prozentsatz für $n = 5, 6, 7, \ldots, 25$ (per Computer oder Taschenrechner).

65.) Die ersten zwei Carmichael-Zahlen sind $561 = 3 \cdot 11 \cdot 17$ und $1105 = 5 \cdot 13 \cdot 19$. (Carmichael-Zahlen sind solche Nicht-Primzahlen n, die den Fermat-Test für alle $a \in \mathbb{Z}_n^*$ bestehen.) Berechnen Sie die Wahrscheinlichkeit, dass 561 bzw. 1105 bei zufälliger Wahl von $a \in_R \{2, \ldots, n-2\}$ den Fermat-Test (fälschlicherweise) besteht.

66.) Beim Diffie-Hellman-Verfahren tragen beide Kommunikationspartner zur Festlegung des geheimen Schlüssels z bei (daher: Schlüsselvereinbarung). In der Vorlesung bzw. im Lehrbuch ist es so, dass beide Partner *Alice* und *Bob* ihre Botschaften $\tilde{x}$ und $\tilde{y}$ gleichzeitig austauschen, und danach berechnet Alice $z = (\tilde{y})^x \bmod n$, sowie Bob berechnet $z = (\tilde{x})^y \bmod n$.

Angenommen, eine gerade Zahl z bringt Alice einen Vorteil und eine ungerade Zahl z bringt Bob einen Vorteil. Nun könnte Bob die Nachricht $\tilde{x}$ von Alice zuerst abwarten, um dann sein y so zu wählen, dass seine Nachricht $\tilde{y}$ insgesamt eine ungerade Zahl z ergibt. Umgekehrt könnte es Alice durch entsprechendes Abwarten analog machen.

Dies ist noch unbehandelter Stoff. Haben Sie einen Vorschlag, wie man dieses Protokoll so arrangieren bzw. modifizieren kann, dass keiner der beiden einen Vorteil davontragen kann?

67.) [Pohlig-Hellman vs. Rivest-Shamir-Adleman]
Sowohl bei PH als auch bei RSA wird der Chiffrierexponent $e \in_R \mathbb{Z}_{\varphi(n)}^*$ gewählt und der Dechiffrierexponent d so bestimmt, dass $d \cdot e \equiv 1 \pmod{\varphi(n)}$. In beiden Fällen ergibt

sich dann $(m^e)^d$ mod $n = m$ für alle Nachrichten $m < n$. Bei PH ist n eine Primzahl; bei RSA hat n die Form $n = p \cdot q$ für zwei verschiedene Primzahlen p und q.
Was ist der wesentliche Unterschied? Wieso kann man PH nicht als Public-Key-System verwenden?

68.) Schätze die folgenden Funktionen im Sinne der O-Notation durch möglichst einfache Funktionen ab.

$$\frac{3n^3 + 5n}{2n + 1}, \quad 42, \quad 5n^2 + 7 \log n, \quad 7n^2 \log n, \quad 3n\sqrt[3]{2n}, \quad (\log n)^{\log n}, \quad \sqrt{2}^{n/3}, \quad \log(n!)$$