



Übungsblatt 14

Dieses Aufgabenblatt ist nur zur Wiederholung des bereits behandelten Stoffes gedacht. In der Musterlösung werden bei Rechenaufgaben daher nur die korrekten Ergebnisse ohne Lösungsweg angegeben.

Aufgabe 1 (Effiziente Berechnungen)

Sie wollen $51^x \bmod 166879$ für alle $x \equiv 16 \pmod{486}$ mit Hilfe der schnellen Exponentiation berechnen. Gibt es eine Methode, bei der Sie nur zwei schnelle Exponentiationen benötigen?

Aufgabe 2 (ElGamal-Verschlüsselung)

Geben Sie eine vollständige Beschreibung der in Aufgabe 1 der 9. Übung vorgestellten Variante der ElGamal-Verschlüsselung.

Aufgabe 3 (ElGamal-Signatur)

Sei $p = 113$ und $g = 3$. Alice signiert mit dem geheimen Schlüssel $a = 5$.

- Bestimmen Sie ihren öffentlichen Schlüssel.
- Verifizieren Sie die Signatur $(r, s) = (76, 109)$ zur Nachricht m mit $h(m) = 11$.
- Verifizieren Sie die Signatur $(r, s) = (66, 99)$ zur Nachricht m mit $h(m) = 13$.
- Signieren Sie eine beliebige Nachricht, z.B.: $h(m) = 13$ mit zufälligem $k = 5$.

Aufgabe 4 (DL)

Bestimmen Sie den diskreten Logarithmus von

- 30 zur Basis 4 in \mathbb{Z}_{113} .
- $X^3 + X^2 + X + 1$ zur Basis $X^3 + X + 1$ in $\mathbb{F}_2[X]/(X^4 + X + 1)$.

Aufgabe 5 (Faktorisieren)

Faktorisieren Sie 17741.

Aufgabe 6 (RSA)

Sei $(n, e) = (4087, 17)$ der öffentliche Schlüssel von Alice.

- Verschlüsseln Sie 117.
- Alices privater Schlüssel ist $d = 233$. Entschlüsseln Sie die Nachricht $c = 148$.

Aufgabe 7 (RSA)

Sei $(n_a, e_a) = (203, 13)$ der öffentliche RSA-Schlüssel von Alice, und $(n_b, e_b) = (203, 11)$ Bobs öffentlicher RSA-Schlüssel. An beide wurde dieselbe Nachricht gesendet. Sie haben die Schlüsseltexte abgehört. An Alice wurde $c_a = 180$ gesendet, an Bob $c_b = 129$. Wie lautet die Nachricht?

Aufgabe 8 (Signaturen)

Jemand schlägt vor, analog zum RSA-Signaturverfahren ein Rabin-Signaturverfahren zu verwenden. Dazu soll die Signatur eines Dokumentes m eine beliebige Quadratwurzel von $h(m)$ in \mathbb{Z}_n sein, wobei $n = pq$ mit p und q Primzahlen, so daß $p \equiv q \equiv 3 \pmod{4}$.

- Was halten Sie davon?
- Jemand schlägt die folgende Modifikation vor: Die Signatur von m ist (i, s) , wobei $i \in \mathbb{N}$ die kleinste Zahl ist, so daß eine Quadratwurzel von $h(m||i)$ existiert. Der Signaturteil s ist dann eine beliebige Quadratwurzel von $h(m||i)$.

- (c) Jemand schlägt die folgende Modifikation vor: Der Signierer wählt ein zufälliges $r \in \mathbb{Z}_n$ und berechnet die Quadratwurzel s von $h(m||r)$. Falls die Quadratwurzel von $h(m||r)$ nicht existiert, so wählt er ein neues r . Ansonsten ist die Signatur von m dann (r, s) . Ist das System dadurch besser geworden?