Hochschule für
Technik und Wirtschaft
des Saarlandes
University of Applied Sciences

Studiengang Kommunikationsinformatik (Master)
Prof. Dr.–Ing. Damian Weber

Sicherheit und Kryptographie – Übung 3

Schreibweise:
Körper der Größe p^n werden auch mit der Abkürzung $\mathbf{F}_{p^n}$ bezeichnet.

Aufgabe 1 (Erweiterter ggT)

a) Benutzen Sie den erweiterten Euklidischen Algorithmus, um $\frac{1}{30}$ in $\mathbf{F}_{167}$ auszurechnen. Überprüfen Sie das Resultat durch geschicktes Multiplizieren ohne Taschenrechner.

b) Benutzen Sie den erweiterten Euklidischen Algorithmus, um $\frac{1}{X^2+1}$ in

$$\mathbf{F}_{5^3} = \mathbf{F}_5[X]/(X^3 + X + 1) = \mathbf{F}_5(\alpha) \qquad \alpha^3 + \alpha + 1 = 0$$

zu bestimmen.

Aufgabe 2 (Einheiten)

Sei R ein Ring (mit Einselement 1).

Falls $a|1$ so heißt a eine Einheit von R. Die Menge der Einheiten von R wird mit R^* bezeichnet.

a) Zeigen Sie, dass die Einheiten von R eine Gruppe bilden.

b) Finden Sie alle Einheiten von $\mathbf{Z}$.

c) Zeigen Sie, daß $3 + 2\sqrt{2}$ eine Einheit des Rings

$$\mathbf{Z}[\sqrt{2}] = \{c + d\sqrt{2} \mid c, d \in \mathbf{Z}\}$$

ist. Finden Sie unendlich viele Einheiten des Rings $\mathbf{Z}[\sqrt{2}]$.

Aufgabe 3 (Diffie–Hellman–Protokoll in $\mathbf{F}_{2^4}$, Pohlig–Hellman/Shanks)

Alice und Bob bilden den Körper $\mathbf{F}_{2^4}$ mit Hilfe des Polynoms $X^4 + X + 1 \in \mathbf{F}_2[X]$.

Als Erzeuger wählen sie $\gamma = 1 + \alpha$. Alice schickt an Bob die Nachricht $\alpha^3 + 1$. Berechnen Sie den geheimen Exponent von Alice

a) mit Hilfe des Pohlig–Hellman–Verfahrens modulo der Primfaktoren der Gruppenordnung

b) mit Hilfe des Shanks–Baby–Step–Giant–Step Algorithmus modulo der Gruppenordnung

Aufgabe 4 (RSA mit Chinesischem Restsatz)

Die RSA–Entschlüsselungsfunktion (bzw. Signaturfunktion) kann beschleunigt werden, indem man

$$m^d \bmod n$$

durch die Berechnung

$$m_1 \equiv m^d \bmod p \qquad\qquad m_2 \equiv m^d \bmod q$$

ersetzt. Die Werte m_1, m_2 werden durch den Chinesischen Restsatz wieder zu einem Ergebnis mod pq zusammengesetzt.

a) Führen Sie diese Operation am Beispiel $n = 366048528639529$, $m = 1234567890$, $d = 98765432101$ mit Hilfe von GP/PARI aus. Zur Überprüfung der Korrektheit Ihrer Schritte vergleichen Sie das Ergebnis mit dem direkten Berechnen von $m^d \bmod n$.

b) Welcher Laufzeitvorteil wird durch diesen ,,Trick" erzielt?