WOLFGANG K. SEILER A5, C201
Tel. 2515

16. März 2007

4. Übungsblatt Höhere Mathematik I

Fragen: *(je ein Punkt)*
Die Antworten auf die nachfolgenden Fragen sollten nicht länger als etwa zwei Zeilen sein und lediglich eine kurze *Begründung enthalten. Antworten ohne Begründung werden nicht gewertet.*

1) Richtig oder falsch: Für $x, y \in \mathbb{F}_{1024}$ ist $(x+y)^6 = x^6 + y^6$.

2) Richtig oder falsch: Jeder Vektorraum über $\mathbb{F}_2$ ist auch ein Vektorraum über $\mathbb{F}_4$.

3) Richtig oder falsch: $\mathbb{F}_8$ ist ein zweidimensionaler $\mathbb{F}_4$-Vektorraum.

4) Richtig oder falsch: Jeder Vektorraum über $\mathbb{F}_{16}$ ist auch ein Vektorraum über $\mathbb{F}_4$.

5) Richtig oder falsch: Die Abbildung $\varphi\colon \mathbb{F}_{256} \to \mathbb{F}_{256}$ mit $\varphi(x) = x^{16}$ ist $\mathbb{F}_2$-linear.

Problem 1: (*5 points)*
Both *TI unlimited* and `SIT.com` are customers of *THRIFTY PRIMES*; their public keys N, M can be found in the file `aufgabe1.java` on the home page of the course. Both companies use public exponent $e = 3$. True to their name, *THRIFTY PRIMES* only generated three prime numbers p, q, r, setting $N = pq$ and $M = qr$.

a) Find the private exponents of *TI unlimited* and `SIT.com`!

b) Sign the message with numerical value 17 with the private key of `SIT.com`, and encrypt the signature with the public key of *TI unlimited*!

Aufgabe 2: (*5 Punkte)*

a) Zeigen Sie, daß sich jedes von Null verschiedene Element des Körpers $\mathbb{F}_{11}$ als Potenz der Zwei schreiben läßt!

b) Bestimmen Sie ein $n \in \mathbb{N}$, so daß $2^n \equiv 3 \bmod 11$ ist!

c) Finden Sie ein Element $x \in \mathbb{F}^4$ derart, daß jedes von Null verschiedene Element aus $\mathbb{F}_4$ als Potenz von x schreiben läßt!

Aufgabe 3: (*5 Punkte)*
Addition und Multiplikation im Körper $\mathbb{F}_{256}$ seien über das Polynom $P = x^8+x^4+x^3+x+1$ erklärt, und $\alpha \in \mathbb{F}_{256}$ sei so gewählt, daß $P(\alpha) = 0$ ist. Stellen Sie die folgenden Potenzen und Produkte in der Form

$$a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\alpha^5 + g\alpha^6 + h\alpha^7$$

dar:

a) α^{11} *b)* $(1+\alpha^5)(1+\alpha^6)$ *c)* $(1+\alpha+\alpha^2+\alpha^3)^2$ *d)* $(\alpha+\alpha^3+\alpha^4+\alpha^6)^2$

Abgabe bis zum Freitag, dem 23. März 2007, um 12.00 Uhr