RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Jun.-Prof. Roberto Avanzi
Enrico Thomae

Hausübungen zur Vorlesung

Diskrete Mathematik II

SoSe 2010

Blatt 5 / 15. Juni 2010 / Abgabe bis spätestens 29. Juni 2010, 10:00 Uhr

AUFGABE 37 (6 Punkte)**:**
Betrachten Sie das McEliece Verfahren mit öffentlichem Schlüssel G' und privatem Schlüssel S, G, P, wobei G ein linearer $[n, k, d]$-Code ist. Eve bekommt einen Chiffretext $\mathbf{c} = \mathbf{m}G' + \mathbf{e}$ für eine unbekannte Nachricht $\mathbf{m}$.
Um die Nachricht zu entschlüsseln, rät Eve k Spalten. Seien G'_k, $\mathbf{c}_k$ und $\mathbf{e}_k$ die Einschränkungen von G', $\mathbf{c}$ und $\mathbf{e}$ auf diese k Spalten.

(a) Welche Bedingungen müssen G'_k und $\mathbf{e}_k$ erfüllen, damit Eve die Nachricht $\mathbf{m}$ als $\mathbf{c}(G'_k)^{-1}$ entschlüsseln kann?

(b) Wie groß ist die Wahrscheinlichkeit, dass $\mathbf{e}_k$ die geforderte Bedingung erfüllt?

AUFGABE 38 (5 Punkte)**:**
Der Geheimtext $c = (7\ 68\ 16\ 9\ 35\ 54)$ wurde mit dem Goldwasser-Micali Kryptosystem mit den öffentlichen Parametern $(N, a) = (77, 24)$ verschlüsselt. Geben sie alle Schritte an, die zum Entschlüsseln notwendig sind und bestimmen sie den Klartext.
Muss N wirklich (wie in der Vorlesung) eine Blumzahl sein? Welchen Vorteil bringt es Blumzahlen zu verwenden?

AUFGABE 39 (4 Punkte)**:**
Folgender Geheimtext $c = (0\ 0\ 0\ 0\ 0\ 0\ 158)$ wurde mit dem Blum-Goldwasser Kryptosystem mit dem öffentlichem Parameter $N = 209$ verschlüsselt. Geben sie alle Schritte an, die zum Entschlüsseln notwendig sind und bestimmen sie den Klartext.
Muss N wirklich eine Blumzahl sein?

AUFGABE 40 (6 Punkte)**:**
Betrachten Sie die Kurve

$$E_p \ : \ y^2 + xy = x^3 - 2x^2 + x + 3$$

über $\mathbb{F}_p$, wobei p eine Primzahl ist.

(a) Für welche Werte von p ist die Kurve E_p singulär?

(b) Bestimmen Sie für alle anderen Werte von p die Weierstraß-Form von E_p.