Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

SS 2001

Übungen zur Kryptologie II

2. Übung

Aufgabe 1 (2 Punkte)

Konstruieren Sie eine $(25, 6, 5, 1)$-Orthogonalmatrix und eine $(27, 13, 3, 3)$-Orthogonalmatrix.

Aufgabe 2 (2 Punkte)

Angenommen, Sie wollen Nachrichten über dem 26-stelligen Alphabet $\{A, \ldots, Z\}$ der Länge 1000 authentisieren. Wie könnte ein entsprechender Authentikationscode aussehen, falls die Erfolgswahrscheinlichkeit eines Gegners bei Durchführung eines Impersonations- oder Substitutionsangriffs nicht größer als 10^{-4} sein soll?

Aufgabe 3

Überlegen Sie sich, wie sich aus zwei gegebenen $(m_i, n_i, l_i, \lambda_i)$-Orthogonalmatrizen, $i = 1, 2$, eine neue (m, n, l, λ)-Orthogonalmatrix mit $l = l_1 \cdot l_2$ konstruieren lässt. Dabei sei angenommen, dass beide Matrizen dieselbe Anzahl $n = n_1 = n_2$ von Spalten besitzen.