Institut für Informatik
Komplexität und Kryptografie
Prof. Dr. Johannes Köbler

Sommersemester 2004

Übungen zur Kryptologie 2

9. Übung

Aufgabe 1

Ein Dealer-Algorithmus für das (t, n)-Schwellenverfahren von Shamir hat für $t = 5$, $n = 10$ und $p = 31847$ die folgenden Teilschlüssel berechnet.

i	1	2	3	4	5	6	7	8	9	10
x_i	413	432	451	470	489	508	527	546	565	584
y_i	25439	14847	24780	5910	12734	12492	12555	28578	20806	21462

Bestimmen Sie den geheimen Schlüssel k und berechnen Sie (möglichst effizient) den Teilschlüssel y, den ein Teilnehmer mit der x-Koordinate 10000 erhalten würde.

Aufgabe 2

Schreiben Sie ein Programm, welches bei Eingabe von t, n, p, sowie n öffentlichen x-Koordinaten $x_1, \ldots, x_n$ und t y-Koordinaten $y_{i_1}, \ldots, y_{i_t}$, den geheimen Schlüssel k berechnet. Überprüfen Sie ihr Programm mit den Werten aus Aufgabe 1.

Aufgabe 3

Es ist möglich, dass ein unehrlicher Dealer beim Shamirverfahren "schlechte" Teilschlüssel vergibt, das heißt, für unterschiedliche Teilmengen von t Teilschlüsseln ergeben sich unterschiedliche Schlüssel k. Um dies für gegebene n Teilschlüssel zu überprüfen, könnte man für alle $\binom{n}{t}$ Teilmengen (bestehend aus t Teilschlüsseln) den Schlüssel berechnen.
Überlegen Sie sich eine effizientere Möglichkeit, dies zu überprüfen.

Aufgabe 4

Es seien t unterschiedliche Elemente $x_1, \ldots x_t$ eines Körpers gegeben.

$$A = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{pmatrix}$$

Zeigen Sie, dass für die Determinante $\det A$ obiger Matrix A (sog. Vandermonde'sche Matrix) gilt: $\det A = \Pi_{1 \le j < i \le t}(x_i - x_j)$.