Prof. Dr. A. Goerdt
M. Auerbach, A. Lanka

TU Chemnitz
Wintersemester 2006/2007
27.10.2006

Datenschutz und Datensicherheit / Systemsicherheit

3. Übung

1. Aufgabe:

   a) Verschlüsseln Sie die Nachricht $m = 01110011001$ mit Hilfe der (in der Vorlesung vorgestellten) Stromchiffre. Benutzen Sie $n = 4$, $c = (c_1c_2c_3c_4) = (1001)$ und den Startschlüssel $k = (1001)$.

   b) Erklären Sie, warum die erzeugten z_i zyklisch sind. Das heißt: Es gibt ein l und ein i_0, so daß gilt: $z_{i+l} = z_i$ für alle $i \geq i_0$.

   c) Geben Sie eine obere Schranke für l und i_0 (in Abhängigkeit von n) an.

2. Aufgabe:

   a) Zeigen oder widerlegen Sie:
   Wenn $a \cdot c \equiv 1 \pmod{m}$ und $b \cdot c \equiv 1 \pmod{m}$, dann gilt $a \equiv b \pmod{m}$.

   b) Bestimmen Sie zu jeder Zahl $n \in \{1 \ldots 10\}$ das multiplikative Inverse modulo 11, d.h. die Zahl $n' \in \{1 \ldots 10\}$, für die $n \cdot n' \equiv 1 \pmod{11}$ gilt.

3. Aufgabe:

   a) Wir benutzen das Alphabet $\Sigma = \{0, 1, \ldots, 9, A\} \mathrel{\widehat{=}} \{0, 1, \ldots, 9, 10\}$. Entschlüsseln Sie das Chiffrat $c = 04967215A38$. Dabei ist c das Ergebnis der affinen Chiffre mit $a = 5$ und $b = 3$.

   b) Bei einem known-plaintext-Angriff erhält der Angreifer ein oder mehrere (Klartext, Chiffrat)-Paare. Daraus versucht er den (Verschlüsselungs-)Schlüssel zu ermitteln. Sie erhalten das Paar $(29456, 72481)$ und wissen, dass eine affine Chiffre modulo 11 benutzt wurde. Ermitteln Sie den Schlüssel (a, b), der zum Verschlüsseln benutzt wurde.

4. Aufgabe:

   Wir betrachten $a, m \in \mathbb{N}$ und die Zerlegung $a = D \cdot m + R$ mit $0 \leq R < m$.

   a) In welcher Laufzeit können Sie a bestimmen, wenn D, m und R gegeben sind?

   b) In welcher Laufzeit können Sie D und R ermitteln, wenn a und m gegeben sind?