Prof. Dr. A. Goerdt
A. Lanka

TU Chemnitz
Wintersemester 2006/2007
26.01.2006

Datenschutz und Datensicherheit / Systemsicherheit

11. Übung

1. Aufgabe:

   Wir betrachten die Funktion $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ mit $f(b) = b^m \bmod n$. Zeigen Sie, daß je zwei Funktionswerte c_1, c_2 die gleiche Anzahl Urbilder haben.

   Hinweis: Konstruieren Sie aus den Urbildern $b_1, \ldots, b_k$ von c_1 Urbilder für c_2.

2. Aufgabe:

   Wir betrachten das Alphabet $\{A, \ldots, H\} \hat{=} \{0, \ldots, 7\}$. A möchte die Nachricht $BACH$ an B senden. Dazu soll der CFB-Modus verwendet werden. A wählt die Verschlüsselungsfunktion $E(x) = 3^x \bmod 7$, den Initialisierungsvektor $IV = 011$ und $r = 2$.

   a) Welche Daten können öffentlich gemacht werden?

   b) Wie können die nicht-öffentlichen Daten (möglichst einfach) über einen unsicheren Kanal an B gesendet werden?

      Hinweis: 3 ist ein Generator von $\mathbb{Z}_7^*$.

   c) Geben Sie alle Schritte an, die A und B machen müssen, bis B das Chiffrat erhalten hat.

   d) Warum eignet sich obiges Verfahren nicht für den CBC-Modus?

   e) Warum ist das ElGamal-Verfahren weder für den CBC- noch für den CFB-Modus geeignet?