Übung 2

Abgabetermin: 3. November 2011 **vor** der Vorlesung

Anmerkung: Sie haben ausnahmsweise **zwei** Wochen Bearbeitungszeit für dieses Übungsblatt.

1. *Kongruenzen*

   (a) Bestimmen Sie folgenden Kongruenzen mit dem Modulus $m = 29$ ohne Taschenrechner. Die Ergebnisse müssen im Bereich $0, 1, \ldots, m-1$ liegen (10 Pkt.):

   i. $13 \cdot 24 \bmod 29$
   ii. $17 \cdot 1337 \bmod 29$
   iii. $69 \cdot 31 \bmod 29$
   iv. $(-36) \cdot (-28) \bmod 29$
   v. $231 \cdot (-51) \bmod 29$

   (b) Beschreiben Sie kurz den Zusammenhang zwischen den einzelnen vorherigen Rechnungen (5 Pkt.).

   (c) Bestimmen Sie jeweils ohne Taschenrechner (15 Pkt.):

   i. $3^{-1} \bmod 29$
   ii. $2 \cdot 6^{-1} \bmod 23$
   iii. $7 \cdot 3^{-1} \cdot 4 \cdot 9^{-1} \bmod 13$

2. *Reading Assignment*

   Lesen Sie den Artikel “Why cryptography is harder than it looks” von Bruce Schneier. Der Artikel liegt als PDF im Blackboard im Ordner zu Übung 2. (Der Inhalt dieses Textes ist Prüfungsrelevant!)

   Beantworten Sie stichpunktartig die folgenden Fragen (40 Pkt.):

   (a) Warum stehen die Wetten besser für den Angreifer als für den Sicherheitsarchitekten ?

   (b) Bis zu welchem Punkt können Sicherheitsziele durch Kryptographie geschützt werden ?

   (c) Wo liegt das Problem, wenn man feststellen möchte ob ein System sicher ist ?

   (d) Warum reicht es nicht ein sicheres kryptographisches System zu entwickeln ? Was muss noch berücksichtigt werden, damit Dieses System, Daten und Resourcen schützen kann ?

   (e) Warum ist die Marketing-Politik bei entdeckten Sicherheitslücken in kryptographischen Anwendungen nicht detailiert über diese zu informieren problematisch ?

   (f) Was sollte laut Schneier getan werden um kryptographische Anwendungen zukunftssicher zu machen ?

3. *Schiebeverschlüsselung*

Ein alternatives Verfahren zur Substitionschiffre ist die Shift-Verschlüsselung (auch bekannt als Schiebechiffre). Hier wird allerdings anstatt einer beliebigen Zuordnung für jeden Buchstaben (z.B. $A \mapsto T, B \mapsto X, C \mapsto F, \ldots$) lediglich eine Verschiebung des gesamten Alphabets um einen geheimen Offset (Verschiebungswert) vorgenommen. So wird z.B. für den Offset $k = 5$ eine Verschiebung des Alphabets um 5 Zeichen durchgeführt, z.B. $A \mapsto F, B \mapsto G, C \mapsto H, \ldots$ und mit dieser Abbildung der Klartext kodiert.

(a) Gehen Sie davon aus, dass Ihnen das Alphabet $\Sigma = \{A, B, C, \ldots, Z\}$ für Klartext und Chiffrat zu Verfügung steht. Wenn Sie eine Shift-Verschlüsselung mit dem Offset $k = 10$ durchführen, wie müssen Sie sinnvoll die Buchstaben $Q, \ldots, Z$ aus dem Klartext belegen? (5 Pkt.)

(b) Verschlüsseln Sie das Wort "`Datensicherheit`" mit der Shift-Verschlüsselung und dem geheimen Offset $k = 10$. (10 Pkt.)

(c) Wenn Sie die Sicherheit der Shift- und der Substitionschiffre bezüglich statistischen Angriffen vergleichen, ist die Shift-Chiffre sicherer? (5 Pkt.)

(d) Wenn Sie den Offset für jedes Klartextzeichen von einem beliebigen Startpunkt an inkrementieren (jeweils um eins erhöhen), wird dadurch die Sicherheit des Verfahrens gegen statistische Angriffe erhöht? (10 Pkt.)
Hinweis: Zum besseren Verständnis des Verfahrens sei folgendes Beispiel gegeben:

```
Klartext:   i n t e r n e t
Offset:     1 2 3 4 5 6 7 8
Geheimtext: J P W I W T L B
```