Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Dipl.-Ing. Stephan Günther, M.Sc.
Nadine Herold, M.Sc.
Dipl.-Inf. Stephan Posselt

Tutorübung zur Vorlesung Grundlagen Rechnernetze und Verteilte Systeme
Übungsblatt 11 (1. Juli – 5. Juli 2013)

Hinweis: Die mit * gekennzeichneten Teilaufgaben sind ohne Kenntnis der Ergebnisse vorhergehender Teilaufgaben lösbar.

Aufgabe 1 Asymmetrische Kryptographie: El Gamal

In der Vorlesung haben wir DH76 als Beispiel für ein symmetrische Schlüsselaustauschverfahren kennengelernt. Mit Hilfe von DH76 konnten zwei Kommunikationspartner Alice und Bob ein gemeinsames Geheimnis errechnen, welches wiederum als Schlüssel für ein symmetrische Verschlüsselungsverfahren wie RC4 verwendet werden kann.
In dieser Aufgabe wollen wir ein asymmetrisches Verfahren untersuchen, bei dem Alice und Bob jeweils einen privaten und einen öffentlichen Schlüssel besitzen. Sei a der öffentliche und u der private Schlüssel von Alice. Will Bob eine Nachricht an Alice senden, so nutzt er a zur Verschlüsselung seiner Nachricht. Zur Entschlüsselung wird der private Schlüssel u benötigt, den nur Alice kennt. Im Detail funktioniert dies wie folgt:

1. Alice wählt eine große Primzahl p und eine dazu passende primitive Kongruenzwurzel g.
2. Alice wählt ihren privaten Schlüssel $u \in \{0, 1, \ldots, p-1\}$. Dieser bleibt geheim.
3. Alice berechnet $a = g^u \bmod p$.
4. Alice veröffentlicht das Tripel (a, p, g) als ihren öffentlichen Schlüssel.

Bob verfährt analog. Im Anschluss möchte Bob eine Nachricht m an Alice schicken. Diese Nachricht sei eine Dezimalzahl $m \in \{0, 1, \ldots, p-1\}$. Um diese zu verschlüsseln, verfährt Bob wie folgt:

1. Bob besorgt sich den öffentlichen Schlüssel von Alice.
2. Bob wählt gleichverteilt ein $v \in \{0, 1, \ldots, p-1\}$ und berechnet $b = g^v \bmod p$ und $k = a^v \bmod p$. Bei k handelt es sich um einen sog. transienten Schlüssel, welcher zur Verschlüsselung der Nachricht dient.
3. Bob berechnet den Ciphertext $c = km \bmod p$.
4. Bob sendet das Tupel (b, c) an Alice.

Zur Entschlüsselung geht Alice wie folgt vor:

1. Alice berechnet $k^{-1} = b^{-u} \bmod p$.
2. Anschließend kann Alice $m = k^{-1}c \bmod p$ bestimmen.

a)* Weswegen kann Eve aus (b, c) nicht ohne weiteres auf m schließen?

b)* Zeigen Sie, dass $m = k^{-1}c \bmod p$ gilt.
Hinweis: $(x \bmod p)(y \bmod p) \bmod p = xy \bmod p$

Bob möchte nun die binäre Nachricht $m = \texttt{10101111}$ an Alice schicken. Der öffentliche Schlüssel von Alice sei $(a, p, g) = (9, 17, 12)$.

c)* Zerlegen Sie die Nachricht m geeignet in zwei Teilnachrichten m_1,m_2 und berechnen Sie die zugehörigen Ciphertexte c_1,c_2.

d) Geben Sie die beiden Nachrichten an, die Bob an Alice überträgt

e) Zeigen Sie, dass Alice c_1,c_2 mit ihrem privaten Schlüssel $u = 10$ wieder entschlüsseln kann.
Hinweis: $k^{-1} \bmod p = k^{p-2} \bmod p$ wenn p prim ist (Euler).

f)* Wie bewerten Sie El Gamal hinsichtlich der Authentizität der Kommunikationspartner?

g)* Da die Verschlüsselung mittels El Gamal im Vergleich zu symmetrischen Verfahren rechenaufwendig ist, wäre eine Kombination beider Verfahren wünschenswert. Wie könnte solch ein hybrides Verfahren funktionieren?

Aufgabe 2 Kompression: Huffman-Kodierung

Gegeben sei das Alphabet $\mathcal{A} = \{a, b, c, d\}$ und die Nachricht

$$m = \texttt{aabccdacababbbbcbddbbbaababdbcbabdbcadba} \in \mathcal{A}^{40}.$$

a)* Bestimmen Sie die Auftrittswahrscheinlichkeiten $p_{i \in \mathcal{A}}$ der einzelnen Zeichen in m.

b) Bestimmen Sie die den Informationsgehalt $I(p_{i \in \mathcal{A}})$ der einzelnen Zeichen.

c) Die Nachricht m stamme aus einer Nachrichtenquelle X. Bestimmen Sie auf Basis der bisherigen Ergebnisse die Quellenentropie $H(X)$.

d) Bestimmen Sie nun einen binären Huffman-Code C für diese Nachrichtenquelle.

e) Bestimmen Sie die durchschnittliche Codewortlänge von C.

f) Vergleichen Sie die durchschnittliche Codewortlänge von C mit der Codewortlänge eines uniformen[1] Binärcodes.

[1] Ein Code heißt *uniform*, wenn alle Codewörter dieselbe Länge aufweisen.