BERGISCHE UNIVERSITÄT
WUPPERTAL

*Fachbereich C*

**MATHEMATIK & INFORMATIK**

Buhl / Feuerstein

**Internet-Technologien**
(Wintersemester 2005/06)

**Übungsblatt 9**

**Übungsaufgaben:**

1) *VPN*

Informieren Sie sich über VPNs. Quelle:

`http://de.wikipedia.org/wiki/VPN`

Beschreiben Sie in eigenen Worten den Unterschied zwischen Site-to-Site und Remote-Access-VPNs. Wie unterscheiden sich IPsec- und SSL-VPNs voneinander?

2) *IPsec over UDP*

Wann benötigt man in UDP-Pakete gekapselte IPsec-Pakete? Quelle:

`http://www.netigator.de/netigator/live/fachartikelarchiv/ha_artikel/powerslave,id,10015837`

3) *WLAN*

- Was unterscheidet WPA-gesicherte WLAN-Verbindungen von WEP-WLANs? Quelle:

  `http://de.wikipedia.org/wiki/Wi-Fi_Protected_Access`

- Wozu wird in WLANs ein Radius-Server genutzt? Quelle:

  `http://de.wikipedia.org/wiki/RADIUS`

4) *QoS*

Was ist unter QoS zu verstehen? Welche der in

`http://de.wikipedia.org/wiki/Quality_of_Service`

beschriebenen QoS-Merkmale werden in der Internet-Telefonie wichtig?
Wie können sie garantiert werden?

5) *pgp / gpg*

- Was unterscheidet ein gpg *Web of Trust* von der X.509-Zertifizierung eines öffentlichen Schlüssels? Für welche Zwecke reicht ein *Web of Trust* aus, für welche benötigt man eine CA?
- Was ist unter einem hybriden Verschlüsselungsverfahren zu verstehen?
  Weshalb und für welche Zwecke setzt man es beim gpg-codierten E-Mail-Versand ein?
- Wie übertragen Sie eines Ihrer gpg-Schlüsselpaare von einem alten Rechner auf einen neuen, ohne die ganzen Schlüsselringe zu kopieren?
- Wozu kann das in

  `http://www.online-tutorials.net/security/gnupg-gpg-tutorial/tutorials-t-69-124.html#zertifikat-fuer-die-ungueltigkeitserklaerung`

  beschriebene Verfahren eingesetzt werden?

**Praktikumsaufgaben:**

*Pretty Good Privacy (pgp / gpg):*

a) (***Ein Bonuspunkt!***) Schaffen Sie die Voraussetzungen für die gpg-Verschlüsselung von Dateien:

- Erzeugen Sie sich ein RSA Schlüsselpaar (der Länge 2048 Bit) zum Verschlüsseln und Entschlüsseln von Dateien.
- Extrahieren Sie Ihren öffentlichen Schlüssel in eine ASCII-Datei, um ihn bei Bedarf weitergeben zu können.
- Lassen Sie Ihren privaten Schlüssel von einer Kommilitonin oder einem Kommilitonen signieren.
- Importieren Sie Ihren (jetzt fremdsignierten) privaten Schlüssel in Ihren privaten Schlüsselring.
- Besorgen Sie sich die öffentlichen Schlüssel von H.-J. Buhl und P. Feuerstein von deren Homepages und fügen Sie diese Schlüssel Ihrem öffentlichen Schlüsselring zu.
- Kodieren Sie eine Textdatei mit dem öffentlichen Schlüssel von P. Feuerstein und schicken Sie ihm die kodierte Textdatei per eMail.

*Serverseitige Scripts / PHP:*

b) (***Drei Bonuspunkte!***) Erstellen Sie ein PHP-Script für das *Sieb des Eratosthenes*:

Algorithmus:

i) Schreibe die Primzahl-Kandidaten $2, \ldots, n$ auf
ii) Setze $p := 2$
iii) Solange $p^2 \leq n$ wiederhole:
   - ☐ Streiche alle Vielfachen von $p$ aus der Kandidatenliste
   - ☐ Setze $p$ auf den nächstgrößeren noch nicht gestrichenen Kandidaten
iv) Gib die nicht gestrichenen Kandidaten aus. Es handelt sich um die Primzahlen in $\{1, \ldots, n\}$.

Aufgabe:

- Erstellen Sie eine Datei `eratosthenes.html` mit einem Formular mit zwei *select*–Elementen für

  die Höhe $h$ (Anzahl der Zeilen), zulässige Werte: $1, \ldots, 15$ , und
  die Breite $b$ (Anzahl der Spalten), zulässige Werte: $5, \ldots, 15$ , einer Tabelle.

  Diese Parameter sollen dann mittels der *get*-Methode an eine Datei `eratosthenes.php` übergeben werden.
- Erstellen Sie eine Datei `eratosthenes.php` mit einer Tabelle der übergebenen Höhe und Breite, in der die Zahlen $1, \ldots, n := hb$ aufgelistet sind.
  Durch wiederholtes Klicken auf einen *Weiter*-Button sollen dann sukzessive die Vielfachen von $2, 3, 5, \ldots$ solange gestrichen werden, bis der Algorithmus terminiert.
- Integrieren Sie die beiden Dateien in Ihre Website.

*Hinweis:* Praktikumsaufgabe a) ist von *jeder* an den Übungen teilnehmenden *Person* durchzuführen. Ein Lösungsbeispiel für Aufgabe b) findet sich unter der URL

`http://www-share.math.uni-wuppertal.de/Eratosthenes/`

***Ende der Bearbeitungszeit:*** 31. Januar 2006