# – Praktikumsaufgabe 3 –

## Thema: *Kryptografische Hashes*

**Zielstellung:** Erarbeitung praktischer Aspekte der Nutzung kryptografischer Hashfunktionen (Werkzeuge, deren Leistungsfähigkeit, prinzipielle Sicherheit), Einführung in die OpenSSL-Bibliothek

1. Ein sehr einfacher Hash wäre eine XOR-Funktion über alle Bytes der Nachricht. Zeigen Sie, dass dies kein guter kryptografischer Hash ist.

2. Überzeugen Sie sich programmtechnisch, dass MD5 bei Änderung eines Bits der Klartextnachricht im Mittel die Hälfte aller Bits im Hash ändert! Nutzen Sie als Vorlage das Gerüst `testmd5-geruest.c`.

3.* Vergleichen Sie SHA-1 (`sha1sum`), SHA-224 (`sha224sum`), SHA-512 (`sha512sum`), MD5 (`md5sum`) und `cksum` hinsichtlich

   a) ihrer Performance und

   b) der theoretischen Dauer der Ermittlung einer Kollision zu einem gegebenen Hash (Brute-Force-Angriff).

   Verschlüsseln Sie für die Leistungsbewertung Dateien verschiedener Länge und messen Sie die benötigte Dauer (z. B. mit dem Kommando `time`).

4.* Implementieren Sie ein Werkzeug, das den MD2-Hash einer von `stdin` eingelesenen Zeichenkette berechnet und ausgibt. Nutzen Sie ausnahmsweise *nicht* die OpenSSL-Bibliothek. Schauen Sie sich den RFC 1319 und dessen Errata genau an. Vergleichen Sie die Geschwindigkeit mit den oben vermessenen Verfahren. Anmerkung: Wegen mehrerer Probleme ist MD2 heutzutage nur noch von historischem Interesse; der Algorithmus ist jedoch so simpel, dass man ihn in wenigen Zeilen Code implementieren kann.

   **Literatur:**

   - *http://www.ietf.org/rfc/rfc1319.txt*
   - *http://www.rfc-editor.org/errata_search.php?rfc=1319*[1]
   - *http://www.rfc-editor.org/info/rfc6149*

5. Analysieren Sie den Quelltext `hash.c`. Was macht das Programm? Modifizieren Sie den Quelltext so, dass MD5 anstatt SHA-1 genutzt wird.

   **Hinweise:**

[1] Ja, in der Tat; der RFC weist einen kleinen, aber umso hinterhältigeren Fehler auf. Vielen Dank an Herrn Marco Ziebell, der dies entdeckte.

- Diese Aufgabe sollten Sie *unbedingt* bearbeiten; sie dient der unmittelbaren Vorbereitung auf den Beleg.
- Das Programm nutzt die OpenSSL-Bibliothek. Informationen zu den einzelnen Funktionen finden Sie auf dem Wiki[2] des Projektes sowie in den entsprechenden Manual-Seiten.
- Viele Beispielprogramme befinden sich im zugehörigen Quellpaket, das Sie unter *http://www.openssl.org/source/* finden. Diese sind für das Bearbeiten der Aufgabe jedoch nicht zwingend nötig.
- Sie müssen alle OpenSSL-Programme mit dem Schalter `-lcrypto` linken!

[2] (*https://wiki.openssl.org/index.php/Main_Page*)