

### Aufgabe 1 (Güte einer HashFunktion)

Gegeben sei die folgende HashFunktion:

```
hashwert = 42;
for (i = nachricht.length; i >= 0; i)
    hashwert = (hashwert + nachricht[i]) % (2^32);
return hashwert;
```

Dabei ist hashwert ein 32 bit integer, und nachricht[i] das i-te byte der Nachricht als 8bit integer. Ist diese HashFunktion sicher? Begründen Sie ihre Antwort.

Eine Hash-Funktion gilt als sicher, wenn Kollisionen "unmöglich" sind, also nicht mit einfachen Mitteln bewerkstelligt werden können. Die hier vorliegende Funktion ist sehr simpel; bereits durch einfaches Umstellen von Buchstaben ist eine Kollision verursachbar. Daher ist diese Hash-Funktion unsicher.

### Aufgabe 2 (Kollisionen bei HashFunktionen)

Gegeben sei eine HashFunktion, die 64 000 000 unterschiedliche HashWerte erzeugen kann, z.B. Zahlen aus dem Intervall 0 .. 63 999 999.

a) Weiterhin sei eine Nachricht N mit HashWert H(N) gegeben. Wieviele Nachrichten müssen sie erzeugen, um mit einer Wahrscheinlichkeit größer als  $\frac{1}{2}$  eine Nachricht mit demselben HashWert H(N) zu erhalten?

Die Formel ergibt sich daraus, dass ein erster Hash-Wert durch einen beliebigen Satz gebildet wird und dann nur noch ein zweiter Satz gefunden werden muss, der den gleichen Hash-Wert ergibt. Die Formel dazu lautet:  $1/2 \geq (63.999.999/64.000.000)^n \Rightarrow \lg(1/2) \geq n \cdot (63.999.999/64.000.000) \Rightarrow \lg(1/2) / \lg(63.999.999/64.000.000) = n = 44.361.419,20 \dots$  Versuche

b) Wie viele zufällige verschiedene Nachrichten müssen Sie erzeugen, damit mit einer Wahrscheinlichkeit größer als  $\frac{1}{2}$  mindestens zwei (beliebige) dieser Nachrichten denselben HashWert haben?

Ein Programm von Wikipedia zur Lösung des Problems auf Basis des Geburtstagsparadoxons:

```
#include <stdio.h>
int main ( )
{
    int n=1;
    double q=1;

    while ( q >= 0.5 )
    {
        q *= ( 365 - n + 1 ) / ( double ) 365;
        n ++;
        printf ( "n=%d P=%f\n", n-1, 1-q );
    }

    return 0;
}
```

### Aufgabe 3 (Zertifikate)

Digitale Zertifikate werden auf ECommerce Web sites zur Authentisierung der Server eingesetzt. Finden Sie heraus, wie man in ihrem meistgenutzten Web Browser die Zertifikate von Servern anschauen kann.

Bei welcher Certification Authority haben die folgenden Firmen ihre ServerZertifikate erstellen lassen und welchen Fingerprintheben die Zertifikate?

- a) Deutsche Bank
- b) Amazon.de
- c) gmx.net
- d) Virtuelle Universität der FernUni Hagen

Deutsche Bank: Verisign, Inc., VeriSign Trust Network

Amazon: Verisign, Inc., RSA Data Security, Inc.

gmx.net: Thawte Consulting cc, Thawte Premium Server CA

Fernuni Hagen: FernUniversitaet in Hagen, Zentrum fuer Medien und IT

### Aufgabe 4

Welche von der Regulierungsbehörde zugelassenen Stellen zur Erstellung von signaturgesetzkonformen Zertifikaten gibt es zur Zeit?

In der Liste ueber den Link

[http://www.bundesnetzagentur.de/enid/40b4a8a1268aa452df071a0bb4b7da09,0/Elektronische\\_Signatur/Zertifizierungsdiensteanbieter\\_ph.html](http://www.bundesnetzagentur.de/enid/40b4a8a1268aa452df071a0bb4b7da09,0/Elektronische_Signatur/Zertifizierungsdiensteanbieter_ph.html) ersichtlich

### Aufgabe 5

a) Arbeiten Sie das Dokument **sinnundzweckdigitalersignaturen.pdf** aus dem Verzeichnis **/home/daten/skripte/skripte/bachelor/betriebssysteme\_netze\_2/WS0607/material/** durch.

b) Welche MD5 und welche SHA1Prüfsumme hat die Datei?

MD5: 4C 8C BB 47 C4 5B 26 A3 96 A1 C0 8E 50 BE 7F 0E

SHA-1: C9 03 73 CE 02 64 58 F2 E1 1D C3 28 79 46 56 58 40 AB D6 93

Unter Linux mit den Befehlen md5sum und sha1sum.