htw saar

Studiengang Kommunikationsinformatik (Master)
Studiengang Praktische Informatik (Master)
Prof. Dr.–Ing. Damian Weber

Sicherheit und Kryptographie – Übung 1

Vorbemerkungen:

- Stellen Sie sicher, dass Sie Zugang zu einem Computer mit OpenSSL und PARI/GP haben, zum Beispiel `isl-s-01.htwsaar.de`
- Abgabe einer Lösung beinhaltet das Erstellen einer Webseite und das Senden der entsprechenden URL an den Dozenten.

Aufgabe 1 (OpenSSL (Hashes, Dictionary))

Auf der Homepage der Veranstaltung befindet sich eine Kopie des Indexes des DE–Wiktionary.

Bilden Sie mit Hilfe von OpenSSL für alle Begriffe die MD5–, SHA-1– und SHA-256–Hashwerte und versuchen Sie, insgesamt drei dieser Hashwerte mit Hilfe der Suchmaschine Google auf einer Webseite aufzufinden. Notieren Sie die Gesamtzeit für die Erstellung der Hashwerte pro Hashverfahren.

(Nebenbemerkung: verwenden Sie in neuentwickelten Anwendungen niemals MD5, vermeiden Sie SHA-1, stattdessen setzen Sie auf die Sicherheit von SHA-256, SHA-512 und SHA-3 (Keccak))

Aufgabe 2 (GP/PARI und RSA)

Erzeugen Sie ein in der Praxis verwendbares Beispiel von RSA Parametern. In Klammern sind die in `gp` aufzurufenden Funktionen angegeben. Schauen Sie sich dabei für jede Funktion (z.B. `func()`) den zugehörigen Hilfetext an (mittels `?func`). Zahlen z mod n stellen Sie als $Mod(z, n)$ dar, damit während der Arithmetik die Zwischenergebnisse klein gehalten werden können.

a) Wählen Sie zufällige 500-bit-Primzahlen p, q (`random(), nextprime()`).

b) Berechnen Sie n.

c) Berechnen Sie $\varphi(n)$. (nicht `eulerphi()` benutzen, nur deren Beschreibung lesen (warum?))

d) Wählen Sie $e = 2^{16} + 1$ und berechnen Sie d.

e) Verschlüsseln Sie die Nachricht $m = 111 \ldots 1$ (100 Einsen).

f) Entschlüsseln Sie die verschlüsselte Nachricht und überprüfen Sie das Ergebnis.