Universität des Saarlandes
FR 6.2 Informatik

Prof. Dr. Kurt Mehlhorn, Adrian Neumann **WiSe 2013/2014**

Übungen zu Ideen der Informatik

http://www.mpi-inf.mpg.de/departments/d1/teaching/ws13/ct/

Blatt 5 Abgabeschluss: 25.11.13

Aufgabe 1 (*10 Punkte*) Betrachten Sie den folgenden mit dem Caesar-Verfahren verschlüsselten Text:

`hfme tqjfmu lfjof spmmf`

a) Entschlüsseln Sie den Text.

b) Nehmen Sie an, wir verwenden das One-Time Pad in einer etwas modifizierten Version. Statt einen Schlüssel mit der selben Länge wie der Ausgangstext zu verwenden, benutzen wir einen Schlüssel, der viel kürzer ist als der Klartext (zum Beispiel 10 Zeichen lang). Wie kann man so eine Verschlüsselung überwinden?

Aufgabe 2 (*10 Punkte*)

a) Diskutieren Sie, ob man nur die Dinge verschlüsseln muss, die Schaden verursachen, wenn sie publik werden (wie etwa Bankdaten, Pläne für Demonstrationen etc.).

b) Nehmen Sie an, der gesamte Internetverkehr sei verschlüsselt. Was kann man durch Abhören des Internets noch über die Nutzer lernen?

Aufgabe 3 (*10 Punkte*) Spielen Sie Baby ElGamal mit folgenden konkreten Zahlen durch: $p = 5793$, $f = 5832$, $m = 354834$, und $s = 457$.

Aufgabe 4 (*9+ (Bonus-) Punkte*) Thunderbird-Nutzer möchten für diese Aufgabe vielleicht Enigmail installieren.

a) (4+$\lceil\sqrt{x}\rceil$ Punkte) Installieren sie GPG und erstellen Sie einen Schlüssel. Suchen Sie sich x Studenten oder Tutoren, die auch einen Schlüssel haben, weisen Sie sich aus und lassen Sie ihren Schlüssel signieren. Machen Sie ihren Schlüssel auf dem Keyserver sks-keyservers.net publik.

b) (5 Punkte) Schreiben Sie eine verschlüsselte und signierte E-Mail an Adrian.

Kryptographie war ☐ spannend ☐ okay ☐ langweilig
☐ schwierig ☐ okay ☐ einfach