Universität des Saarlandes
FR 6.2 Informatik

Prof. Dr. Kurt Mehlhorn, Adrian Neumann **WiSe 2014/2015**

Übungen zu Ideen der Informatik

http://resources.mpi-inf.mpg.de/departments/d1/teaching/ws14/Ideen-der-Informatik/

Blatt 7 Abgabeschluss: 15.12.14

Aufgabe 1 (*15 Punkte*) Betrachten Sie den folgenden mit dem Caesar-Verfahren verschlüsselten Text:

hfme tqjfmu lfjof spmmf

a) Entschlüsseln Sie den Text und nennen Sie den verwendeten Schlüssel.

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 (*5 Punkte*) Spielen Sie Baby ElGamal mit folgenden konkreten Zahlen durch:

$$p = 5793,\ f = 5832,\ m = 354834, \text{ und } s = 457.$$

Aufgabe 3 (*5 Punkte*) Diskutieren Sie Vor- und Nachteile der folgenden Passwörter.

mylaptop	26101949
semi49rundinaria	Ie90%dÄf7E!
Ich esse 90% der Äpfel für 7 Euro!	braun froh identisch Schauspieler

Aufgabe 4 (*5 Punkte*) Diskutieren Sie, ob man nur die Dinge verschlüsseln muss, die Schaden verursachen, wenn sie publik werden (wie etwa Bankdaten, Pläne für Demonstrationen etc.).