Privatdozent Dr. C. Diem
diem@math.uni-leipzig.de
http://www.math.uni-leipzig.de/∼diem/krypto

KRYPTOGRAPHIE
ÜBUNGSBLATT NR. 2

Aufgabe 1 Gilt die folgende Aussage:
Ein Verschlüsselungssytem (wie in §3 der Vorlesung) ist genau dann perfekt sicher, wenn für jede zufällige Nachricht m und entsprechenden zufälligen Chiffriertext $c := \mathcal{E}nc_k(m)$ gilt: Für je zwei Chiffriertexte $c^{(1)}, c^{(2)} \in \mathcal{C}$ ist $\mathbb{P}[c = c^{(1)}] = \mathbb{P}[c = c^{(2)}]$.

Aufgabe 2 Für wieviele gesendete Zeichen sind die folgenden Verfahren perfekt sicher? Caesar, Mono-Substitution, Vigenère.

Aufgabe 3 Wir betrachten ein one-time pad der Länge ℓ. Wenn nun der Schlüssel 0^ℓ ist, wird der Klartext unverschlüsselt gesendet. Man könnte nun sagen, dass dies eine Sicherheitslücke ist und man deshalb nur pads $\neq 0^\ell$ verwenden sollte (die dann wiederum unform generiert werden).

a) Ist das resultierende Verfahren perfekt sicher?

b) Wie beurteilen Sie die Aussage bezüglich der Sicherheitslücke? Welches Verfahren ist Ihrer Meinung nach besser bei einer praktischen Verwirklichung (mit einem physikalischen Zufallszahlgenerator zur Erzeugung des pads)?

Aufgabe 4 Geben Sie eine Definition von "perfekt sicher bis auf die Länge" an. Das folgende Verfahren sollte dann (in einem geeigneten mathematischen Modell) die Definition erfüllen:
Man tauscht ein zufälliges pad der Länge ℓ. (Das pad nehmen wir als uniform zufällig erzeugt an.) Dann verschlüsselt man Nachrichten einer beliebigen Länge $\ell' \leq \ell$ hiermit mit bitweisem XOR und verschickt dann den resultierenden String der Länge ℓ'. Die Entschlüsselung ist identisch zur Verschlüsseung.