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

KRYPTOGRAPHIE
ÜBUNGSBLATT NR. 5

Aufgabe 1 Wir haben den Begriff von (t, ϵ)-sicher (bezüglich eines Angriffsszenarios). Entsprechend können wir die Ausgabe eines Bit-Generators (t, ϵ)-ununterscheidbar von einen "echt zufälligen" nennen.

a) Wie sollte hiervon die Definition lauten?

b) Wie kann man dann die "konkreten Sicherheitsresultate" bezüglich Bit-Generatoren und entsprechenden Stromchiffren formulieren?

Aufgabe 2 Es sei $\mathcal{G}$ ein Pseudozufallsgenerator, k polynomiell in n und $\leq \ell$ (=Ausgabelänge)
Zeigen Sie: Für alle PPT-Algorithmen $\mathcal{A}$ gilt mit $\mathcal{G}(s) = w_1 w_2 \dots w_k \dots$ (und s in $\{0,1\}^n$ uniform):

$$\mathbf{P}[\mathcal{A}(1^n, w_1 \dots w_{k-1}) = w_k] - \frac{1}{2}$$

ist vernachlässigbar (in n).

Also inhaltlich: Man kann das nächste Bit nicht effizient vorherberechnen.

Geben Sie auch ein konkretes Sicherheitsresultat an.