Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 2 / 8./10. November 2010

Für die erste Aufgabe ist folgende Definition von *vernachlässigbar* hilfreich, deren Äquivalenz zur Definition aus der Vorlesung wir auf dem Hausaufgabenzettel beweisen.

Definition 1. Eine Funktion $f : \mathbb{N} \to \mathbb{N}$ heißt *vernachlässigbar*, wenn für jede Konstante $c \in \mathbb{R}, c > 0$ ein $N = N(c) \in \mathbb{N}$ existiert, so dass $f(n) < n^{-c}$ für alle $n > N$ gilt.

AUFGABE 1. Vernachlässigbares.
Entscheiden Sie, welche der folgenden Funktionen vernachlässigbar sind. Begründen Sie Ihre Antwort.

a) $2^{-\log^2 n}$

b) 0.99^n

c) $2^{-100} n^{-1}$

d) $2^{-\sqrt{n}}$

Hinweis: Für vernachlässigbare Funktionen können Sie beispielsweise eine konkrete Wahl für $N(c)$ aus der obigen Definition angeben. Für nicht-vernachlässigbare Funktionen reicht es, ein $c \in \mathbb{R}$ anzugeben, welches die Definition widerlegt.

Wir definieren ein Spiel $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,b)$ exakt wie das $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$-Spiel aus der Vorlesung wobei nun ein *festes* b (anstelle eines zufälligen) verwendet wird. Außerdem bezeichnen wir $\mathcal{A}$'s Ausgabe b' mit $\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,b))$. Hiermit definieren wir folgende alternative Definition für die Ununterscheidbarkeit von Verschlüsselungen gegenüber KPA.

Definition 2. Ein symmetrisches Verschlüsselungsverfahren Π besitzt *ununterscheidbare Chiffretexte gegenüber KPA*, wenn für jeden ppt-Angreifer $\mathcal{A}$ gilt

$$\left|\mathbf{Ws}\left[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,1))=1\right]-\mathbf{Ws}\left[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,0))=1\right]\right|\leq \mathsf{negl}(n)\ .$$

AUFGABE 2. Definitionssache.
Zeigen Sie, dass die obige Definition die Definition aus der Vorlesung (siehe Folie 31) impliziert.

Hinweis: Zeigen Sie hierzu zunächst, dass

$$\mathbf{Ws}\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)=1\right]=\frac{1}{2}+\frac{1}{2}\cdot\left(\mathbf{Ws}\left[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,1))=1\right]-\mathbf{Ws}\left[\mathsf{out}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,0))=1\right]\right)$$

gilt.

AUFGABE 3. Pseudozufall.

a) Sei $G:\{0,1\}^{n/2}\to\{0,1\}^{n+1}$ ein Pseudozufallsgenerator (kurz PRG). Betrachten Sie nun $G':\{0,1\}^{n}\to\{0,1\}^{n+1}$ mit $G'(s)=G(s_1,\ldots,s_{n/2})$ für einen Seed $s=(s_1,\ldots,s_n)$ der Länge n. Beweisen Sie, das auch G' ein PRG ist, indem Sie aus einem Unterscheider für G' einen Unterscheider für G konstruieren.

b) Sei $G:\{0,1\}^{n}\to\{0,1\}^{n+1}$ ein PRG. Definiere $G'':\{0,1\}^{n/2}\to\{0,1\}^{n+1}$ durch $G''(s):=G(0^{n/2}s)$ für einen Seed $s=(s_1,\ldots,s_{n/2})$. Zeigen Sie, dass G'' im Allgemeinen kein Pseudozufallsgenerator ist!

   Hinweis: Verwenden Sie Teil a) um Teil b) zu lösen.