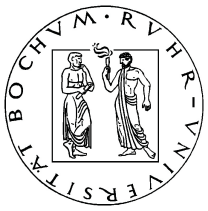
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Präsenzübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 2 / 30. Oktober 2009 / Abgabe 9. November 2009, 12 Uhr

AUFGABE 1 (5 Punkte)**:**
Die Vorraussetzungen seien wie in der Präsenzübung, Zettel 2, Aufgabe 1. Sie möchten Geheimnisse schützen, die mindestens 22 Jahre lang vor einem Gegner, der jedes Jahr 1 Milliarde EU für Computer ausgeben kann, geheim bleiben sollen. Hierfür wollen sie ein Kryptosystem, welches auf der Schwierigkeit des Faktorisierungsproblems beruht, konstruieren.

- Wieviele Rechenoperationen kann Ihr Gegner in den 22 Jahren ausführen ?
- Würden Sie 512, 1024, 2048, 3072 oder 4096 für n empfehlen ?

AUFGABE 2 (5 Punkte)**:**
Beweisen Sie die Äquivalenz der folgenden Definitionen:

Definition 1. *Ein* private-key-*Verschlüsselungsschema* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *besitzt* ***ununterscheidbare Verschlüsselungen gegenüber KPA*** *wenn für jeden* ppt $\mathcal{A}$ *gilt, dass*

$$\mathsf{Ws}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \leq \frac{1}{2} + \mathsf{negl}(n)$$

wobei die Wahrscheinlichkeit über die zufälligen Münzwürfe von $\mathcal{A}$ *und dem Spiel* $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ *berechnet wird.*

Definition 2. *Sei* $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,b)$ *wie üblich definiert, wobei jedoch ein festes* b *(statt eines zuälligen) verwendet wird. Die Ausgabe von* $\mathcal{A}$ *in dem Spiel* $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,b)$ *wird mit* $\mathsf{output}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi})$ *bezeichnet.*
Ein private-key-*Verschlüsselungsschema* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *besitzt* ***ununterscheidbare Verschlüsselungen gegenüber KPA*** *wenn für jeden* ppt $\mathcal{A}$ *gilt*

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

AUFGABE 3 (5 Punkte)**:**
Angenommen, Sie hätten einen Algorithmus, der aus einem zufälligen 16-Bit-String x einen pseudozufälligen 64-Bit-String generiert. Sie wissen nun, dass die Teilstrings $x_0 \dots x_{15}$, $x_{16}, \dots, x_{31}$, $x_{32}, \dots x_{47}$ und $x_{48}, \dots, x_{64}$ alle die gleiche Anzahl von Einsen wie x enthalten werden.
Konstruieren sie einen Unterscheidungsalgorithmus, der mit einer Fehlerwahrscheinlichkeit von weniger als 2^{-64} den Pseudozufallsgenerator von "echtem" Zufall unterscheidet.

AUFGABE 4 (5 Punkte)**:**
Sei G ein Pseudozufallsgenerator mit $|G(s)| > 2|s|$. Definiere $G'(s) = G(s_1, \dots s_{n/2})$ mit $s = s_1, \dots s_n$. Ist G' notwendigerweise auch ein Pseudozufallsgenerator ?