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

Präsenzübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 3 / 22./24. November 2010

AUFGABE 1. Unter Strom.
Wir betrachten die Konstruktion „Stromchiffre“ und den zugehörigen Sicherheitsbeweis aus der Vorlesung (siehe Folie 44 ff) mit folgender spezieller Wahl für G. Sei $G : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$ ein Pseudozufallsgenerator mit Expansionsfaktor $\ell(n) > 4n$. Wir definieren ein symmetrisches Verschlüsselungsverfahren $\Pi_{s_2} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Sicherheitsparameter 1^n für Nachrichten der Länge $\frac{\ell(n)}{2}$ wie folgt.

$\mathsf{Gen}(1^n)$: Wähle $k \in_R \{0,1\}^n$.

$\mathsf{Enc}_k(m)$: Zur Nachricht $m = (m_1, \ldots, m_{\frac{\ell(n)}{2}}) \in \{0,1\}^{\frac{\ell(n)}{2}}$ berechne $c = (c_1, \ldots, c_{\frac{\ell(n)}{2}}) \in \{0,1\}^{\frac{\ell(n)}{2}}$ mit

$$c_i := G(k)_{2i} \oplus m_i$$

für $i = 1, \ldots, \frac{\ell(n)}{2}$ wobei $G(k)_{2i}$ das $2i$-te Ausgabebit von $G(k)$ bezeichnet.

$\mathsf{Dec}_k(c)$: Aus $c = (c_1, \ldots, c_{\frac{\ell(n)}{2}}) \in \{0,1\}^{\frac{\ell(n)}{2}}$ berechne $m = (m_1, \ldots, m_{\frac{\ell(n)}{2}}) \in \{0,1\}^{\frac{\ell(n)}{2}}$ mit

$$m_i := G(k)_{2i} \oplus c_i$$

für $i = 1, \ldots, \frac{\ell(n)}{2}$.

Beweisen Sie die KPA-Sicherheit von Π_{s_2} auf zwei verschiedene Arten.

a) Betrachten Sie $G' : \{0,1\}^n \rightarrow \{0,1\}^{\frac{\ell(n)}{2}}$ mit $s \mapsto G(s)_{2i}$ für $i = 1, \ldots, \frac{\ell(n)}{2}$ und zeigen Sie, dass G' ein Pseudozufallsgenerator ist, d.h. konstruieren Sie aus einem Unterscheider $\mathcal{D}'$ für G' einen Unterscheider $\mathcal{D}$ für G. Begründen sie damit die KPA-Sicherheit.

b) Beweisen Sie die KPA-Sicherheit *direkt*, indem Sie den Beweis zur „Stromchiffe “(Folie 45 ff) immitieren, d.h. konstruieren Sie aus einem KPA-Angreifer $\mathcal{A}$ einen Unterscheider $\mathcal{D}$ für G.

AUFGABE 2. Zu wenig Zufall.
Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein KPA-sicheres, symmetrisches Verschlüsselungsverfahren mit deterministischer Verschlüsselungsfunktion Enc. Aus der Vorlesung wissen wir, dass Π dann nicht mult-KPA sicher sein kann. Betrachten Sie folgende randomisierte Variante Π^{rand} von Π mit

$$\mathsf{Enc}_k^{\mathsf{rand}}(m) := \mathsf{Enc}_k(r||m)$$

für $r \in \{0,1\}^2$ und $m \in \{0,1\}^{n-2}$ und

$$\mathsf{Dec}_k^{\mathsf{rand}}(c) := (\mathsf{Dec}_k(c)_3, \ldots, \mathsf{Dec}_k(c)_n)$$

wobei $\mathsf{Dec}(c)_i$ das i-te Bit der Ausgabe von Dec bezeichnet.

a) Ist Π^{rand} nun mult-KPA-sicher? Beweisen Sie die Sicherheit oder geben Sie einen Angreifer $\mathcal{A}$ an.

b) Ist das Verfahren CPA-sicher?

AUFGABE 3. Auf die Länge kommt es an.
In der Vorlesung betrachten wir nun auch Verschlüsselungsverfahren, die für Nachrichten $m \in \{0,1\}^*$ beliebiger Länge anwendbar sind. Wenn man solche Verschlüsselungsverfahren betrachtet, so muss man in der Definition der KPA-Sicherheit die zusätzliche Forderung $|m_0| = |m_1|$ stellen, d.h. die Challenge-Nachrichten von $\mathcal{A}$ müssen gleichlang sein.

Zeigen Sie, wieso man diese Forderung nicht weglassen darf. Konstruieren Sie hierzu einen KPA-Angreifer $\mathcal{A}$, der das Verfahren bricht, indem er zwei geeignete Nachrichten m_0, m_1 unterschiedlicher Länge verwendet.

Hinweis: Wählen Sie $m_0 \in_R \{0,1\}$ und $m_1 \in_R \{0,1\}^{p(n)+2}$ wobei $p(n)$ ein Polynom ist, welches die Laufzeit von Enc beschränkt, wenn *ein* Bit verschlüsselt wird. Zeigen Sie dann zunächst, dass für eine zufällig gewählte Nachricht $m_1 \in_R \{0,1\}^{p(n)+2}$ mit Wahrscheinlichkeit mindestens $\frac{1}{2}$ gilt, dass $|\mathsf{Enc}_k(m_1)| > p(n)$. Kann man damit nun einen KPA-Angreifer konstruieren?