Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Dr. Christopher Wolf
Alexander Meurer

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 2

SS 2010

Blatt 1 / 14. April 2010 / Abgabe 26. April, 10:00 Uhr, Kasten NA 02

AUFGABE 1. Gruppendiskussion. (6 Punkte)

a) Geben Sie ein Beispiel für eine (nicht notwendig multiplikative) zyklische Gruppe an, in der das CDH-Problem leicht ist.

b) Sei $\mathcal{G}$ eine zyklische Gruppe primer Ordnung q und sei g ein Generator von $\mathcal{G}$. Zeigen Sie, dass

   i) $\mathbf{Pr}_{x_1,x_2 \in_R \mathbb{Z}_q}[\mathsf{DH}_g(g^{x_1}, g^{x_2}) = 1] = \frac{2}{q} - \frac{1}{q^2}$

   ii) $\mathbf{Pr}_{x_1,x_2 \in_R \mathbb{Z}_q}[\mathsf{DH}_g(g^{x_1}, g^{x_2}) = y] = \frac{1}{q} - \frac{1}{q^2}$ für jedes $y \in \mathcal{G} \setminus \{1\}$

   Hierbei ist $\mathsf{DH}_g(g^{x_1}, g^{x_2}) = g^{x_1 \cdot x_2 \mod q}$. Vergleichen Sie die Verteilung von DH_g mit der Gleichverteilung auf $\mathcal{G}$ und interpretieren Sie Ihre Beobachtung in Bezug auf die Härte des DDH-Problems.

c) Zeigen Sie, dass die Härte des CDH Problems relativ zu $\mathcal{G}$ die Härte des diskreten Logarithmus DLog relativ zu $\mathcal{G}$ impliziert.

AUFGABE 2. Schlamüssel. (2 Punkte)
Betrachten Sie das folgende Schlüsselaustausch Protokoll:

1. Alice wählt zufällig $k, r \xleftarrow{R} \{0,1\}^n$ und sendet $s := k \oplus r$ an Bob.
2. Bob wählt zufällig $t \xleftarrow{R} \{0,1\}^n$ und sendet $u := s \oplus t$ an Alice.
3. Alice berechnet $w := u \oplus r$ und sendet w an Bob.
4. Alice gibt den Schlüssel k aus und Bob berechnet den Schlüssel als $w \oplus t$.

Zeigen Sie, dass Alice und Bob denselben Schlüssel berechnen. Analysieren Sie die Sicherheit des Protokolls, d.h. beweisen Sie entweder die Sicherheit oder geben Sie einen konkreten Angriff an.

AUFGABE 3. Null Problemo. (4 Punkte)
Beurteilen Sie, ob das folgende Problem schwer ist:

> Sei p eine Primzahl und $x \in \mathbb{Z}_{p-1}^*$.
> Gegeben p, x und $y := g^x \bmod p$
> wobei g ein zufälliger Wert zwischen 1 und $p-1$ ist.
> Finde g, d.h. berechne $y^{\frac{1}{x}} \bmod p$.

Halten Sie das Problem für schwer, dann zeigen Sie, dass das Problem mindestens so schwer ist wie eines der in der Vorlesung betrachteten schweren Probleme. Sollte das Problem einfach sein, dann geben Sie einen Algorithmus zur Lösung an, verifizieren seine Korrektheit und analysieren die Laufzeit.

Exkurs Semantische Sicherheit bei einem passiven Angreifer

Ein symmetrisches Verfahren Π besteht aus drei Algorithmen Gen, Enc und Dec zur Schlüsselerzeugung, Verschlüsselung und Entschlüsselung. Wir betrachten das folgende Spiel $PrivK^{eav}_{\mathcal{A},\Pi}(n)$:

1. Der Angreifer $\mathcal{A}$ erhält den Sicherheitsparameter 1^n und gibt zwei Nachrichten m_0, m_1 der gleichen Länge aus.
2. Ein Schlüssel k wird durch $Gen(1^n)$ erzeugt und ein zufälliges Bit $b \xleftarrow{R} \{0,1\}$ wird gewählt. Der Chiffretext $c \leftarrow Enc_k(m_b)$ wird an $\mathcal{A}$ gegeben.
3. $\mathcal{A}$ gibt ein Bit b' aus.
4. Das Resultat ist 1, falls $b' = b$ und 0 sonst.

Wir sagen $\mathcal{A}$ gewinnt, falls $PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1$.

Die Definition von semantischer Sicherheit sagt nun aus, dass die Erfolgswahrscheinlichkeit eines ppt Angreifers in obigem Spiel nur vernachlässigbar größer als $\frac{1}{2}$ ist:

Definition 1. Ein symmetrisches Verschlüsselungsverfahren $\Pi = (Gen, Enc, Dec)$ ist semantisch sicher bezüglich eines passiven Angreifers, wenn für alle ppt Angreifer $\mathcal{A}$ eine vernachlässigbare Funktion $negl$ existiert, so dass

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

wobei die Wahrscheinlichkeit über die zufälligen Münzwürfe von $\mathcal{A}$ und die zufälligen Münzwürfe im Spiel geht.

AUFGABE 4. Schlüsselspiel. (5 Punkte)
Betrachten Sie nun das folgende interaktive Protokoll Π' zum Verschlüsseln einer Nachricht: Zunächst führen Sender und Empfänger ein Schlüsselaustauschprotokoll Π durch, um einen Schlüssel k auszuhandeln. Anschließend berechnet der Sender $c \leftarrow Enc_k(m)$ und schickt c an den Empfänger, der die Nachricht m mit Hilfe von k rekonstruieren kann.

a) Formulieren Sie eine Definition für den Begriff der *semantische Sicherheit bzgl. eines passiven Angreifers* für dieses interaktive Protokoll.

b) Zeigen Sie, dass falls Π sicher gegen passive Angreifer und (Gen, Enc, Dec) ein semantisch sicheres symmetrisches Verfahren ist, dann erfüllt Π' die gegebene Definition.

AUFGABE 5. Trivialitätenkiste. (3 Punkte)
Betrachten Sie ein CPA-sicheres Public-Key Verfahren Π welches einzelne Bits verschlüsselt.

a) Zeigen Sie, dass ein unbeschränkter Angreifer mit Eingabe Public Key pk und Ciphertext $c \leftarrow Enc_{pk}(m)$ den Klartext m mit Wahrscheinlichkeit 1 bestimmen kann.

b) Zeigen Sie, dass die Chiffretext-Größe eines einzelnen Bits superlogarithmisch im Sicherheitsparameter ist, d.h. $|Enc_{pk}(b)| = \omega(\log n)$ für $b \in \{0, 1\}$.
Tipp: Nehmen Sie das Gegenteil an und betrachten Sie die Größe des Chiffretextraumes!