Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Eike Kiltz
Gottfried Herold

Hausübungen zur Vorlesung

Kryptographie II

SS 2012

Blatt 1 / 11. April 2012 / Abgabe **bis spätestens Mittwoch, 25.04.2012 10:00 Uhr**

AUFGABE 1:

Sei $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec})$ ein beliebiges Public-Key Verschlüsselungsverfahren (mit Nachritenraum $|\mathcal{M}| \geq 2$).

Zeigen Sie: [3 Punkte]
Es gibt stets einen *unbeschränkten* (d. h. nicht notwendig ppt) Angreifer A mit

$$\mathrm{Ws}[\mathrm{PubK}^{\mathrm{cpa}}_{A,\Pi} = 1] = 1$$

AUFGABE 2:

Sei $\mathcal{G}(1^n)$ ein Algorithmus, der eine zyklische Gruppe G der bekannten Ordnung q und einen Generator g für G erzeugt, wobei q eine n-Bit *Primzahl* ist.
Wir betrachten das InvDH-Problem (Inverse-Diffie-Hellman) bzgl. $\mathcal{G}$, dass darin besteht, zu durch $\mathcal{G}$ gegebenem G, q, g und g^a für zufälliges a das Gruppenelement $g^{(a^{-1})}$ zu berechnen:
Wir nennen InvDH hart/schwierig bzgl. $\mathcal{G}$, wenn für jeden ppt. Algorithmus A gilt:

$$\mathrm{Ws}[A(q, g, g^a) = g^{(a^{-1})}] = \mathrm{negl}(n)$$

wobei $q, g \leftarrow \mathcal{G}$, $a \in_R \mathbb{Z}_q^*$ und die Wahrscheinlichkeit über diese Wahlen sowie die internen Münzwürfe von A gebildet wird.

Zeigen Sie: Wenn das InvDH-Problem hart bzgl. $\mathcal{G}$ ist, so ist auch CDH hart bzgl. $\mathcal{G}$ [4 Punkte]

Bemerkung: Sie dürfen wie üblich annehmen, dass man Gruppenoperationen in Zeit $\mathrm{poly}(n)$ durchfüren kann.

- bitte wenden -

AUFGABE 3:

Sei $\mathcal{G}$ ein ppt. Algorithmus, der bei Eingabe 1^n eine $n-$Bit Primzahl p ausgibt, welche die zyklische Gruppe $\mathbb{Z}_p^*$ definiert, sowie einen Generator g für $\mathbb{Z}_p^*$.

(a) Zeigen Sie, dass das DDH-Problem *nicht* hart bzgl $\mathcal{G}$ ist. [4 Punkte]

Wir betrachten nun weiterhin das ElGamal-Verschlüsselungsverfahren $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec})$, instanziiert mit diesem $\mathcal{G}$, d.h.:

$\mathbf{Gen}(1^n)$: Berechnet $(p, g) \leftarrow_\$ \mathcal{G}$. Wähle $x \in_R \mathbb{Z}_{p-1}$ und setze $h = g^x \bmod p$.
Der public key ist $\text{pk} = (p, g, h)$, der secret key $\text{sk} = (p, x)$, der Nachrichtenraum $\mathcal{M} = \mathbb{Z}_p^*$.
$\mathbf{Enc}_{p,g,h}(m)$: Wähle zufälliges $r \in_R \mathbb{Z}_{p-1}$, Gib Ciphertext $c = (g^r \bmod p, h^r \cdot m \bmod p)$ aus.
$\mathbf{Dec}_{p,x}(c_1, c_2)$: Gibt Nachricht $m = c_2 \cdot c_1^{-x} \bmod p$ aus.

(b) Verifizieren Sie die Korrektheit von Π [1 Punkt]

(c) Zeigen Sie, dass Π *nicht* CPA-sicher ist. [3 Punkte]

Hinweise: Beachten Sie, dass $|\mathbb{Z}_p^*| = p - 1 = \text{ord}(g)$, was für $p > 2$ insbesondere gerade ist. Versuchen Sie, zu gegebenem g^x zu ermitteln, ob x gerade oder ungerade ist und nutzen sie dies aus.