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

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2010

Blatt 1 / 21. April 2010

AUFGABE 1. Mittelmann.

a) Beschreiben Sie einen aktiven Angriff (man-in-the-middle) auf das Diffie-Hellman Schlüsselaustauschprotokoll.

b) Können sich Alice und Bob vor einem MITM schützen, indem sie sich gegenseitig (verschlüsselte) Fragen zuschicken, die jeweils nur der andere beantworten kann?

Definition 1. Sei $\mathcal{G}$ eine endliche (multiplikative) Gruppe und $g \in \mathcal{G}$. Die *Ordnung* von g ist definiert als

$$ord(g) := \min\{i \in \mathbb{N} : g^i = 1\}.$$

Eine Gruppe $\mathcal{G}$ heißt *zyklisch*, falls es einen *Generator* $g \in G$ gibt, d.h. wir können $\mathcal{G}$ darstellen als

$$\mathcal{G} = \{1, g, g^2, \ldots, g^{ord(g)-1}\}.$$

AUFGABE 2. Algebraisches.

Sei $\mathcal{G}$ eine endliche Gruppe mit $|\mathcal{G}| = m$ und sei $g \in \mathcal{G}$ ein Element der Ordnung $i = ord(g)$. Zeigen Sie:

a) $g^x = g^y \Leftrightarrow x \equiv y \mod i$

b) $i|m$

c) Wenn $m = p$ prim ist, dann ist $\mathcal{G}$ zyklisch.

AUFGABE 3. Diskreter Logarithmus.
Sei $\mathcal{G} \simeq \mathbb{Z}_p^*$ die zyklische Einheitengruppe und sei g ein Generator[1]. Der diskrete Logarithmus $\log_g : \mathbb{Z}_p^* \to \mathbb{Z}_{p-1}$ bildet jedes Element $h = g^x$ auf den zugehörigen Exponenten $x \in \mathbb{Z}_{p-1}$ ab.

a) Berechnen Sie die diskreten Logarithmen $\log_2(13)$ in $\mathbb{Z}_{23}^*$ sowie $\log_{10}(22)$ in $\mathbb{Z}_{47}^*$.

b) Begründen Sie mit Teil a) von Aufgabe 1, wieso $\log_g(\_)$ eine *wohldefinierte* Abbildung ist.

AUFGABE 4. Diffie-Hellman.
Sei $\mathcal{G}$ eine zyklische Gruppe der Ordnung p. Man kann zum Diffie-Hellman Problem eine passende Abbildung $\mathsf{DH}(g^{x_1}, g^{x_2}) = g^{x_1 \cdot x_2 \bmod p}$ definieren. Wie sieht diese Abbildung für eine additive Gruppe aus? Berechnen Sie exemplarisch die Verteilung dieser Abbildung in der additiven zyklischen Gruppe $(\mathbb{Z}_6, +)$, wobei die Exponenten $x_1, x_2 \in_R \{0, \ldots 5\}$ gewählt werden. Interpretieren Sie Ihr Ergebnis in Bezug auf die Härte des DDH-Problems bzgl. dieser Gruppe.

AUFGABE 5. Härtefall.
Zeigen Sie, dass die Härte des DDH-Problems bzgl. einer Gruppe $\mathcal{G}$ die Härte des CDH-Problems bzgl. der gleichen Gruppe $\mathcal{G}$ impliziert.

[1]Man kann zeigen, dass $\mathbb{Z}_p^*$ zyklisch ist, falls $p \in \{2, 4, p^\ell, 2 \cdot p^\ell\}$ gilt wobei p eine ungerade Primzahl ist und $\ell \in \mathbb{N} \setminus \{0\}$