4. Übungsblatt

SS 2015
Rechnersicherheit
Ausgegeben am 07.05.2015
Abgabe 14.05.2015

Marian Margraf
Inst. für Informatik
Freie Universität Berlin

Aufgabe 1 (Message Authentication Codes)

Beschreiben Sie das MAC-Verfahren CMAC.

Aufgabe 2. (RSA Singnaturverfahren)

Welche Angriffe auf das RSA-Signaturverfahren gibt es. Wie können diese verhindert werden?

Aufgabe 3. (Digital Signature Algorithm)

In der Vorlesung wurde die Schlüsselgenerierung wie folgt definiert:

1. Wähle zwei Primzahlen p und q mit q teilt $p-1$
2. Wähle x in $\mathbb{Z}_p^*$ und berechne $g := x^{(p-1)/q} \bmod p$.
3. Falls $g = 1$, gehe zu 2.
4. Wähle eine Zahl $a \in \{1, ..., q-1\}$ und setze $A := g^a$.

(*a*) Zeigen Sie $g : \mathbb{Z}_p^*(g) := \{g^1, g^2, ...\} = \{g^i; i \in \mathbb{N}\}$ enthält genau q Elemente.

(*b*) Wie groß müssen p, q sein, um Sicherheitsniveau 100 Bit zu erhalten?

Aufgabe 4. (ECDSA)

Diskretes Logarithmusproblem (in $\bar{E}$):
Gegeben: G und $n \cdot G = \underbrace{G + \ldots + G}_{n-mal}$.
Lösung: Finde n
Dieses Problem ist in elliptischen Gruppen schwerer als DL in $\mathbb{Z}_p$
Bester derzeit bekannter Algorithmus hat Laufzeit $\mathcal{O}(\sqrt{p})$.
Also: Für Sicherheitsniveau 100 Bit muss $p \approx 2^{200}$ gelten.
Auf ell. Kurven basierende Kryptographie benötigt deutlich kürzere Schlüssellängen.

Studieren Sie den Signaturalgorithmus ECDSA. Stellen Sie insb. Schlüsselerzeugung, Signaturerzeugung und -verifikation dar. An welchen Stellen geht für die Sicherheit die Schwere des DL-Problems ein? Welche Bedingung muss für G (in der obigen Formulierung des Problems) gelten, damit das Problem tatsächlich schwer ist?