TECHNISCHE UNIVERSITÄT BERLIN WS 2007-2008
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. Florian Heß
Assistent: Osmanbey Uzunkol
`www.math.tu-berlin.de/∼hess/krypto-ws2007`
Abgabe: 23.11.2007
in der Übung

5. Übung Kryptographie

(HMAC, Zertifikate, Einwegfunktionen mit Falltür, mathematische Grundlagen)

---

1. Aufgabe

(a) Wir haben im Skript gesehen, wie die Zertifikatbehörde CA das Authentizitätsproblem lösst. Argumentieren Sie, Wie Alice der Behörde nachweisen kann, dass der verwendete öffentliche Schlüssel von ihr stammt, ohne die Information über dem geheimen Schlüssel zu geben.

(b) SHA-1 sei die verwendete Hashfunktion in HMAC, welcher wie im Skript definiert ist. Ferner sei k der bekannte Schlüssel, welcher mehrfach benutzt wird. Argumentieren Sie welche Art der von Nachricht unabhängigen Vorberechnungen benutzt werden kann um die Berechnung der HMAC-Werte mit diesem Schlüssel k effizienter durchzuführen.

(7 Punkte)

2. Aufgabe

Im Skript wurde beschrieben, wie man Kryptosysteme mit Hilfe der Einwegfunktionen mit Falltür ermöglicht. Argumentieren Sie, wie man ein digitales Signaturverfahren mittels einer Einwegfunktion mit Falltür realisieren kann.

(3 Punkte)

3. Aufgabe

(a) Sei $G := (\mathbb{Z}/p^k\mathbb{Z})^\times$ (p eine Primzahl, $k \geq 2$) und $J := \{a \in G \ : \ a^{p^k-1} \equiv 1 \mod p^k\}$. Zeigen Sie, dass $(J, \cdot)$ eine Untergruppe von G ist und $(G : J) \geq p^{k-1}$ gilt.

(b) Sei $G := (\mathbb{Z}/9\mathbb{Z})^\times$ und J wie in (a). Bestimmen Sie $(G : J)$.

(c) Sei G eine Gruppe mit 265236007426667381701 Elementen. Gibt es eine Untergruppe von G mit 2182256131 Elementen?

(d) Man sagt, dass eine Untergruppe H von G eine echte Untergruppe von G ist, falls $\{1_G\} \neq H \neq G$ gilt. Seien nun G eine Gruppe und $\{N_i | i \in I\}$ eine Familie der echten Normalteiler von G mit der Indexmenge I. Es gelten $G = \cup_i N_i$ und $N_j \cap N_k = \{1_G\}$ für $j \neq k$. Sind die folgenden Aussagen wahr oder falsch? Begründen Sie Ihre Antwort.

- G ist eine Abelsche Gruppe.
- Es gibt Untergruppen von G, die nicht Normalteiler sind.

(8 Punkte)

4. Aufgabe

Man kann mit Hilfe des in der Übung beschriebenen Verfahrens für ein gegebenes Element g einer Gruppe $(G, \cdot)$ und $n \in \mathbb{N}$ effizient g^n berechnen. Wie kann man dieses Verfahren verallgemeinern, damit für gegebene Elemente g_1 und g_2 dieser Gruppe G mit $n_1, n_2 \in \mathbb{N}$ effizient die simultane Exponentiation $g^{n_1} \cdot g^{n_2}$ berechnet werden kann. Wie groß ist der Aufwand dieser simultanen Exponentiation?

(5 Punkte)