TECHNISCHE UNIVERSITÄT BERLIN WS06/07
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr.F. Heß
WM: Dipl.-Math. M. Wagner
www.math.tu-berlin.de/~hess/krypto-ws2006

5. Übung Kryptographie

1. Aufgabe Chinesischer Restsatz (4 Punkte)

(a) Sei $n = pq$ mit $p, q > 2$ verschiedene Primzahlen und $a, b \in \mathbb{N}$ mit $ab \equiv 1 \mod (p-1)(q-1)$. Zeigen Sie, daß für beliebiges $x \in \mathbb{Z}/n\mathbb{Z}$ gilt: $x^{ba} \equiv x \mod n$.

(b) Sei $m \in \mathbb{N}$ und $m \geq 2$ mit Primfaktorzerlegung $m = \prod_{i=1}^{n} p_i^{n_i}$ gegeben. Zeigen Sie, daß für die Eulersche ϕ-Funktion

$$\phi(m) = \prod_{i=1}^{n} (p_i - 1) \cdot p_i^{n_i - 1}$$

gilt.

2. Aufgabe Schnitt und Verenigung von Gruppen (4 Punkte)

Sei I eine Indexmenge und $\{G_i\}_{i \in I}$ eine Familie von Untergruppen einer Gruppe G.

(a) Zeige, dass

$$\bigcap_{i \in I} G_i$$

eine Gruppe ist.

(b) Ist die Vereinigung

$$\bigcup_{i \in I} G_i$$

wieder eine Gruppe?

(c) Angenommen es gilt, dass für alle $i, j \in I$ ein $k \in I$ existiert mit $G_i, G_j \subseteq G_k$. Ist dann die Vereinigung der $G_i,\ i \in I$, eine Gruppe?

3. Aufgabe MAC **(4 Punkte)**

Wie sollten die Ausgabeblocklängen m von g und n von h im Verhältnis zueinander dimensioniert werden, um ein optimales Effizienz/Sicherheitsverhältnis gemäss der Reduktion des Satzes über geschachtelte MACs im Idealfall zu erhalten? Begründe die Antwort!

4. Aufgabe Geburtstagsattacke **(8 Punkte)**

Alice schickt an Bob eine Mail, in der festgehalten wird, daß Bob das Auto von Alice für 1000 Euro kaufen möchte. Die Mail enthält einen Header. Alice hat herausbekommen, daß dieser Header noch aus alten Zeiten stammt. Mail-Programme die heutzutage in Gebrauch sind benutzen diesen Header nicht mehr. Wohl aus Bequemlichkeit hat man diese nicht entfernt. In einer zweiten fingierten Mail schreibt Alice, daß der Verkaufspreis 10000 Euro beträgt statt 1000. Nun versucht Alice, die fingierte Nachricht im Header so abzuändern, daß sie den gleichen Hashwert hat wie die ursprüngliche Nachricht.

In der Datei AliceMail.k auf der Kryptographie-Homepage ist eine Hashfunktion SHA1Light vorgegeben, welche beliebige Strings auf Hexadezimalstrings der Länge 7 abbildet. Es gibt zwei Mails, eine Original-Mail und eine Fälschung. Finde mit Hilfe der Geburtstagsattacke eine Kollision, so daß die fingierte Mail den gleichen Hashwert hat wie die ursprüngliche Mail.

Gesamt: 20 Punkte