Netzsicherheit I, WS 2011
Übung 5

Prof. Dr. Jörg Schwenk

Betreuer: Florian Feldmann, Florian Giesen

Abgabe: Montag, 05. Dezember 2011, 11:00h

In der Übung, am Kasten vor ID 2/467, oder per Mail an Florian.Giesen AT rub.de
Gruppenarbeit bis max. 3 Studenten pro Gruppe ist erlaubt und erwünscht.

1 Broadcast Encryption I

Zeigen Sie, dass das Basisschema auf Folie 49 und Folie 50 (Annahme 1: Es gibt Einwegfunktionen) tatsächlich nur 1-resilient ist.

2 Broadcast Encryption II

Betrachten Sie das Broadcast Encryption Verfahren aus der Vorlesung, welches auf der Berechnung von p_i-ten Wurzeln modulo $N = PQ$ beruht (Folie 51 im Skript). Drei Benutzer U_1, U_2, U_3 verfügen über folgendes Schlüsselmaterial:

1. U_1: $(N, p_1, g_1) = (629, 7, 133)$
2. U_2: $(N, p_2, g_2) = (629, 5, 92)$
3. U_3: $(N, p_3, g_3) = (629, 11, 5)$

a) Welche Teile eines Schlüssels (N, p_i, g_i) sind öffentlich (d.h. allen Benutzern bekannt)? Welche sind geheim (d.h. nur Benutzer i bekannt)?

b) Führen Sie die Berechnung des Gruppenschlüssels der Gruppe $T = \{U_1, U_2, U_3\}$ für jedes einzelne Gruppenmitglied durch!

c) Führen Sie die Berechnung des Gruppenschlüssels der Gruppe $T = \{U_1, U_3\}$ für jedes einzelne Gruppenmitglied durch.

d) Bruce Schneier gibt U_2 den Gruppenschlüssel von $T = \{U_1, U_3\}$ aus Aufgabe c). Berechnen Sie mit Hilfe der Werte die U_2 bekannt sind den Wert g. (Wie in der Notation auf den Folien ist g der Wert, der die Gleichungen $g_i = g^{p_i}$ für $i \in \{1, 2, 3\}$ erfüllt).