Sommersemester 2005
Hasso- Plattner- Institut, Universität Potsdam
Übung zur Vorlesung
Fachgebiet Internet- Technologien und - Systeme
Meinel / Kutzner

Aufgabenblatt 12
(NUR FÜR ULI-STUDENTEN)

(URL: http://www.hpi.uni- potsdam.de/index.php?id=411)

Abgabe: Mo, 11.07.2005, bis 12 Uhr MEZ (per E-Mail an mathias.kutzner@hpi.uni- potsdam.de)

Thema: Schlüsselvereinbarung und - verteilung

Erreichbare Punkte: 11

Aufgabe 1: **2 Punkte**

Für den Schlüsselaustausch über das Diffie- Hellman Verfahren werden die Zahlen $p = 2447$ und $g = 1867$ festgelegt. Zeigen Sie, dass g ein primitives Element von Z_p^* ist.

Aufgabe 2: **5 Punkte**

Benutzer U und V verwenden das Diffie- Hellman Verfahren mit p und g aus Aufgabe 1. Benutzer U wählt $a_U = 1347$. Welches b_U sendet er an V? Benutzer V antwortet mit $b_V = 848$. Welchen gemeinsamen Schlüssel benutzen U und V für die Kommunikation? Ermitteln Sie das a_V, dass V gewählt hat. Welches praktisch unlösbare Problem verhindert, dass ein Außenstehender a_V ermitteln kann?

Geben Sie Ihre Überlegungen bzw. Ihren Rechenweg an.

Aufgabe 3: **4 Punkte**

Ein Key Access Server (KAS) dient als vertrauenswürdiger Dritter, der für die Aufbewahrung und Verteilung gemeinsamer geheimer Schlüssel verantwortlich ist. Welche Aufgaben übernimmt KAS in den Schlüsselvereinbarungprotokollen Diffie- Hellman, Girault, MTI und Station- to- Station.

Hinweise:

Sei p eine Primzahl mit $p \geq 5$. Eine ganze Zahl g ist genau dann primitives Element von Z_p^*, wenn für keinen Primfaktor q von $p-1$ gilt: $g^{(p-1)/q} \equiv 1 \bmod p$.

Bitte wenden!

Schlüsselvereinbarung und -verteilung nach Diffie-Hellman zwischen Teilnehmer U (Initiator) und V:

- Allen Kommunikationspartnern sind die vereinbarte große Primzahl p und eine Zahl g, die primitives Element in Z_p^* ist, bekannt.
- U wählt zufällig einen Wert $a_U < p-1$ und berechnet damit den Wert $b_U = g^{a_U} \bmod p$. U sendet b_U an V.
- V wählt zufällig einen Wert $a_V < p-1$ und berechnet damit den Wert $b_V = g^{a_V} \bmod p$. V sendet b_V an U.
- U berechnet den Schlüssel K gemäß $K = b_V{}^{a_U} \bmod p = g^{a_V \cdot a_U} \bmod p$
- V berechnet den Schlüssel K gemäß $K = b_U{}^{a_V} \bmod p = g^{a_U \cdot a_V} \bmod p$