Technische Informatik 2 WS 2012/13
Tutor:

Übungsblatt 1

1	2	3	4	5	$\sum$

Hauke Hansen
Lukas Heinrich
Florian Kraemer

Lösungsvorschlag
Abgabe: 31.10.2012

Aufgabe 1

1

Aufgabe 2

1.

Die öffentliche Zugänglichkeit der public-keys stellt kein Sicherheitsproblem dar, da SSH auf einem asymmetrischen Verschlüsselungsverfahren beruht. Das zugrundeliegende Prinzip beruht dann auf mathematischen Einwegfunktionen, sprich Funktionen die (mittels public-key) einfach zu berechnen sind. Das Ergebnis aber dann zu invertieren, sprich zu entschlüsseln, ist ohne Kenntnis des private-keys unmöglich. Letzteres ist allerdings eine angenommene unbewiesene Bahauptung für einen endlichen Zeitraum.[1][2]

2.

Das Senden eines Passwortes über einen ungesicherten Kanal könnte leicht abgehört werden, und würde einen Angreifer direkt in Besitz unverschlüsselter Zugangsdaten bringen.

[1] http://de.wikipedia.org/wiki/Einwegfunktion
[2] http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem