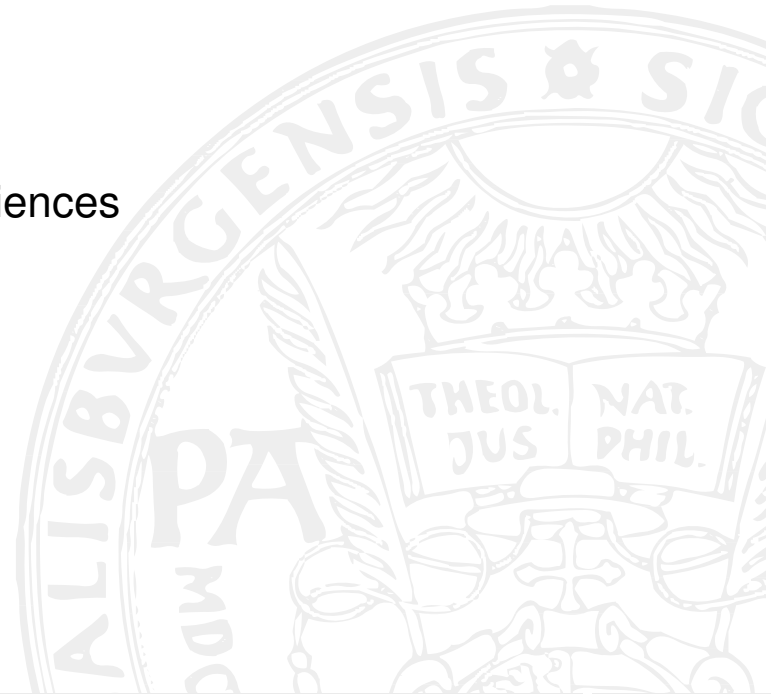
# Einführung Kryptographie und IT-Sicherheit

## Sommersemester 2020

Andreas Uhl

Department of Computer Sciences
University of Salzburg

June 8th, 2020



# Montag 8. Juni, 13:15

## Fragen zum Skriptum - Abschnitt 4 - 4.1.1

1. Auf welchen Ebenen können im Bereich Netzwerksicherheit Sicherheitsfeatures realisiert werden ?
2. Diskutieren sie Vor- und Nachteile dieser Ebenen in diesem Zusammenhang.
3. Welche kryptographischen Grundfunktionalitäten deckt IPSec ab ?
4. Beschreiben sie das klassische Szenario zum Einsatz von IPSec in einer Organisation / Firma mit Zweigstellen.
5. Diskutieren sie Pros und Cons des IPSec Ansatzes.
6. Vergleichen sie AH und ESP.
7. Was ist eine Security Association (SA) ?

# Montag 8. Juni, 13:15

## Fragen zum Skriptum - Abschnitt 4.1.1 - 4.1.2

8. Vergleichen sie Tunnel und Transport Mode (Anwendungssetting, Realisierung).
9. Wie wird eine SA etabliert ?
10. Welche Verfahren verwendet IKE zur Autentifizierung und zum Key Exchange ?
11. Welche Kritikpunkte gibt es gegen IPSec ?
12. Was sind konstruktive Verbesserungsvorschläge ?
13. *** Welche Probleme gibt es bei der Verwendung von IPSec und NAT ? (jeweils bei AH und ESP) ***
14. Welche (kryptographischen) Ziele verfolgt DNSSec ?

# Montag 8. Juni, 13:15

## Fragen zum Skriptum - Abschnitt 4.1.2

15. Warum ist eine Absicherung des DNS Systems notwendig ?
16. Welche zentralen Services werden durch DNSSec eingeführt ?
17. Beschreiben sie die dafür eingeführten RRs !
18. Wie funktioniert die DNS-Lookup Prozedur bei recursive name servers ?
19. Wie werden Top Level domains signiert und was passiert wenn es keine TLD Signatur gibt ?
20. Was sind Schwachstellen von DNSSec ?
21. *** Was ist ein Zertifikat und wie ist ein X.509 Zertifikat strukturiert ? ***