# Einführung Kryptographie und IT-Sicherheit

## Sommersemester 2020

Andreas Uhl

Department of Computer Sciences
University of Salzburg

March 19th, 2020

## Fragen zum Skriptum - Abschnitt 1.2.1

1. Warum wird Kryptographie häufig als Privileg der Regierungen betrachtet ?
2. Was sind wesentliche Unterschiede zu anderen Teilgebieten der Informatik ?
3. Wie funktioniert der Ceasar Cipher ?
4. Wann wurde der Grundstein für Public-key Kryptographie gelegt ?
5. Welches sind die 4 wesentlichen Aufgaben der Kryptographie ?
6. Was bedeutet “Security by Obscurity” und warum ist das nicht state-of-the art ?
7. Was besagt das Kerckhoff’sche Prinzip und was sind bekannte Beispiele von Verstössen gegen dieses Prinzip ?

# Montag 23 März, 13:15

## Fragen zum Skriptum - Abschnitt 1.2.2 - Abschnitt 1.2.4

8. Was ist das Hauptproblem bei Symmetrischen Verschlüsselungsverfahren (und warum heissen sie “symmetrisch”) ?
9. Welche Hauptkategorien können unterschieden werden ?
10. Warum heissen public-key Algorithmen auch “asymmetrische” Verfahren ? Welche Funktion haben die zwei unterschiedlichen Schüssel und inwiefern ist der public-key öffentlich ?
11. Was ändert sich bei der Verwendung von public-key Kryptographie im Zusammenhang mit digitalen Unterschriften ?
12. Was ist der Hauptvorteil dieser Verfahren gegenüber der symmetrischen Kryptographie ?
13. Kann eine Ciphertext-only Attacke immer durchgeführt werden ?
14. Welche Attacken können immer gegen Public-key Systeme durchgeführt werden ? Warum ? Design von solchen Verfahren ?

# Montag 23 März, 13:15

## Fragen zum Skriptum - Abschnitt 1.2.5 - Abschnitt 1.3.1.2

15. Beschreiben sie die verschiedenen Kategorien des Brechens eines Verschlüsselungsalgorithmus.
16. Was haben Zeit und Kosten eines Angriffes mit der Algorithmensicherheit zu tun ?
17. Was ist eine Brute-force Attack ? Was muss man beurteilen können damit so eine Attacke funktionieren kann ?
18. Was bedeutet computationally secure (im Gegensatz zu unconditionally secure) ?
19. Wie funktioniert die Häufigkeitsanalyse als Attacke gegen Monoalphabetische Cipher (simple Substitution Ciphers) ?
20. Was sind polyalphabetische Cipher und im Speziellen der sog. Vigenere Cipher ?
21. Warum können Transposition Ciphers (Permutationen) einer Known-Plaintext Attacke nicht widerstehen ?

SALISBVRGENSIS
THEOL.
JUS
NAT.
PHIL.