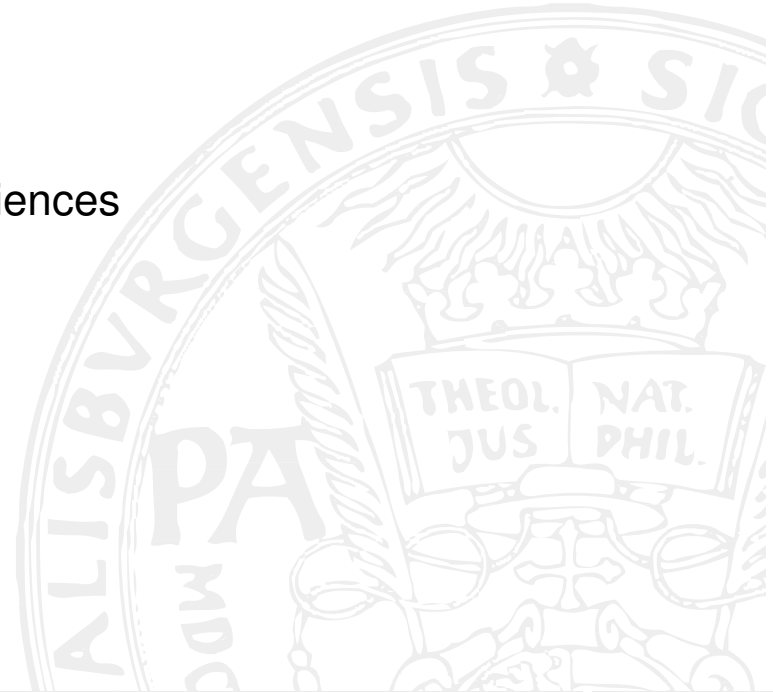
Einführung Kryptographie und IT-Sicherheit

Sommersemester 2020

Andreas Uhl

Department of Computer Sciences
University of Salzburg

18. Mai, 2020



Fragen zum Skriptum - Abschnitt 3.1.3 - 3.2.1

1. Welche DES Varianten erhöhen die Sicherheit nicht ?
2. Welche DES Varianten verbessern die Sicherheit ? Ist dies aus heutiger Sicht ausreichend ?
3. Wie kam es zur Definition / Standardisierung von AES ?
4. Welche AES Parameter werden auf welche Weise festgelegt ?
5. Beschreiben sie die Elemente einer einzelnen AES Runde.
6. Wie funktioniert der gesamte AES Verschlüsselungsablauf ?
7. *** Vergleicht man die einzelenen Komponenten von DES und AES, was fällt bezüglich einer eventuellen Sicherheitsanalyse auf ? Wie ist die aktuelle Sicherheit von AES einzustufen ? Aktuelle Attacken ? ***

Montag 18. Mai, 13:15

Fragen zum Skriptum - Abschnitt 3.2.2 - 3.3

8. Was ist ein auffälliges Designprinzip von IDEA (auch verglichen mit DES) ?
9. Gemeinsamkeiten und Unterschiede zwischen DES und GOST ?
10. Beschreiben sie die drei grundlegenden Eigenschaften von One-Way Hash Funktionen.
11. *** Leiten sie die namensgebenden kombinatorischen Werte ("Wie viele Menschen müssen in einem Raum sein .....") im Zusammenhang mit der Geburtstagsattacke her. ***
12. *** Erklären sie die Analogie zu Hashwerten und leiten sie die angegebenen Mengen von Hash-Werten her, die für die beiden Angriffsvarianten notwendig sind (2^m vs. $2^{m/2}$). ***
13. Erklären sie die Durchführung der Geburtstagsattacke.
14. Beschreiben sie, wie aus einer gegebenen Hashfunktion eine Variante mit längerem Hashwert erzeugt werden kann.

Montag 18. Mai, 13:15

Fragen zum Skriptum - Abschnitt 3.3.1 - 3.3.6

15. Beschreiben sie den Ablauf von MD-5.
16. Wie ist es um die Sicherheit der heute oft verwendeten Hashfunktionen MD-5 und SHA-1 bestellt ? Welche Hashfunktion muss aus heutiger Sicht verwendet werden ?
17. Beschreiben sie verschiedenen Varianten wie symmetrische Blockciphers eingesetzt werden können um One-Way Hash-Funktionen zu realisieren. Warum ist das attraktiv ?
18. *** Beschreiben sie den Einsatz von AES (welche Variante/ Parameterwerte?) in einem Tandem Davies Mayer Setup und welche Parameter die resultierende Hashfunktion dann hat ! ***
19. Warum erscheint die beschriebene public-key one-way Hashfunktion als wenig praxistauglich ?
20. Wie funktioniert ein MAC ?
21. Vor- und Nachteile eines MAC gegenüber der klassischen digitalen Signatur ?