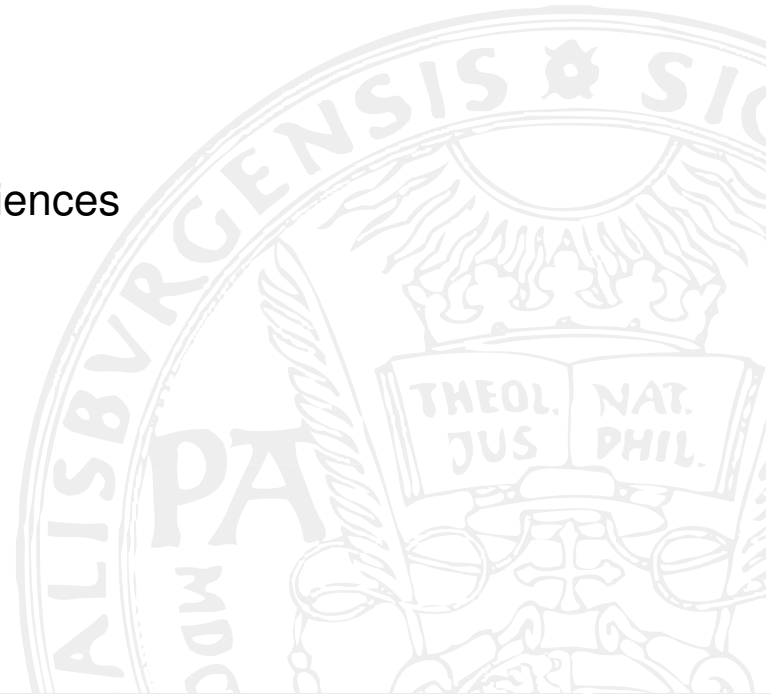
Einführung Kryptographie und IT-Sicherheit

Sommersemester 2020

Andreas Uhl

Department of Computer Sciences
University of Salzburg

May 4th, 2020



Montag 4. Mai, 13:15

Fragen zum Skriptum - Abschnitt 2.1.2 - 2.1.4

1. Beschreiben sie eine Schleife von DES mit den jeweiligen Bitanzahlen der Komponenten (begleitende Slides S.3)
2. Beschreiben sie den gesamten Ablauf einer Verschlüssleung mit DES (begleitende Slides S.2)
3. *** Beschreiben sie die DES S-Box Operation und geben sie ein Beispiel (unterschiedlich zum Skriptum) anhand der S-Box Definitionen auf S.5 der begleitenden Slides.***
4. Warum kann DES so effizient in Hardware realisiert werden ? Was sind die dominierenden Operationen ?
5. Wie unterschiedet sich der DES Entschüsselungsvorgang vom Verschlüsselungsvorgang ?
6. Was sind Vor- bzw. Nachteile des ECM ?
7. Definieren sie die Funktionsweise des CBC Modus. Was ist die Rolle des Initialisierungsvektors ?

Montag 4. Mai März, 13:15

Fragen zum Skriptum - Abschnitt 2.1.4 - 2.1.5

8. *** Erklären und begründen sie detailliert die Auswirkungen eines 1-bit Ciphertextfehlers bei CBC nach dem Entschlüsseln. ***
9. Erklären sie Funktionsweise und Unterschiede bei CFB und OFB.
10. *** Erklären und begründen sie detailliert die Auswirkungen eines 1-bit Ciphertextfehlers bei CFB und OFB. ***
11. Eklären sie die Funktionsweise des CTR Modus. Warum ist parallele Verarbeitung und random access Zugriff möglich ?
12. Warum ist die Auswirkung eines Ciphertextfehlers bei CTR identisch zum OFB Fall ?
13. Was sind “Weak Keys” und warum warum verändern sich diese in DES Rundendurchläufen nicht ?
14. Warum sinkt die Komplexität einer chosen Plaintextattacke gegen DES wenn man die Eigenschaft von “komplement keys” benutzt ?

Montag 4. Mai, 13:15

Fragen zum Skriptum - Abschnitt 2.1.5 - 2.2

15. Welches Sicherheitsproblem hat das Missverhältnis von DES Blockgrösse und Keypsace zur Folge ?
16. Welche Rolle spielt die algebraische Gruppeneigenschaft von DES bezüglich einer Mehrfachverschlüsselung ?
17. Ist die Rundenanzahl von DES zufällig gewählt ?
18. Erklären sie das Grundkonzept von “Differential Cryptoanalysis”. Um welche grundlegende Angriffsart handelt es sich ?
19. Erklären sie das Grundkonzept von “Linear Cryptoanalysis”. Um welche grundlegende Angriffsart handelt es sich ?
20. Was ist eine Primzahl und wieviele Primzahlen gibt es ? Sind diese gleichmässig verteilt ?
21. Warum ist Modulararithemtik für die Kryptographie interessant ?

Fragen zum Skriptum - Abschnitt 2.2

22 *** Erklären sie, warum die Berechnung von diskreten Logarithmen um so vieles aufwändiger ist als die Logarithmierung in klassischer Arithmetik. ***

23 Was ist ein probabilistischer Primzahltest ? Warum ist dessen Existenz wichtig für die Kryptographie ?

24 Was bedeutet $3/4 \mod 5$ und was ist das Ergebnis ?

25 Was besagt der kleine Satz von Fermat ?

26 Wann gibt es in Modulararithmetik eine eindeutige Lösung für das Finden der Inversen ? Was lässt sich beobachten wenn diese Bedingung nicht erfüllt ist ? Gibt es immer eine Inverse ?

27 Was ist die Euler'sche Phi-Funktion $\phi(n)$?

28 Was besagt die Euler'sche Verallgemeinerung des kleinen Satzes von Fermat ?