
Kryptographie

Vorlesung im WS 2007/8

<http://www.math.tu-berlin.de/~hess/krypto-ws2007>

*Florian Heß / Osmanbey Uzunkol
Technische Universität Berlin*

1

18. Oktober 2007

Vorlesungsplan

Einleitung und grundlegende Fragestellungen der Kryptographie

- Verschlüsselung, digitale Signaturen
- Angreifer und Sicherheitsmodelle
- Symmetrische und asymmetrische Verfahren

Vorlesungsteile:

- Symmetrische Verfahren
 - Blockchiffren, Stromchiffren, Hashfunktionen, MACs
- Asymmetrische Verfahren
 - Mathematische Grundlagen
 - RSA und DL-basierte Systeme
 - Algorithmen der Computeralgebra
 - Sicherheitsbeweise
 - Variationen, weitere Themen und Anwendungen

2

18. Oktober 2007

Vorlesungsplan

Vorlesungsteile (voraussichtlich):

- Gitter
 - Mathematische Grundlagen
 - Reduktionsalgorithmus LLL
 - Anwendungen auf die Kryptographie

3

18. Oktober 2007