Cryptography Seminar
SS 2017

Session 1 - 25.04.2015: Giorgio Laguzzi

Historical Ciphers: shift cipher, substitution cipher, Vigenère cipher, permutation cipher ([Sm2004, Chapter 3]).

Session 2 - 02.05.2015: Sarah Schmid - Annette Lietz

The Enigma Machine, part I ([Sm2004, Chapter 4, sections 1-5]).

Session 3 - 09.05.2015: Sarah Schmid - Annette Lietz

The Enigma Machine, part II ([Sm2004, Chapter 4, sections 6-9]).

Session 4 - 16.05.2015: Felix Schimdt

Information Theoretic Security: probability and ciphers, entropy, spuriuos key and unicity distance ([Sm2004, Chapter 5]).

Session 5 - 23.05.2015: Stefan Haulitschke

Historical Stream Ciphers: symmetric ciphers, cipher basics, Lorenz cipher ([Sm2004, Chapter 6]).

Session 6 - 30.05.2015: tba

Modern Stream Ciphers: Linear feedback shift register, combining LFSRs, RC4 ([Sm2004, Chapter 7]).

Session 7 - 13.06.2015: Julia Baiker

Block Ciphers: Feistel ciphers and DES, Rijndael, modes of operation ([Sm2004, Chapter 8]).

Session 8 - 20.06.2015: Nils Lauinger

Symmetric Key Distribution: key management, secret key distribution, formal approaches to protocol checking ([Sm2004, Chapter 9]).

Session 9 - 27.06.2015: Paul Widmaier - Britta Tho Pesch

Basic Public Key Encryption Algorithms, part I ([Sm2004, Chapter 11, sections 1-3.3]).

Session 10 - 04.07.2015: Paul Widmaier - Britta Tho Pesch

Basic Public Key Encryption Algorithms, part II ([Sm2004, Chapter 11, sections 3.4-6]).

Session 11 - 11.07.2015: Roman Haale

Primality Testing and Factoring, part I ([Sm2004, Chapter 12, Sections 1-2]).

Session 12 - 18.07.2015: tba

Primality Testing and Factoring, part II ([Sm2004, Chapter 12, Sections 3-4]).

Session 13 - 25.07.2015: tba

Discrete algorithms ([Sm2004, Chapter 13]).

References

[Sm2004] Nigel Smart, *Cryptography: an introduction*, Mcgraw-Hill College (2004).