Cryptography Seminar
SS 2015

Session 1 - 23.04.2015: Schmidt, Hendrik

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

Session 2 - 30.04.2015: Burgold, Lino

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

Session 3 - 07.05.2015: Kirchner Ankatrin - Waadt, Georg

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

Session 4 - 13.05.2015 (we switch the day, since 14.05 is holiday): Grundner-Culemann, Franziska

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

Session 5 - 21.05.2015: Kilchling, Daniel

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

Session 6 - 03.06.2015 (we switch the day, since 04.06 is holiday): Kucharzewski, Sofia

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

Session 7 - 11.06.2015: Meyer, Frank

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

Session 8 - 18.06.2015: Schriche, Tobias

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

Session 9 - 25.06.2015: Friedmann, Mathias

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

Session 10 - 02.07.2015: Heus, Maria

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

Session 11 - 09.07.2015: Pichler, Arvid

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

Session 12 - 16.07.2015: Engert, Andreas

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

Session 13 - 23.07.2015: Rein, Stefanie

Discrete algorithms ([Sm2004, Chapter 13]).

References

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