Resources on Cryptography

Preparation Lecture 1

- Core principles and algorithms of cryptosystems:
  Information Security: Principles and Practice by M. Stamp
  Chapter 2 on Crypto Basics, chapter 3 on Symmetric Key Crypto
  http://tinyurl.com/y9dkjx76

Literature Lecture 1

- Attacks on the WEP protocol:
  Intercepting Mobile Communications: The Insecurity of 802.11 by N. Borisov et al.
  http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
  Emphasize on sections 2, 3 and 4.1
- Announcing the Crypto1 hack on the OV-chipkaart:
  Security Flaw in MIFARE Classic by R. Schreur et al.
  https://www.cs.bham.ac.uk//~garciaf/publications/Security_Flaw_in_MIFARE_Classic.pdf

Extras Lecture 1

- Core principles of cryptosystems:
  Handbook of Applied Cryptography, by A. Menezes
  https://cacr.uwaterloo.ca/hac/
- Core principles and algorithms of symmetric cryptosystems:
  Network Security Essentials: Application And Standards by W. Stallings
- Refreshing probability theory:
  Introduction to Mathematical Statistics by D. Wackerly et al.
  Emphasize on chapter 2 and expand to discrete/continuous distributions on chapters 3, 4

Preparation Lecture 2

- Core principles and algorithms of cryptosystems:
  Information Security: Principles and Practice by M. Stamp
  Chapter 4 on Public Key Crypto and chapter 5 on Hash Functions
  http://tinyurl.com/mr35nx4n
- Get started with MATLAB by doing the tutorials listed here
  https://nl.mathworks.com/help/matlab/getting-started-with-matlab.html

Literature Lecture 2

- The padding oracle attack:
  Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS... by S. Vaudenay
  https://www.iacr.org/archive/eurocrypt2002/23320530/cbc02_e02d.pdf
  Emphasize on sections 3.1 and 3.2
- Find and browse the SHA-256 hash function:
  The Secure Hash Standard (SHS) by NIST
  https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

- Find and browse the RSA Digital Signature:
  Digital Signature Standard (DSS) by NIST
  https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

Extras Lectures 2

- Hash functions introduction:
  Handbook of Applied Cryptography Chapter 9, by A. Menezes
  https://cacr.uwaterloo.ca/hac/about/chap9.pdf