Introduction

Cryptography and Protocols

Andrei Bulatov

Course Info

- **Instructor: Andrei Bulatov**
  - Email: abulatov@cs.sfu.ca
  - Room: TASC 8013
  - Office hours (tentative):
    Monday 13:00 – 14:30,
    Wednesday 11:30 – 12:30
- **Lectures:**
  - Tuesday: 10:30 – 11:20, AQ 3005
  - Thursday: 9:30 – 11:20, AQ 3149
- **Course webpage**
  - http://www.cs.sfu.ca/CC/404/abulatov

Course Info

- **Books:**

  Cryptography and network security. Principles and practice, William Stallings, Pearson, 20014: 6th edition

  Introduction to modern cryptography, Jonathan Katz, Yehuda Lindell, Chapman and Hall, 2008

  Handbook of Applied Cryptography, Alfred J.Menezes, Paul C. van Oorschot, and Scott A. Vanston, CRC-Press, 1996

  Practical Cryptography, Niels Ferguson, Bruce Schneier, Wiley Publishing, 2003

Course Info

- **Online Lecture Notes:**
  - Bellare-Rogaway's lecture notes
    http://www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf
  - Bellare's lecture notes
    http://www-cse.ucsd.edu/users/mihir/cse107/index.html
  - Barak's lecture notes
    http://www.cs.princeton.edu/courses/archive/fall05/cos433
  - Biryukov's lecture notes
    http://www.wisdom.weizmann.ac.il/~albi/cryptanalysis

Course Info

- **Other online resources:**

  Cryptology ePrint archive

  http://eprint.iarch.org

  Wikipedia Cryptography portal

  http://en.wikipedia.org/wiki/Portal:Cryptography

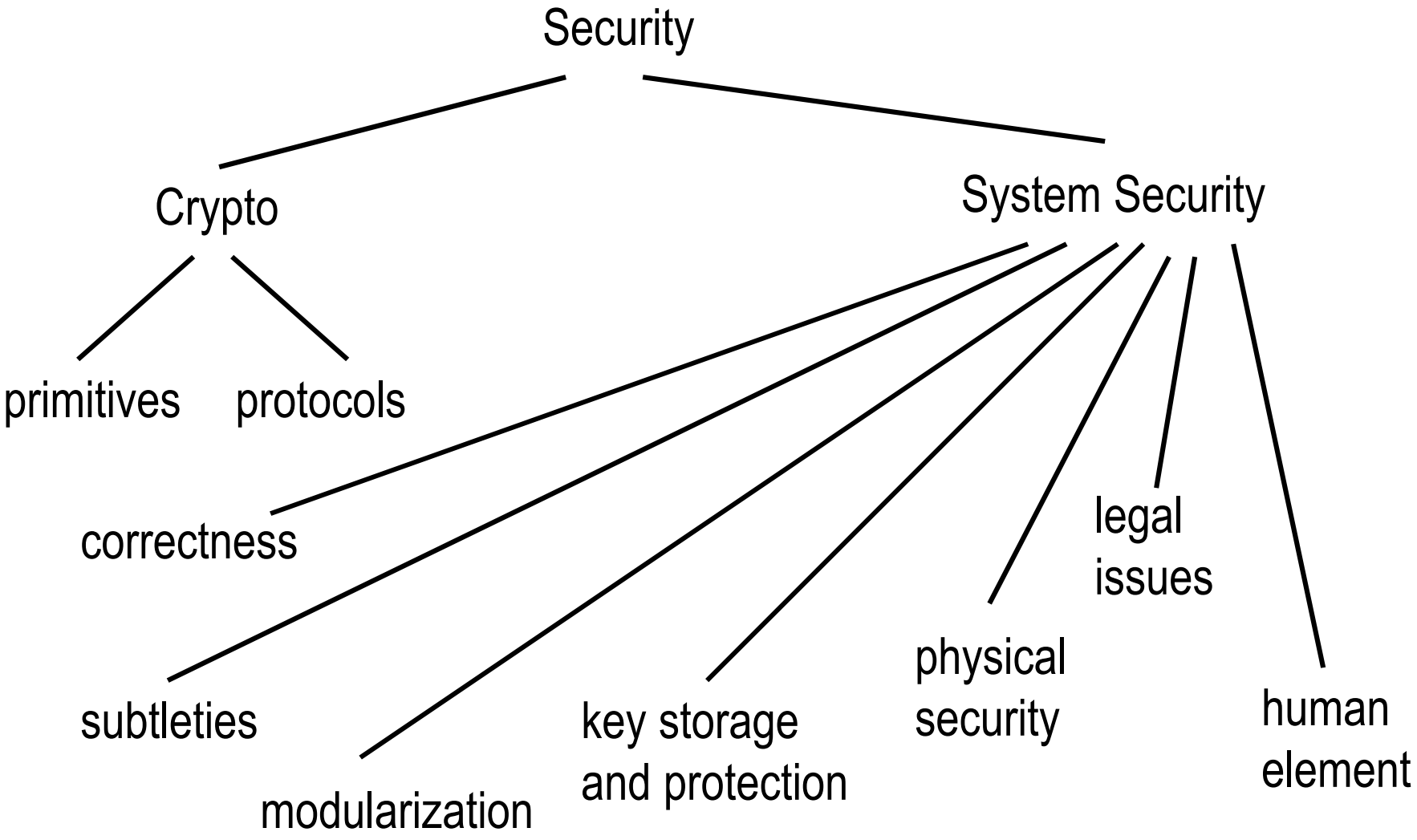
  National Institute of Standards and Technology

  http://csrc.nist.gov/groups/ST/index.html:

Course Info

- **Grading:**
  - 4 Assignments (4 × 8%)
  - 3 Quizzes (3 x 8%)
  - 1 Final Exam 44%

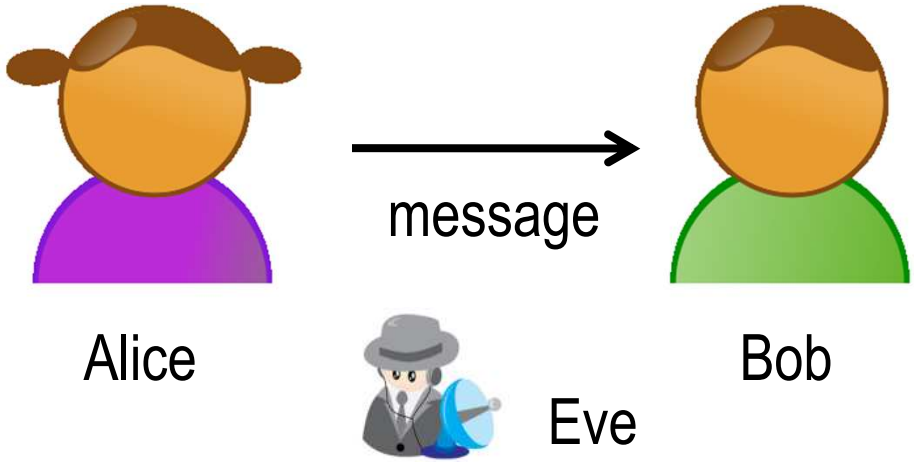
Security and Cryptography



Course objective

- What is good security?
- What kind of primitives are there, and what are good primitives?
- How can we construct good protocols from good primitives?

Model of Cryptography: classical

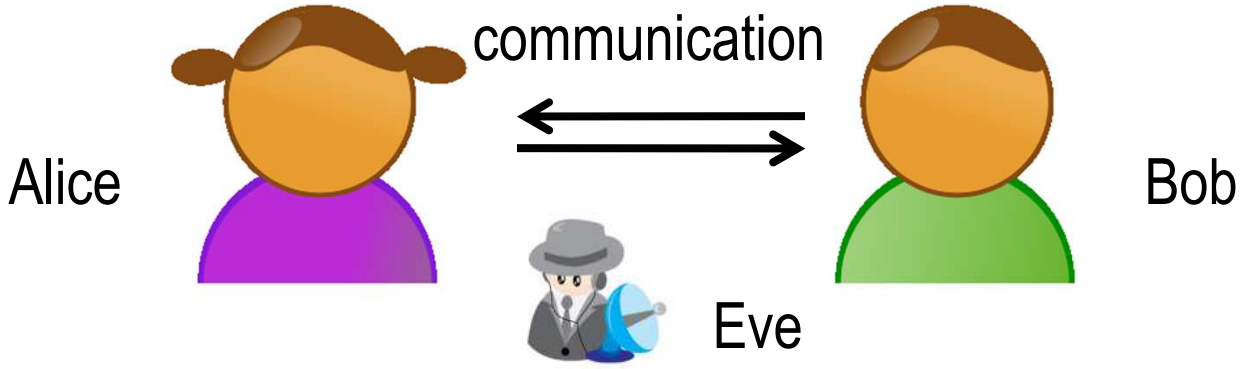


Protocol: a collection of algorithms
(K, E, D)

- K – key generation algorithm
- E – encryption algorithm
- D – decryption algorithm

Goal: privacy
Ideal: ideal channel
Eve's capabilities: known ciphertext attack

Model of Cryptography: modern



Goals:

- privacy
- authenticity
- integrity
- non-repudiation
- More:
  - e-auctions
  - online coin flipping
  - zero-knowledge proofs
  - …

Eve's capabilities:

- known cipher text attack
- known plaintext attack
- chosen plaintext attack
- chosen ciphertext attack

Topics

- Historical remarks
- Security: perfect, statistical, and computational
- Pseudo-random generators and stream ciphers
- Pseudo-random functions and authentication
- Block ciphers, DES
- Symmetric encryption schemes
- Symmetric authentication schemes, Kerberos
- Public key cryptography, RSA
- Asymmetric encryption schemes
- Key distribution, SSL
- Digital signatures, WEP, PKI
- Zero knowledge
- E-commerce, e-voting, etc.