

INST 346 Final Exam Study Guide

Exam Coverage

- Exam 3 is comprehensive, covering the entire course. About half of the exam will cover material from after exam 2, and a quarter each will cover material from before exam 1 and before exam 2. There are already topic lists posted for exams 1 and 2, so this study guide contains the topic list for material covered after exam 2. But you must also refer to the other two topic lists to have a complete picture of the topics that may be tested!
- This will be a two-hour exam, and the use of a computer with network access and Wireshark installed is required. Electronic submission (by both ELMS and email) will be required. Submission of supplemental materials on paper (e.g., for diagrams) will be allowed if you prefer.
- As always, material covered in assigned readings, in class, in homeworks, and on labs is testable.
- Our last class of the semester (December 7) will be devoted entirely to exam review, and there will also be an optional one-hour ELMS text chat at 8 PM on Thursday December 14. In both cases, you should come with questions since there is no lecture planned in either case – these are times to get your questions answered. No further office hours are scheduled after December 4, but Rashmi and I will be happy to talk with you by appointment either in person or (for me) by skype or phone. Because I am in Japan, please allow 24 hours for setting up appointments (and we'll likely need to limit them to the evening, Maryland time).

Encryption

- Symmetric key encryption
- Public key encryption
- PGP for email
- SSL (and TLS)

Authentication

- Hash
- Message Authentication Codes
- Digital signatures
- Man-in-the-middle attacks
- Certificate authorities

Appropriate Use

- Legal system (constitution, laws, regulations, treaties)
- Contracts (e.g., terms of service)
- Policy (e.g., privacy policies)
- Norms
- Technical means
- Jurisdiction
- Controlling collection vs. controlling use
- Balancing interests

Privacy

- FISA Section 702
- Upstream collection
- About collection

- Multi-communication transactions

Twitter

- Agile development methods
- Adoption of innovation (social structure, social structure, predictors)
- Financing

The Interplanetary Internet

- Interplanetary propagation delays
- Interplanetary queueing delays
- Delay tolerant networking
- Sneakernet
- Edge caching

Global Internet Access

- Demographic challenges
- Spatial challenges
- Last-mile technology (Fiber optics, radio towers, drones, balloons, sneakernet, ...)
- Context-sensitive design