CS 376 Syllabus – Online for the rest of the Spring Semester

Udacity.com has the best online version of this course called Applied Cryptography. The lessons are free. You will need to sign up for an account.

Once you are logged in, search for the Applied Cryptography course or try: https://www.udacity.com/course/applied-cryptography--cs387

Course Organization

The course is organized as follows:

Lesson 1 – Lesson 1  Lesson 4 – Lesson 2  Lesson 7 - Lesson 3
Lesson 2 – Problem Set  Lesson 5 – Problem Set  Lesson 8 – Problem Set
Lesson 3 – Q&A Session  Lesson 6 – Q&A Session

You should watch the lessons (in red) first before attempting the problem set Q&A, or quizzes.

The following lessons (approximately one lesson per week) are the ones needed for the rest of this class.

Lesson 3 – Key Exchange
  Intro
  Diffie Hellman
  Secret Paint Mixing
  Properties of Multiplication
  DH Security
  Faster Primality Test

Lesson 4 – Asymmetric Ciphers
  Asymmetric Cryptosystems
  One-way functions
  RSA Cryptosystem
  Computing D still hard

Lesson 5 – Authentication
  Overview
  SSH Authentication
  Master Secret
  Weak Ciphers
  Interesting Certificate Chains
  Handshake Recap
  CBC Attack

Lesson 6 – Using Cryptography to Solve Problems
  Solving Problems
  Traffic Analysis
  Voting
  Blindfolded Signatures

Lesson 7 – Conclusion
Quizzes and Problem Sets

Quizzes and problem sets should be attempted. The take-home exam will incorporate the problem set and quizzes from these lessons.

Lab Assignment Submission

Email me your lab assignment by the due date.

Final Exam

You will be given a take-home exam and have a week to complete it. Email me the exam when completed.