From: Introduction to Cryptography Course Team <noreply@coursera.org>
Sent: Monday, February 11, 2013 8:26 AM
To: jeeproject@yahoo.com
Subject: Online Cryptography class: week 5

Dear jeffrey epstein,

The week 5 lectures and problem set are now posted on the course web site at

https://crypto.stanford.edu/OnlineCrypto

The problem set is due in three weeks. As usual, there is also an extra credit programming project.

This week's topic is basic key exchange: how to setup a secret key between two parties. For now we only consider protocols secure against eavesdropping. This question motivates the main concepts of public key cryptography, but before we build public key systems we need to take a brief detour and cover a few basic concepts from computational number theory. We will start with algorithms dating back to antiquity (Euclid) and work our way up to Fermat, Euler, and Legendre. We will also mention in passing a few useful concepts from 20th century math. For those seeing this material for the first time I recommend also taking a look at the first four chapters of this book:

http://shoup.net/ntb/ntb-v2.pdf

Next week we will put our hard work from this week to good use and construct several public key encryption systems.

As always, please keep discussing the material on the course forums. The discussions so far have been very good and your posts help improve the course.

Enjoy,
Dan

date-last-viewed 0.0 date-received 1360571144 flags 8623750145 original-mailbox imap://jeevacation@imap.gmail.com/%5BGmail%5D/All%20Mail remote-id 275394