From: Introduction to Cryptography Course Team <noreply@coursera.org>
Sent: Monday, February 18, 2013 8:25 AM
To: jeeproject@yahoo.com
Subject: Online Cryptography class: week 6

Dear jeffrey epstein,

The week 6 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. There is also an extra credit programming project that will enhance your understanding of RSA.

This week's topic is public key encryption: how to encrypt using a public key and decrypt using a secret key. Public key encryption is used for session setup in HTTPS, for key management in encrypted file systems, and for many other tasks. We will see how to use public-key encryption in the video segments.

The videos cover two families of public key encryption systems. One based on trapdoor functions (RSA in particular) and the other based on the Diffie-Hellman protocol. We consider both basic semantic security and security against tampering also known as chosen ciphertext security (CCA security). There has been a ton of research on CCA security over the past decade and given the allotted time we can only summarize the main results from the last few years. The lectures contain suggestions for further readings for those interested in learning more about CCA secure public-key systems. The problem set this week involves a bit more math than usual, but should expand your understanding of public-key encryption. Please don't be shy about posting questions in the forum.

This is the last week of this Crypto I course. I hope everyone learned a lot and enjoyed the material. Crypto is a beautiful topic with lots of open problems and room for further research. I look forward to seeing you in Crypto II where we will cover additional core topics and a few more advanced topics.

The final exam will be made available next week and students will have three weeks to complete the exam. We will send statements of accomplishment once the exam window ends.

Enjoy,
Dan

date-last-viewed 0.0 date-received 1361175940 flags 8623750145 original-mailbox imap://jeevacation@imap.gmail.com/%5BGmail%5D/All%20Mail remote-id 276904