Key exchange (cont'd)
Public-key Encryption

CS 161: Computer Security

Prof. Raluca Ada Popa

Sept 20, 2016

This lecture is on the whiteboard

Announcements

- Project due today
- Homework 1 out, 9/27

Crypto Acronym Party

Security definitions:
IND-KPA -> “known”
IND-CPA C->”chosen”
For both, the attacker chooses m_0 and m_1 but for IND-CPA, it can also query the $Enc_K()$ oracle

Block cipher modes:
CBC -> cipher block chaining because it chains
CTR -> counter
ECB -> electronic code book --- easy

PRG: pseudo random generator
AES: a widely used block cipher