

Outline for October 10, 2025

Reading: *text*, §10.2.3–10.42.5,10.3.2

Due: Homework 1, due October 10; Project selection, due Oct 10

1. Class overview
2. Product ciphers
 - (a) DES
 - i. DES modes
 - (b) AES
3. Public-Key Cryptography
 - (a) Basic idea: 2 keys, one private, one public
 - (b) Cryptosystem must satisfy:
 - i. Given public key, computationally infeasible to get private key;
 - ii. Cipher withstands chosen plaintext attack;
 - iii. Encryption, decryption computationally feasible (*note*: commutativity not required)
 - (c) Benefits: can give confidentiality or authentication or both
4. Use of public key cryptosystem
 - (a) Normally used as key interchange system to exchange secret keys (cheap)
 - (b) Then use secret key system (too expensive to use public key cryptosystem for this)
5. RSA
 - (a) Provides both authenticity and confidentiality
 - (b) Based on difficulty of computing totient, $\phi(n)$, when n is difficult to factor