T-79.5501
Cryptology

Lecture 12 (April 24, 2007):

- Diffie-Hellman Key Exchange
- Diffie-Hellman Problems Sec 6.7.3
- Signature Schemes, Sec. 7.1, and Hash Functions Sec. 7.2.1
- ElGamal signature schemes and forgeries 7.3
- Schnorr's Signature Scheme 7.4.1
- DSA 7.4.2
- Elliptic Curve DSA 7.4.3