T-79.5501
Cryptology

Lecture 11 (Nov 29, 2005):

- ElGamal Cryptosystem and Diffie-Hellman Key Exchange on a multiplicative group
- ECIES, Section 6.5.4
- Signature Schemes, Sec. 7.1, and Hash Functions Sec. 7.2.1
- Schnorr's Signature Scheme 7.4.1
- DSA 7.4.2
- Elliptic Curve DSA