1. Introduction (week 1)
   1. Course Overview (11 min)
   2. What is cryptography? (15 min)
   3. History of cryptography (19 min)
   4. Discrete probability (Crash course) (18 min)
   5. Discrete probability (crash course, cont.) (14 min)
2. Stream Ciphers (week 1)
   1. Information theoretic security and the one time pad (19 min)
   2. Stream ciphers and pseudo random generators (20 min)
   3. Attacks on stream ciphers and the one time pad (24 min)
   4. Real-world stream ciphers (20 min)
   5. PRG Security Definitions (25 min)
   6. Semantic Security (16 min)
   7. Stream ciphers are semantically secure (11 min) [optional]
3. Block Ciphers (week 2)
   1. What are block ciphers? (17 min)
   2. The Data Encryption Standard (22 min)
   3. Exhaustive search attacks (20 min)
   4. More attacks on block ciphers (16 min)
   5. The AES block cipher (14 min)
   6. Block ciphers from PRGs(12 min)
4. Using Block Ciphers (week 2)
   1. Review: PRPs and PRFs (12 min)
   2. Modes of operation: one time key (8 min)
   3. Security for many-time key (23 min)
   4. Modes of operation: many time key (CBC) (16 min)
   5. Modes of operation: many time key (CTR) (10 min)
5. Message Integrity (week 3)
   1. Message Authentication Codes (16 min)
   2. MACs Based On PRFs (10 min)
   3. CBC-MAC and NMAC (20 min)
   4. MAC padding (9 min)
   5. PMAC and the Carter-Wegman MAC (16 min)
6. Collision Resistance (week 3)
   1. Introduction (11 min)
   2. Generic birthday attack (16 min)
   3. The Merkle-Damgard Paradigm (12 min)
   4. Constructing compression functions (8 min)
   5. HMAC (7 min)
   6. Timing attacks on MAC verification (9 min)
7. Authenticated Encryption (week 4)
   1. Active attacks on CPA-secure encryption (13 min)
   2. Definitions (6 min)
   3. Chosen ciphertext attacks (12 min)
   4. Constructions from ciphers and MACs (21 min)
   5. Case study: TLS (18 min)
   6. CBC padding attacks (14 min)
   7. Attacking non-atomic decryption (10 min)
8. Odds and ends (week 4)
   1. Key Derivation (14 min)
   2. Deterministic Encryption (15 min)
   3. Deterministic Encryption:SIV and wide PRP (21 min)
   4. Tweakable encryption (15 min)
   5. Format preserving encryption (13 min)
9. Basic key exchange (week 5)
   1. Trusted 3rd parties (11 min)
   2. Merkle Puzzles (11 min)
   3. The Diffie-Hellman protocol (19 min)
   4. Public-key encryption (11 min)
10. Intro. Number Theory (week 5)
    1. Notation (15 min)
    2. Fermat and Euler (18 min)
    3. Modular e'th roots (17 min)14
    4. Arithmetic algorithms (13 min)
    5. Intractable problems (19 min)
11. Public Key Encryption from trapdoor permutations (week 6)
    1. Definitions and security (16 min)
    2. Constructions (11 min)
    3. The RSA trapdoor permutation (18 min)
    4. PKCS 1 (23 min)
    5. Is RSA a one-way function? (17 min)
    6. RSA in practice (14 min)
12. Public key encryption from Diffie-Hellman (week 6)
    1. The ElGamal Public-key System (23 min)
    2. ElGamal Security (14 min)
    3. ElGamal Variants With Better Security (11 min)
    4. A Unifying Theme (12 min)
    5. Farewell (for now) (6 min)