1. Classical Cryptography
   (a) Basic concepts: encryption/decryption, types of attack, classification of cryptosystems.
   (b) Primitive cryptosystems: shift cipher, affine cipher, substitution cipher, transposition cipher, 
       Vigenère cipher, Hill cipher, ADFGX cipher.
   (c) One time pad, stream ciphers, sequence generators, linear feedback shift registers.

2. Number Theory
   (a) Modular arithmetic, linear equations.
   (b) Euclidean algorithm.
   (c) Fast multiplication.
   (d) Fast modular exponentiation.
   (e) Chinese remainder theorem.
   (f) Modular square roots.
   (g) Fermat’s theorem, Euler’s theorem, and primitive roots.
   (h) Legendre and Jacobi symbols.

3. Block Ciphers
   (a) Feistel networks.
   (b) Data Encryption Standard (DES).
   (c) Modes of operation.
   (d) Storing passwords.
   (e) Attacks on DES.
   (f) Strengthening DES and meet in the middle attacks.