Introduction to Cryptography Midterm Exam

Topics

1. Everything we did in class until Thursday, March 11 (closed interval - Thursday included)
2. Homeworks 1-5.
3. In particular:
    - Basics of symmetric cryptography
    - Key space, key size, security level
    - Substitution Ciphers (Shift Cipher, Affine Cipher and Vigenere Cipher)
    - Classical Permutation Ciphers (Transposition cipher and Permutation cipher)
    - The Greatest Common Divisor (gcd)
    - Euclidean algorithm
    - Modular arithmetic
    - Hill cipher
    - Intro to stream ciphers
    - Random number generators (RNGs) (Linear Congruential Generator, Blum Blum Shub)
    - One-Time Pad (OTP)
    - Linear feedback shift registers (LFSRs)
    - Trivium
    - RC4
    - Block Ciphers, Block Cipher Primitives: Confusion and Diffusion
    - Feistel Cipher (Feistel network)
    - DES, 3DES, Meet in the middle attack, S-boxes, permutations
    - Finite fields (polynomial arithmetic over finite fields modulo polynomials, Finite fields of the form $GF(p^m)$, **inverse elements**)
    - AES
    - Brute-Force Attack against Symmetric Ciphers
    - Block Cipher modes of operations (ECB, CBC, OFB, CFB, CTR)
    - Expected number of false keys
    - Key Whitening