MATH 233: MIDTERM TOPICS

1. Encryption, decryption, and related topics in the following classical cryptosystems (and their variations/combinations).
    - Shift ciphers
    - Affine ciphers
    - Vigenère ciphers
    - Playfair ciphers
    - ADFG(V)X ciphers
    - Hill ciphers
    - One-time pads
2. Number theory topics
    - (Extended) Euclidean algorithm
    - Chinese remainder theorem (both versions)
    - Fermat's little theorem and Euler's theorem
    - Modular exponentiation and primitive roots
    - Square roots in modular arithmetic
    - Legendre and Jacobi symbols
3. RSA cryptosystem
    - Encryption and decryption
    - Primality (compositeness) tests
    - Factoring techniques
4. Discrete logarithm
    - Techniques to compute discrete logs
    - Diffie-Hellman key exchange
    - ElGamal cryptosystem