MATH 233: FINAL TOPICS

1. Everything on the midterm topics list, **excluding** classical cryptosystems
2. LFSR sequences
    - Attacking LFSR sequences using determinants
3. Block ciphers
    - Modes of operation
    - Multiple encryption (meet-in-the-middle attack)
4. Finite fields
    - Definition of addition and multiplication
    - Finding multiplicative inverse
5. DES
    - Encryption/Decryption scheme (Feistel system)
    - Chosen plaintext attack for DES
6. AES
    - Encryption/Decryption scheme (layers)
    - Connection with finite field $GF(2^8)$
7. Hash function
    - Properties of cryptographic hash functions
    - Birthday attack
8. Digital signature
    - RSA and ElGamal signature schemes
    - Digital Signature Algorithm
9. Password protocol
10. Blockchains (**including** Bitcoin overview)
11. Elliptic curves
    - Definition and addition rule (geometric/algebraic)
    - Prime factorization using elliptic curves
    - Discrete log problem on elliptic curves
    - Elliptic curve cryptography (Diffie-Hellman/ElGamal/signature)