Syllabus

1. Introduction
    a. Basic Communication: Alice, Bob, and Mallory
    b. Remote Coin Flipping
    c. General Overview of Secure Transactions
    d. Bit Commitment, One Way Functions, Modular Arithmetic, GCD, EEA, Large Integer Arithmetic
    e. RSA, Diffie-Hellman Key Exchange
    f. Authentication, Attacks
2. Public Key Cryptography
    a. RSA, DH, DSA, One-Way Trapdoor Functions
    b. Modular Arithmetic, Extended Euclidean Algorithm
    c. Fermat's Little Theorem
    d. Prime Numbers and Generation, Prime Number Theorem
    e. Primality Testing, Miller-Rabin Test, Sieving
    f. Elliptic Curve Cryptography, ECDH, ECDSA
3. Symmetric Cryptography
    a. Hash Functions, Merkle-Damgård Construction, SHA-1, SHA-2, SHA-3
    b. Block and Stream Ciphers, Mode of Operation, Feistel Ciphers
    c. Random Number Generation
    d. Confidentiality and Integrity
    e. RC4, DES, AES
    f. MAC: Message Authentication Codes, HMAC
4. Cryptanalysis
    a. Adversaries and attack models
    b. Wiretaps and a little bit of history
    c. Linear and Differential Cryptanalysis
5. Security Protocols
    a. SSL/TLS: Confidentiality, Integrity, Authentication
    b. Kerberos and OAuth
    c. Public Key Infrastructure (PKI), Certificates, and Trust Model
    d. Synopsis of an Attack: Flame
    e. Message Based Protocols
    f. Challenge-Response Protocols
    g. Proofs of Knowledge, Zero Knowledge Proofs
    h. Password-Based Cryptography
    i. Quorum Cryptography, Secret Sharing, Threshold Schemes
6. Elections
    a. Traditional Voting Methods
    b. Verifiable elections
    c. Privacy
    d. Auditing
    e. Mix Nets
    f. Tallying, Consensus, Ballots
    g. Homomorphic Elections
7. Homomorphic Cryptography and Multi-Party Computation
    a. Bilinear Maps

    b. Homomorphic Transforms
    c. Homomorphic Encryption
    d. MPC
    e. Group Signatures
8. Side Channel Attacks
    a. Fault, timing, Cache, Power, EM, Acoustic
9. Block Chains and Cyber Currencies
    a. What is Money?
    b. What is a block chain?
    c. BitCoin and derivatives
    d. Cyber currencies, decentralization
    e. Hype and Reality
    f. Security Analysis and Attacks
10. Payments
    a. How Credit Cards Work?
    b. EMV and Chip Cards
    c. Tap-to-Pay with mobile devices
    d. Web Payments
    e. Tokenization
11. Hardware Cryptography
    a. Smart Cards
    b. Hardware Security Modules (HSM)
    c. Trusted Platform Module (TPM)
    d. Virtualized cryptographic processors
    e. Secure Boot, Attestation, Sealing
12. Quantum Computation and Cryptography
    a. Search and Period Finding
    b. Factorization
    c. Quantum Computers
13. Cryptography Policy
    a. Politics of Crypto and a Historical Walkthrough
    b. Export/Import Controls and National Security
    c. Key Escrow, Key Recovery Alliance, Clipper
    d. Copyright, DMCA, Whitebox Cryptography, Obfuscation, Rights Management
    e. Current Political Landscape: FBI vs Apple, DoJ vs Microsoft, etc.