Review

1. Symmetric ciphers, asymmetric ciphers, cryptographic hashes: design requirements, computational margins.
2. Kinds of attacks: Cipher-text only, corresponding plaintext/ciphertext, chosen cipher-text.
3. Classical Crypto
    a. Frequency curves
    b. Multialphabetic substitutions: aligning alphabets.
    c. One time pads
    d. IC
    e. Runs
    f. Group theory: Decomposing complex transformations into simple ones
    g. Cycle structure and similarity
    h. Enigma
    i. Probable Words
4. Information theory and Unicity
    a. Entropy
    b. Mutual information
5. Euclidean algorithm and equation solving
6. Stream Ciphers
    a. LFSRs as recurrence
    b. Breaking LSFRs and non-linear filter SRs: correlation attacks.
    c. Berlekamp-Massey.
7. Block ciphers
    a. Confusion and diffusion.
    b. Simple attacks: parallel systems, mixing.
    c. Feistel Ciphers
    d. DES
    e. DES expressed as basic transformations
    f. AES
    g. Field inversion and high degree substitutions
    h. Linear and differential attacks.
    i. Functions as polynomials.
    j. Walsh transformations and linear approximation.
    k. Balance.
    l. Berlekamp factoring
8. Time Memory Trade-offs, Man in the Middle Attacks (especially for Diffie Hellman).
9. Factoring based public key methods
    a. Addition, multiplication, exponential mod p
    b. RSA algorithm.
    c. Chinese remainder Theorem
    d. Inverses mod p, mod ϕ(p), solving equations in the integers.

e. Glitching attacks, common modulus attack.
f. Montgomery multiplication.
g. Primality testing.
h. Prime number theorem.
i. Fermat/Euler's theorem.
j. Quadratic reciprocity.
k. Quadratic sieve.
l. Universal exponents
m. Factoring: $x^2-y^2= (x-y)(x+y)$
n. Pollard p-1
o. Lattice and lattice attacks
p. Timing attacks
q. Factor Bases

10. Discrete Log problem
    a. El Gamal
    b. Diffie Hellman
    c. Primitive elements.
    d. Baby step – Giant step
    e. Qquare root mod p, mod n (CRT)
    f. NP completeness
    g. Index calculus
11. Cryptographic Hashes
    a. 1-wayness
    b. Collision resistance.
    c. SHA-1, SHA-2, MD4/5.
    d. Multicollisions.
    e. Birthday attacks.
12. Elliptic curves.
    a. Group structure: adding and subtracting, tangents.
    b. The Elliptic Group
    c. Point counting
    d. Picking curves
13. Solving equations.
    a. SAT
    b. Linear equations