Planned Coverage

- Topic-1: Introduction to Crypto Landscape, Pseudorandom objects
    - Landscape of Crypto - Idea of functionality/task, primitive, assumption and security model
    - Examples of OTP, PRG, (supplementary reading: Joy of Crypto Chapter-1,2,4,5)
    - Diffie-Hellman KEX to achieve secure communication.
    - Security def, OWF (Bellare-Goldwasser, Chap 2.1, 2.2, 2.3, 2.3.1)
    - Hardcode Predicate, OWF + HP -> PRG
    - Goldreich-Levin (Goldreich Levin construction, proof (optional)), (Bellare-Goldwasser 2.4.1, Pass Lecture Notes)
    - PRG expansion (Boneh Shoup, Chapter 3.4); PRF
    - PRG->PRF (Boneh Shoup Chapter 4.4; Joy of Crypto Chapter 6); GGM Construction (Joy of Crypto Chapter 6); Naor-Reingold (Original Paper, Survey-Section-4.1)
- Topic-2: Public-key Encryptions and Commitments
    - El-Gammal and its variants, additive homomorphism (Joy of Crypto - Chapter 15.3, Boneh-Shoup Chapter 11.5)
    - CCA-security, Fujisaki-Okamoto (Boneh-Shoup 12.2, 12.2, 12.6), Cramer-Shoup (Boaz Barak Note)
    - Commitment Schemes (Damgard-Nielsen)
- Topic-3: Zero-knowledge Proofs
    - Proof of Knowledge, Schnorr (Boneh-Shoup Chapter-19.1)
    - More Sigma Protocols, Generalization (Sec 4.1 and 4.2 from https://eprint.iacr.org/2024/1713.pdf)
    - Existential Soundness OR proofs, Existential Soundness (Boneh Shoup Chapter-19 and Chapter-20)
- Topic-4: Basic Multi Party Computation
    - Introduction to MPC (additional material on simulation: https://eprint.iacr.org/2016/046.pdf, Section-4 for Semi-honest)
    - Oblivious Transfer (additional material: https://crypto.stanford.edu/pbc/notes/crypto/ot.html)
    - Garbled Circuit and Shamir's secret sharing. (additional material: https://people.eecs.berkeley.edu/~sanjamg/classes/cs276-fall14/scribe/lec17.pdf)
- Topic-5: Advanced Multi Party Computation and ZK from MPC
    - GMW protocol, GMW compiler (https://people.eecs.berkeley.edu/~sanjamg/classes/cs276-fall14/scribe/lec16.pdf , https://www.cs.umd.edu/~jkatz/gradcrypto2/f13/lecture13.pdf)
    - BGW protocol (https://www.cs.umd.edu/~jkatz/gradcrypto2/f13/lecture13.pdf, a full proof)

    - Beaver's protocol (Boneh Shoup - 23.2) Universal Composability (https://www.youtube.com/watch?v=5kF3TxEt-_A&list=PLqc9MPlwib9nSuyH4oUIwPsyDiZ4bwuEE)
    - MPC in the head (https://people.eecs.berkeley.edu/~sanjamg/assets/classes/cs294-spring16/scribes/15.pdf)
- Topic-6: Lattice-based Crypto (Lecture Notes by Vinod)
    - Basic of lattice based crypto, Regev Encryption (from LWE) [https://eprint.iacr.org/2015/939.pdf ; https://cims.nyu.edu/~regev/papers/pqc.pdf, https://people.csail.mit.edu/vinodv/CS294/lecture1.pdf];
    - Fully Homomorphic Encryption - GSW (MW paper Section 5.1)
    - GPV signature (from SIS) (GPV paper, https://eprint.iacr.org/2015/939.pdf ,ROM chapter Katz Lindel)
- Topic-7: Pairing based Crypto
    - Day-19: Basic of Pairing (https://pratmukh.wordpress.com/wp-content/uploads/2025/11/pairing-notes-bellare.pdf)
    - BLS signature (https://pratmukh.wordpress.com/wp-content/uploads/2025/11/pairing-notes-bellare.pdf)
        - Additional reading: VRF (unpredictability vs Pseudorandomness) [Chainlink Blog - https://chain.link/education-hub/verifiable-random-function-vrf]
    - Boneh-Franklin IBE (https://crypto.stanford.edu/~dabo/papers/bfibe.pdf)
    - Additional Reading: Polynomial/Vector commitments (https://www.iacr.org/archive/asiacrypt2010/6477178/6477178.pdf)
        1. PLONK https://www.youtube.com/watch?v=A0oZVEXav24
        2. Online ZKP Mooc https://zk-learning.org/
- Topic-8 (1): Threshold Cryptography
    - Threshold PKE (Boneh-Shoup)
    - Threshold BLS; (Distributed) and PRF (https://eprint.iacr.org/2018/727.pdf)
    - Multi-signature (Boneh-Shoup, https://crypto.stanford.edu/~dabo/pubs/papers/BLSmultisig.html#BNN07)
    - Additional reading: VRF (https://eprint.iacr.org/2020/096.pdf);
    - Additional Reading: Threshold Schnor (https://eprint.iacr.org/2022/374.pdf)

Books:

- A Graduate Course in Applied Cryptography - Dan Boneh and Victor Shoup (https://toc.cryptobook.us/book.pdf)
- Introduction to Modern Cryptography (3rd edition) - Jonathan Katz and Yehuda Lindell http://www.cs.umd.edu/~jkatz/imc.html
- The Joy of Cryptography - Mike Rosulek https://joyofcryptography.com/pdf/book.pdf
- Foundation of Crypto - Goldreich (https://www.wisdom.weizmann.ac.il/~oded/foc.html)

Other Resources:

- Lecture Notes: Bellare-Goldwasser https://cseweb.ucsd.edu/~mihir/papers/gb.pdf
- Course Webpage: Andrew Miller (UIUC) https://soc1024.ece.illinois.edu/teaching/ececs407/fa21/
- Course Webpage: Sanjam Garg (UC Berkeley) https://people.eecs.berkeley.edu/~sanjamg/classes/cs276-fall16/
- Lecture Notes on Lattices by Vinod (MIT) https://people.csail.mit.edu/vinodv/CS294/lecturenotes.pdf