Date	Topic	Reading	Homework
Aug 19, 2024	Course Introduction	Read Chapter 1	problem 1
Aug 21, 2024	Mathematical Review of Number Theory, Probability Theory, and Notations	Read Chapter 2	
Secret Key Cryptography			
Sep 4, 2024	Chapter 2: Encryption	Read Chapter 3	
Sep 9, 2024	Chapter 3: Stream Ciphers (Part 1)		
Sep 11, 2024	Chapter 3: Stream Ciphers (Part 2)	Read Chapter 4	
Sep 16, 2024	Chapter 4: Block Ciphers (Part 1)		
Sep 18, 2024	Chapter 4: Block Ciphers (Part 2)	Read Chapter 5	
Sep 23, 2024	Chapter 5: Chosen Plaintext Attacks	Reach Chapter 6	
Sep 25, 2024	Chapter 6: Message Integrity	Reach Chapter 7	
Sep 30, 2024	Chapter 7: Message Integrity from Universal Hashing		
Oct 2, 2024	Mid-Term Exam	Read Chapter 8	
Oct 7, 2024	Chapter 8: Message Integrity from Collision Resistant Hashing	Read Chapter 9	
Oct 9, 2024	Chapter 9: Authenticated Encryption	Read Chapter 10	
Public Key Cryptography			
Oct 14, 2024	Chapter 10: Public Key Tools One-Way Trapdoor Functions DIffie-Hellman Key Exchange		
Oct 16, 2024	Chapter 11: Public Key Encryption ElGamal RSA		
Oct 21, 2024	Chapter 13: Digital Signatures		
Oct 23, 2024	Chapter 14: Fast Signatures from One-Way Functions		
Oct 28, 2024	Chapter 15: Elliptic Curve Cryptography and Pairings		
Nov 4, 2024	Chapter 16: Attacks on Number Theoretic Assumptions		
Nov 6, 2024	Mid-Term Exam	Study for the exam	
Protocols			
Nov 11 2024	Chapter 18: Protocols for Identification and Login		
Nov 13, 2024	Chapter 19: Identification and Signatures from Sigma Protocols		
Nov 18, 2024	Chapter 20: Proving Properties in Zero-Knowledge		
Nov 20, 2024	Chapter 21: Authenticated Key Exchange		
Nov 27, 2024	Chapter 22: Threshold Cryptography		
Dec 2, 2024	Review and Catch-Up		
Dec 5, 2024	Final Exam		