This schedule is tentative.

Unit	Week #	Date range	Agenda	Note
Applied Cryptography	Week 1	Jan 6-10	• Overview, Hash function constructions • Hash application (password authentication) • Entropy & extraction, Pseudorandom generators	
	Week 2	Jan 13-17	• One-Time Pad / Stream Ciphers • Block Ciphers and modes of operations	
	Week 3	Jan 20-24	• MACs • Authenticated encryption	Quiz1 (Jan20)
	Week 4	Jan 27-31	• Number theory • Diffie-Hellman / Elgamal, public key • Digital signature	
OS Security	Week 5	Feb 3-7	• Access control matrix • Access control list and capabilities • SUID	Quiz2 (Feb5) Assignment1 release
	Week 6	Feb 10-14	• Confidentiality policy • Integrity policy • Hybrid policy • Chinese wall	Assignment1 due (Feb 10) Assignment2 release
	Week 8	Feb 17-21	Winter reading week	Assignment2 due (Feb 17)
Software and web security	Week 9	Feb 24-Feb28	• Architecture • Buffer overflow • Format string	Assigment3 release
	Week 10	Mar 3 -7	• Malicious logics and countermeasures • SQL injection	**First exam (Mar 3)** Assignment4 release
	Week 11	Mar 10-14	• Secure web application (cross-site scripting) • Cookies	Assignment3 due (Mar10) Quiz3 (Mar12)
Threat detection and investigation	Week 12	Mar 17-21	• Intrusion detection • Evading IDS • Provenance auditing	Assignment4 due (Mar 19)
Network Security	Week 13	Mar 24-28	• Security of different network layers • Confidentiality/anonymity on the Internet	
	Week 14	Mar 31-Apr 4	TBD	Assignment5 due (Mar31) **Second Exam (Date determined by faculty)**