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 • MACs • Authenticated encryption	
	Week 3	Jan 20-24	• Number theory • Diffie-Hellman / Elgamal, public key • RSA • Digital signature	Quiz1 (Jan20)
OS Security	Week 4	Jan 27-31	• PKI • Access control matrix • Access control list and capabilities • UNIX security	
	Week 5	Feb 3-7	• Confidentiality policy • Integrity policy • Hybrid policy	Quiz2 (Feb5) Assignment1 release
Software and web security	Week 6	Feb 10-14	• Chinese wall • Memory fundamentals • Buffer overflow	Assignment1 due (Feb 10) Assignment2 release
	Week 7	Feb 17-21	Winter reading week	
	Week 8	Feb 24-Feb28	• Format string • Malicious logics and countermeasures • Web	Assignment2 due (Feb 24) Assigment3 release
	Week 9	Mar 3 -7	• Midterm • Cookies • SQL injection	**First exam (Mar 3)** Assignment4 release
Threat detection and investigation	Week 10	Mar 10-14	• Secure web application (XSS and CSRF) • Session management • Intrusion detection1 (Auditing+ anomaly-based IDS)	Assignment3 due (Mar10) Quiz3 (Mar12)
	Week 11	Mar 17-21	• Intrusion detection2 (accuracy+signature-based) • Evading IDS • Data provenance • Network background	Assignment4 due (Mar 19)
Network Security	Week 12	Mar 24-28	• Network attacks • Guest lecture (provenance evasion) • firewalls	
	Week 13	Mar 31-Apr 4	• Anonymity on the Internet	Assignment5 due (Mar31) **Second Exam (Date determined by faculty)**