Event	Date	Topic	Kaufman et al.	Stallings
L 1	Wed 9.3	Introduction to data security	Chapter 1	Chapter 1
L 2	Fri 11.3	Classical cryptosystems; Introduction to modern cryptography	Chapter 2	Chapter 2; Chapter 7
H 1	Tue15.3 / Fri 18.3			
L 3	Wed 16.3	Block ciphers: DES, IDEA, AES	Chapter 3	Chapters 3,5
L 4	Fri 18.3	LFSR; Stream ciphers: RC4, UMTS f8; Block ciphers: modes of operation	- Chapter 4	Chapter 6 Chapter 3
H 2	Tue 22.3 / Fri 1.4			
L 5	23.3	Hash-functions and MACs	Chapter 5	Chapters 11,12
H 3	Tue 5.4/ Fri 8.4			
L 6	6.4	Modular arithmetic; Euclid's algorithm, Chinese remainder theorem, Euler's totient function, Euler's theorem	Chapter 6.1-2 Chapter 7	Chapter 8
L 7	8.4	Public key cryptosystems: RSA Prime number generation	Chapter 6.3	Chapter 9.1-2 Chapter 8
H 4	Tue 12.4/ Fri 15.4			
L 8	13.4	Public key cryptosystems: Diffie-Hellman, DSS; Polynomial arithmetic	Ch. 6.4-7; Chapter 8	Chapters 5, 8, 10
H 5	Tue 19.4/ Fri 22.4			
L 9	20.4	Principles of Authentication; Digital Signatures	Ch. 6.3; 6.5	Chapter 13
10	22.4	Random number generation; Distribution of symmetric keys; Management of public keys	Chapter 11.6; Chapter 9.7-8; Chapter 15	Chapter 7.4; Chapter 7.3; Chapters 14, 15
H 6	Tue 26.4/ Fri 29.4			
L 11	27.4	Pretty Good Privacy (PGP); SSL/TLS; IPSec	Chapter 15; 17; 18; 19	Chapters 16; 17;18
L 12	29.4	Cancelled		-