Spring 2022

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reading
January 24	25 Introduction Services	26	27 Modular Math Historic Ciphers	28	**29**	**30**	P&P. Chap 1 Stall. 1, 2.1-2.3 Stall. 3.1-3.4 Stall. 5.1-5.3
31	**February 1** More Historic Ciphers	2	3 Stream Ciphers PRNG/OTP	4 **HW1 Due**	**5**	**6**	P&P. Chap 2 Stall. 8.1-8.4 Stall. 8.6
7	8 LFSRs **Quiz 1**	9	10 DES	11 **HW2 Due**	**12**	**13**	P&P. Chap 3 Stall. Chap 4 Stall. 7.1
14	15 Galois Fields **Quiz 2**	16	17 AES	18 **HW3 Due**	**19** Historical Ciphers **Project Due**	**20**	P&P. Chap 4 Stall. 5.4-5.7 Stall. Chap 6
21	22 AES **Quiz 3**	23	24 Modes of Operation	25 **HW4 Due**	**26** Breaking Ciphers **Project Due**	**27**	P&P. Chap 5 Stall. Chap 7
28	**March 1** Multi- Encryption **Quiz 4**	2	3 Number Theory	4 **HW5 Due**	**5**	**6**	P&P. Chap 6 Stall. 2.4-2.5
7	8 Review **Quiz 5**	9	10 **Midterm** **Exam**	11	**12**	**13**	
14	15	16	17	18	**19**	**20**	
Spring Recess							
21	22 RSA	23	24 Side Channel Analysis	25	**26**	**27**	P&P. Chap 7 Stall. 9
28	29 Diffie- Hellman	30	31 Discrete Log Problem	**April 1** **HW6 Due**	**2** SCA CPA Aquisition **Project Due**	**3**	P&P. 8.1-8.4 Stall. 2.8, 10.1
4	5 Digital Signatures **Quiz 6**	6	7 Hash Functions	8 **HW7 Due**	**9** SCA CPA Analysis **Project Due**	**10**	P&P. 10.1-10.2, P&P. Chap 11 Stall. 13.1, 13.4 Stall. 11.1-11.6
11	12 MAC **Quiz 7**	13	14 Key Manage- ment, PGP	15 **HW8 Due**	**16** SCA T-Test **Project Due**	**17**	P&P. Chap 12 P&P. 13.1 Stall. Chap 12 Stall. 14.1-14.2,

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Reading
18	19 PKI **Quiz 8**	20	21 Elliptic Curve Introduction	22 **HW9 Due**	**23** PGP Setup **Project Due**	**24**	P&P. Chap 9 P&P. 13.2-13.3 Stall. 10.2-10.4 Stall. 14.3-14.5
25	26 Elliptic Curve Cryptography **Quiz 9**	27	28 Post Quantum Cryptography	29 **HW10 Due**	30	**May 1**	P&P. 10.5 Stall. 13.5
2	3 Timing Side Channel **Quiz 10**	4	5 Review	6	**7** PGP **Project Due**	**8**	
9 Reading Day	10 Reading Day	11 Start Exam Period	12	13	**14**	**15**	
16 **Final Exam 1:30-4:15pm**	17	18	19 End Exam Period	20	**21**	**22**	

Reading Assignments Example

P&P. Chap 1	Reading from Christof Paar and Jan Pelzl, Chapter 1
Stall. 1,2.1-2.3	Reading from Stallings Chapter 1 and Chapters 2.1 through 2.3

Lectures Tuesday / Thursday 3:00 pm – 4:15 pm MTB 1006

The Course Schedule is Subject to Change!!!

Last updated 01/13/22