SY308: Security Fundamental Principles

Calendar	Policy

Course Calendar

January 2020						
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
			1	2	3	4
5	6 Plebe Major brief	7 Introduction	8 Security principles	9	10 Private-Key Encryption	11 HW01
12	13 Probability basics	14	15 Perfect Secrecy	16	17 Perfect Indistinguishability, OTP w/ python	18 HW02
19	20 ML King Jr Day	21	22 Perfect Indistinguishability, OTP w/ python	23	24 Limitation of Perfect Secrecy	25 HW03
26	27 Computational Indistingushability	28	29 IND-CPA	30	31 IND-CPA	

February 2020

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
						1 HW04
2	3 Enc w/ python	4	5 Modes of operation	6	7 Lab: Implementing CBC	8 HW05
9	10 Project Pt I	11	12 6-Week Exam 6Wk Exam	13	14 Exam review	15 HW06
16	17 Presidents Day	18	19 MAC	20	21 HMAC	22 HW07
23	24 Authenticated Encryption	25	26 Number Theory	27	28 Key Exchange	29

March 2020

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2 Key Exchange	3	4 ElGamal PKE	5	6 RSA PKE	7 HW08
8	9 Spring break	10 Spring break	11 Spring break	12 Spring break	13 Spring break	14 Project Pt Ia
15	16 RSA PKE	17	18 Digital Signature	19	20 PKI	21 HW09 Project Pt 2/2a
22	23 TLS	24	25 C: Hello World! GDB	26	27 C: Hello World! GDB	28
29	30 12Wk Exam	31				

April 2020

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
			1 12Wk Exam From MAC to TLS Exam Review	2	3 C: Pointers and Memory layout	4
5	6 C: Strings C: File operations	7	8 Buffer overflow	9	10 Shellcode Call Stack	11 HW10
12	13 Stack Smashing Attack	14	15 NOP Sled Lab: Stack smashing	16	17 Buffer-overflow Defenses	18 HW11
19	20 Format String Attack	21	22 Capstone day	23	24 SS + FS: Bypassing the stack protection	25 HW12
26	27 Survey	28 Spring Term Ends	29	30		

May 2020

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						