

Math 316, S2017, Unit 3 Plan

Mon	Wed	Fri
Mar 27, 2017	Mar 29, 2017	Mar 31, 2017
12.4, 12.5 Quadratic Reciprocity, Fast Comp'n <i>For next class:</i> RQ 13.5, 13.6 D 13.3: 1*, 2*, 3*, 4*; 13.4: 2* W 12.5: 7	13.3, 13.4 Euler Ps-primes, Solovay-Strassen Test <i>For next class:</i> RQ 10.1, 10.2, 14.1, 14.2 D 13.6: 1*, 2, 3, 7 W 13.4: 3*	13.5, 13.6 Strong Ps-primes, The Miller-Rabin Test <i>For next class:</i> RQ 9.6, 10.3 D 10.2: 3, 4, 5, 6 W 13.6: 9*
Apr 3, 2017	Apr 5, 2017	Apr 7, 2017
10.1, 10.2 Sun Ze's Thm; 14.1, 14.2 Basic Public-Key Protocol, Secret-Sharing <i>For next class:</i> RQ 14.3, 14.4 D 9.6: 2*, 3*; 10.3: 3, 6, 7 W 10.2: 7	9.6, 10.3 Squares Roots mod p and mod n Quiz 3 (10.1-10.2) <i>For next class:</i> RQ 16.1, 16.2, 16.3 D 14.3: 1*-6*; 14.4: 1*, 2* W 10.3: 4	14.3, 14.4 Oblivious Transfer, Zero Knowledge Proofs <i>For next class:</i> RQ 16.4 D 16.3: 1, 2, 3 W 14.3: 7*
Apr 10, 2017	Apr 12, 2017	Apr 14, 2017
16.1, 16.2, 16.3 pRNGs, LCGs <i>For next class:</i> RQ 16.6 D 16.3: 1, 2, 3 W 16.3: 4	16.4 LFSGs <i>For next class:</i> RQ 18.1 D 16.4: 1, 3*, 4* W 16.4: 5*	Good Friday
Apr 17, 2017	Apr 19, 2017	Apr 21, 2017
Easter Monday	16.6 BBS Generator <i>For next class:</i> W 16.6: 4*	Exam 3 <i>For next class:</i> RQ 18.2 D 18.1: 1, 2, 3

*Please see "Additions/Modifications to Homework Problems" on Blackboard.