Math 316, S2016, Unit Plan (04/17 ver.)

Mon	**Wed**	**Fri**
Mar 28, 2016	Mar 30, 2016	Apr 1, 2016
Easter Monday *For next class:* RQ 14.3	14.1, 14.2 Basic Public-Key Protocol, Secret-Sharing *For next class:* RQ 14.4 D 14.3: 1*, 2*, 3*, 4*, 5*, 6* W 10.2: 7	14.3 Oblivious Transfer *For next class:* RQ 16.1, 16.2, 16.3 D 14.4: 1*, 2*, 3* W 14.3: 7*
Apr 4, 2016	Apr 6, 2016	Apr 8, 2016
14.4 Zero Knowledge Proofs *For next class:* RQ 16.4 D 16.3: 1, 2, 3 W 14.4: 4*	16.1, 16.2, 16.3 pRNGs, LCGs *For next class:* RQ 16.6 D 16.4: 1, 3*, 4* W 16.3: 4	16.4 LFSGs *For next class:* RQ 18.1 D 16.6: 1*, 2*, 3* W 16.4: 5*
Apr 11, 2016	Apr 13, 2016	Apr 15, 2016
16.6 BBS Generator **Quiz 3** *For next class:* RQ 18.2 D 18.1: 1, 2, 3 W 16.6: 4*	18.1 Pollard's Rho Method *For next class:* RQ 18.3 D 18.2: 1, 2, 3 W 18.1: 4*	18.2 Pollard's *p*-1 Method *For next class:* W 18.2: 4
Apr 18, 2016	Apr 20, 2016	Apr 22, 2016
Exam 3 *For next class:* RQ 18.4 D 18.3: 1, 2, 3	18.3 Pocklington-Lehmer Criterion *For next class:* RQ 18.5 D 18.4* W 18.3:	18.4 Strong Primes *For next class:* RQ 19.1 D 18.5* W 18.4*

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