

Mon	Wed	Fri
Feb 20, 2017	Feb 22, 2017	Feb 24, 2017
<p align="center">Exam 1</p> <p><i>For next class:</i> RQ 4.5A D 4.4: 1, 2, 3, 4*, 5*, 8*</p>	<p align="center">4.4 Expected Values</p> <p><i>For next class:</i> RQ 4.5B D 4.5: 7*, 8*, 9*, 10* W 4.4: 10</p>	<p align="center">4.5A Friedman Attack</p> <p><i>For next class:</i> RQ 7.1, 7.2 D 4.5B: 12* W 4.5: 11*</p>
Feb 27, 2017	Mar 1, 2017	Mar 3, 2017
<p>4.5B Friedman Attack (con't)</p> <p><i>For next class:</i> RQ 9.5 D 7.2: 1, 2, 4, 5, 10 W 4.5: 12*</p>	<p align="center">7.1, 7.2 Trapdoors, The RSA Cipher</p> <p><i>For next class:</i> RQ 7.4-5 D 9.5: 1, 2, 5, 9* W 7.2: 8</p>	<p align="center">9.5 Exponentiation Algorithm</p> <p><i>For next class:</i> RQ 7.5 D 7.3: 1-3, 5-9 W 9.5: 12</p>
Mar 6, 2017	Mar 8, 2017	Mar 10, 2017
<p align="center">7.3 Primitive Roots, Discrete Logs; 7.4 DH Key Exchange</p> <p><i>For next class:</i> RQ 13.1, 13.2 D 7.5: 1, 2, 3* W 7.3: 4*</p>	<p align="center">7.5 ElGamal Cipher Quiz 2 (7.3)</p> <p><i>For next class:</i> RQ 10.8, 12.1-12.3 D 13.1: 1, 2, 7*, 8; 13.2: 1, 2 W 7.5: 4*</p>	<p align="center">13.1, 13.2 F. Pseudoprimes, Non-prime Ps-primes</p> <p><i>For next class:</i> RQ 12.4, 12.5 D 12.3: 1* W 13.2: 3</p>
Mar 13, 2017	Mar 15, 2017	Mar 17, 2017
<p align="center">10.8, 12.1-12.3 Euler's Criterion, Quadratic Symbols</p> <p><i>For next class:</i> W 12.3: 2*</p>	<p align="center">Exam 2</p> <p><i>For next class:</i> Read 3.1, 3.2</p>	<p align="center">3.1, 3.2 Cryptograms and Anagrams</p> <p><i>For next class:</i> RQ 13.3, 13.4 D 12.5: 1, 2, 3, 4, 5, 6</p>

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