

Mon	Wed	Fri
Feb 22, 2016	Feb 24, 2016	Feb 26, 2016
<p>Exam 1</p> <p><i>For next class:</i> RQ 4.5 D 4.4: 1, 2, 5, 9, 10</p>	<p>4.4 Expected Values</p> <p><i>For next class:</i> RQ 7.1, 7.2A D 4.5: 1, 2 W 4.4: 11</p>	<p>4.5 Friedman Attack</p> <p><i>For next class:</i> RQ 7.2B D 7.2: 1, 2, 3, 4, 5</p>
Feb 29, 2016	Mar 2, 2016	Mar 4, 2016
<p>7.1 Trapdoors 7.2A The RSA Cipher</p> <p><i>For next class:</i> RQ 7.3 D 7.2: 9, 10 W 4.5: 3, 7.2: 6</p>	<p>7.2B The RSA Cipher</p> <p><i>For next class:</i> RQ 7.5 D 7.3: 1-3, 5-9 W 7.2: 8</p>	<p>7.3 Primitive Roots, Discrete Logs</p> <p><i>For next class:</i> RQ 13.1, 13.2 D 7.5: 1, 2, 3* W 7.3: 4*</p>
Mar 7, 2016	Mar 9, 2016	Mar 11, 2016
<p>7.4, 7.5 Diffie-Hellman Key Exchange, ElGamal Cipher</p> <p><i>For next class:</i> RQ 13.3, 13.4 D 13.1: 1, 2, 7*, 8; 13.2: 1, 2 W 7.5*</p>	<p>13.1, 13.2 F. Pseudoprimes, Non-prime Pseudoprimes Quiz 2</p> <p><i>For next class:</i> RQ 13.5, 13.6 D 13.3: 1*, 2*; 13.4: 2* W 13.2: 3</p>	<p>13.3, 13.4 Euler Ps-primes, Solovay-Strassen Test</p> <p><i>For next class:</i> RQ 14.1, 14.2 D 13.6: 1, 2, 3, 4, 5, 7 W 13.4: 1</p>
Mar 14, 2016	Mar 16, 2016	Mar 18, 2016
<p>13.5, 13.6 Strong Ps-primes, The Miller-Rabin Test</p> <p><i>For next class:</i> W 13.6: 6</p>	<p>Exam 2</p> <p><i>For next class:</i> Read 3.1, 3.2</p>	<p>3.1, 3.2 Cryptograms and Anagrams</p> <p><i>For next class:</i> RQ 14.3</p>

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