

**Computer Science 349 Draft Syllabus**  
*Cryptography*  
*Spring 2004*

<p>Thursday, January 29  Reading    Supplementary  Handouts</p>	<p>What me worry?  Singh, Introduction, and Chapter 1,  Stinson, Introduction and §1.1.1, 1.1.2, 1.1.3  <i>Secrets and Lies</i>, Bruce Schneier, Chapters 1 -- 4  Introduction, Transparencies §1  Assignment 1, due Thursday, February 5</p>
<p>Monday, February 2  Reading    Supplementary    Handouts</p>	<p>Decrypted secrets: Classic conventional cryptography  Singh, Chapter 2  Stinson, §1.1.4, 1.1.6, 1.1.7. 1.2.1, 1.2.2  Stinson, §1.1.5  <i>Decrypted Secrets</i>, B.L. Bauer §14. – 14.4  Transparencies §2</p>
<p>Thursday, February 5  Reading  Handout  Due in class</p>	<p>Modular arithmetic and affine ciphers  Singh, Chapter 3  Assignment 2, due Thursday, February 12  Assignment 1</p>
<p>Monday, February 9  Reading  Supplementary    Handout  Return</p>	<p>Cracking the Enigma  Singh, Chapter 4  <i>Decrypted Secrets</i>, B.L Bauer §14.4  <i>Breaking the Code</i>, by Hugh Whitmore  Transparencies §3  Grade assignment 1</p>
<p>Thursday, February 12  Reading  Supplementary  Handouts    Due in class</p>	<p>The strange affair of G.W. Kulp  Stinson, §1.2.3, 1.2.4, 1.2.5, 1.3  <i>Decrypted Secrets</i>, B.L Bauer Chapter 17, §18.1  Transparencies §4,  Assignment 3, due Thursday, February 19  Assignment 2</p>
<p>Monday, February 16</p>	<p>President's day, no class</p>
<p>Thursday, February 19  Reading  Handout    Return  Due in class</p>	<p>Introduction to probability theory  Stinson, § 2.1, 2.2  Transparencies §5  Assignment 4, due Thursday, February 26  Graded assignment 2  Assignment 3</p>
<p>Friday, February 20      Reading      No additional handouts</p>	<p>Shannon's theory of secrecy systems  Perfect secrecy encoding  (Monday's schedule)  Stinson, §2.3</p>

Monday, February 23 Reading Supplementary  Handouts Return:	Entropy and Huffman Stinson, § 2.4 Disappearing cryptography, by Peter Wayner Chapters 5 -- 8  Transparencies §6 Graded assignment 3
Thursday, February 26 Reading Handout  Due in class	Properties of entropy Stinson, §2.5 Transparencies §7 Assignment 5, due Thursday, March 4 Assignment 4
Monday, March 1 Reading Handout Return	Spurious keys Stinson §2.6 Transparencies §8 Graded assignment 4
Thursday, March 4 Reading No additional handouts Due in class	Unicity distance Stinson §2.6  Assignment 5
Monday, March 8 Reading Handout Supplementary	Hiding in plain sight: An intro to steganography Singh, Chapter 5 Transparencies §9 Information Hiding: Techniques for Steganography And Digital Watermarking, Chapters 1
Thursday, March 11	Midterm examination 1
Monday, March 15 Supplementary  Handout	Steganography techniques Information Hiding: Techniques for Steganography And Digital Watermarking, Chapter 3 Disappearing cryptography, by Peter Wayner Chapters 9, 13, 14  Transparencies §10
Thursday, March 18 Reading Handouts	Pastry dough mixing: Modern conventional ciphers Stinson §2.7, 3.1, 3.2, 3.5, 3.7 Transparencies §11 Assignment 6, due Monday, March 29
Monday, March 22 – Friday, March 26 Spring Break	
Monday, March 29 Reading Handouts  Due in class	Block ciphers Stinson §3.3 Transparencies §12 Assignment 7, due Thursday, April 8 Assignment 6

Thursday, April 1	Breaking conventional ciphers: Linear and Differential cryptanalysis Stinson §3.4, 3.6 Linear and differential cryptanalysis, Howard Heys
Reading Supplementary No additional handouts Return	Graded assignment 6
Monday, April 5	Document integrity: Hash functions and MACs Stinson, §4.1, 4.2, 1, 4.2.2 Transparencies §14
Reading Handouts	
Thursday, April 8	Iterated hash functions Stinson, §4.2.3, 4.3 Transparencies §15 Assignment 8, due Thursday, April 15 Assignment 7
Reading Handout	
Due in class	
Monday, April 12	Unconditional secure message authentication codes Stinson, §4.4, 4.5 Transparencies §16 Graded assignment 7
Reading Handouts Return	
Thursday, April 15	Big MAC attacks No additional reading or handouts Assignment 8
Reading Due	
Monday, April 19	Patriots' Day, no class Assignment 8 (outside instructor's office)
Return	
Thursday, April 22	Midterm examination 2
Monday, April 26	Introduction to public key cryptography Singh, Chapter 6 Stinson, §5.1, 5.2, 5.3 Transparencies §17 Assignment 9, due Thursday, May 6
Reading  Handouts	
Thursday, April 29	Why can't they get it right: Secure protocols <i>Network Security: Private Communication in a Public World</i> , Kaufman, Perlman, Speciner, Chapter 11 Transparencies §18
Supplementary  Handout	
Monday, May 3	Putting it all together Singh, Chapter 7 <i>Cryptography and Network Security: Principles and Practice</i> , Stallings Chapter 15 Transparencies §20
Reading Supplementary  Handout	
Thursday, May 6	PGP Singh, Chapter 8 No additional handouts Assignment 9
Reading Handouts Due in class	