SM468 SYLLABUS AND CALENDAR

SM468: Cryptography, Codes, and Information Security

Spring 2011

Course Coordinator: Prof. George Nakos
Office: Chauvenet 324 or Nimitz G017
E-mail: gcn@usna.edu
Phone 410-293-6779 or 410-293-2511

Recommended Text: **Introduction to Cryptography with Coding Theory, 2nd edition**
By Wade Trappe and Lawrence C. Washington

Also: Prof. Nakos' notes available to the students of the class

January 2011

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
						1
2	3	4	5	6	7	8
9	10	11 Lesson 1 Shift Cipher, Modular Arithmetic	12 Lesson 2 Modular Arithmetic, inversion	13	14 Lesson 3 ***Quiz 1*** Affine Cipher	15
16	17 M.L. King Holiday	18	19 Lesson 4 Affine Cipher, letter frequencies	20	21 Lesson 5 ***Quiz 2*** Vigenere Cipher	22
23	24 Lesson 6 Kasiski Attack	25	26 Lesson 7 Friedman Attack, Hill Cipher	27	28 Lesson 8 ***Quiz 3***, **Hwk1 due** Hill Cipher	29
30	31 Lesson 9 Affine Hill Cipher Perfect Secrecy					

February 2011

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	**2** Lesson 10 Perfect Secrecy	**3**	**4** Lesson 11 ***Quiz 4*** Perfect Secrecy	**5**
6	**7** Lesson 12 Modern Symmetric Ciphers, Feistel, DES	**8**	**9** Lesson 13 Modern Symmetric Ciphers, DES	**10**	**11** Lesson 14 ***Quiz 5*** Modern Symmetric Ciphers, AES	**12**
13	**14** Lesson 15 Modern Symmetric Ciphers, AES	**15**	**16** Lesson 16 Entropy	**17**	**18** Lesson 17 ***Quiz 6***, **Hwk2 due** Entropy	**19**
20	**21** Washington's Birthday	**22**	**23** Lesson 18 Entropy, Number Theory (GRADES DUE)	**24**	**25** Lesson 19 ***Quiz 7*** RSA	**26**
27	**28** Lesson 20 RSA, **REVIEW 1**					

March 2011

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2 Lesson 21 **REVIEW 2**	3	4 Lesson 22 **TEST 1**	5
6	7 Lesson 23 RSA, Primality Testing	8	9 Lesson 24 Primality Testing	10	11 Lesson 25 **Hwk3 due**, Square Roots, Rabin Cipher	12
13	14 Spring Break	15 Spring Break	16 Spring Break	17 Spring Break	18 Spring Break	19
20	21 Lesson 26 Factorization of integers	22	23 Lesson 27 Factorization of integers	24	25 Lesson 28 ***Quiz 8*** Discrete Logarithms, ElGamal Cipher	26
27	28 Lesson 29 El Gamal Cipher	29	30 Lesson 30 Algorithms for Discrete Logarithms	31		

April 2011

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1 Lesson 31 Finite Fields, Elliptic Curves	**2**
3	**4** Lesson 32 Elliptic Curve Cryptography	**5**	**6** Lesson 33 **Hwk4 due,** Elliptic Curve Cryptography	**7**	**8** Lesson 34 ***Quiz 9*** Knapsack Cipher, Error Correcting Codes	**9**
10	**11** Lesson 35 Error Correcting Codes, **Written Projects due**	**12** (GRADES DUE)	**13** Lesson 36 Error Correcting Codes	**14**	**15** Lesson 37 ***Quiz 10*** Error Correcting Codes	**16**
17	**18** Lesson 38 **Hwk5 due**, Information Security and Digital Signatures	**19**	**20** Lesson 39 **Project Presentations**	**21**	**22** Lesson 40 **Project Presentations**	**23**
24	**25** Lesson 41 **Project Presentations**	**26**	**27** Lesson 42 **REVIEW**	**28**	**29** Lesson 43 **TEST 2**	**30**

May 2011

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2 Lesson 44 **REVIEW**	3 CLASSES END	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				