**Pries: 360 Mathematics of Information Security:** Fall 2019 Homework

| Week | Topics |
|---|---|
| | **Introduction to number theory and cryptography** |
| 1 | Read HPS 1.1: substitution ciphers, frequency analysis,<br>1.2: Euclidean algorithm<br>1.3: arithmetic modulo $m$, 1.4: unique factorization.<br>Problems to review: 1.2(a), 1.4(b), 1.15(c), 1.16(a,c), 1.25(a), 1.28(a) |
| Turn in W 9/4 | 1.9(a), 1.10(a), 1.17(bcde), 1.18, 1.19, 1.21(a), 1.23(a), 1.27 |
| modified: turn in 8 of | Chapter 1: 9(a), 10(a), 17(bcde), 18(bcde), 19, 20, 21, 22(a), 23, 24(a), 27, 29 |
| 2 | Read HPS 1.4: unique factorization,<br>1.5: Fermat's little theorem, order, primitive root (lot of material here)<br>1.6 cryptography, 1.7: affine cipher, random sequences |
| Turn in F 9/13 | Chapter 1: 24(b), 29, 32(a), 34(ad), 36(abc), 38, 43(ac) |
| 3 | Read HPS 2.1 public key cryptography; 2.2 discrete log problem;<br>2.3 Diffie-Hellman key exchange; 2.4 El Gamal public key cryptosystem |
| Turn in F 9/20 | Chapter 2: 2.3, 2.4(a), 2.5, 2.6, 2.7, go over review sheet |
| 4 | |
| 5 | Monday, midterm 1. |
| | **Computation and public key cryptosystems** |
| 6 | Computer lab, writing assignment due |
| 7 | Computer lab, computer lab due |
| 8 | Read: HPS 2.6 (big-O), 2.7 (Baby/Giant),<br>2.8 (Chinese Remainder), 2.9 (Pohlig-Hellman) |
| Turn in M 10/21 | Chapter 2: 2.16 (acd), 2.17(a), 2.19, 2.20, 2.26, 2.28(a) |
| 9 | |
| 10 | |
| | |
| 11 | Monday, midterm 2. |
| 12 | Read HPS 3.5 (Pollard's factorization) and 3.9 (Quadratic reciprocity) |
| Turn in M 11/18 | 3.22(ab), 3.38, 3.39 (a,b(i)), 3.41, 3.42 |
| 13 | |
| | Fall break |
| 14 | Finite fields |
| 15 | Finite fields |