Math 314
Final Exam Study Guide
Wednesday, May 15, 3–5pm

1. Use a shift cipher with a shift of 11 to encode "I love cryptography!". Use all of the conventions from Chapter 2 of the text.
2. The ciphertext `CRWWZ` was encrypted by an affine cipher. The attacker determines that the first two letters of the plaintext are `ha`. Decrypt the message.
3. Prove that if a message in encrypted by an affine cipher, and then encrypted again by a different affine cipher, this is equivalent to encrypting the message by a single, third affine cipher. Determine the properties of the third cipher in terms of the first two.
4. The ciphertext `YIFZMA` was encrypted by a Hill cipher with matrix $\begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix}$. Find the plaintext.
5. Let a, b, and c be integers. Suppose that $a|b$ and $a|c$. Prove that $a|(bs + ct)$ for all integers s and t.
6. State the Prime Number Theorem precisely.
7. Solve $17x \equiv 1 \pmod{101}$. Show all steps. The purpose of this question is to demonstrate your understanding of the algorithm, and you are graded solely on the algorithm.
8. Let a and b be integers, and let p be prime. Suppose that $p|ab$. Prove that $p|a$ or $p|b$.
9. Let a, b, c, and n be integers with $n \neq 0$. Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Prove that $a \equiv c \pmod{n}$.
10. Solve $12x \equiv 21 \pmod{39}$.
11. State and prove the Chinese remainder theorem.
12. Suppose that $x \equiv 3 \pmod{6}$ and $x \equiv 11 \pmod{31}$. Solve for x.
13. State and prove Fermat's Little Theorem.
14. How many integers less than 240 are relatively prime to 240?
15. Evaluate $\phi(120)$.
16. State and prove Euler's theorem.
17. What are the last three digits of 9^{802}?
18. Suppose a, x, y, and $n > 1$ are integers with $\gcd(a, n) = 1$. If $x \equiv y \pmod{\phi(n)}$ then $a^x \equiv a^y \pmod{n}$. Prove this, or provide a counterexample that shows that it is false.
19. Solve $x^2 \equiv 5 \pmod{11}$.
20. Identify all of the primitive roots for $p = 19$.
21. Evaluate the Jacobi symbol $\left(\frac{4}{135}\right)$.
22. Let $a(X) = X^4 + X^3 + 1$ and $b(X) = X^2 + X + 1$ be polynomials in $\mathbf{Z}_2[X]$. Find polynomials $q(X)$ and $r(X)$ with $\deg r < \deg a$ so that $a(X) = q(X)b(X) + r(X)$.

23. Show that $X^{15} \equiv 1 \pmod{X^4 + X + 1}$.

24. For simplified DES, suppose that the message in round i is (L_i, R_i). What is L_{i+1}?

25. For simplified DES, define the expander function. A graph showing how the input bits are matched to the output bits is sufficient.

26. Consider the following S-Box.

$$S = \begin{bmatrix} 101 & 010 & 001 & 110 & 011 & 100 & 111 & 000 \\ 001 & 100 & 110 & 010 & 000 & 111 & 101 & 011 \end{bmatrix}$$

How does it work? Provide an example.

27. For simplified DES, suppose the key is 192. What is the key for the first round of encryption?

28. What are the disadvantages of Electronic Codebook?

29. Describe the algorithm for cipher feedback mode.

30. Describe the algorithm for counter mode.

31. What is the difference between a block cipher and a stream cipher? Provide an example of each.

32. Provide a high-level overview of how AES works.

33. For RSA, the following quantities are used: n, p, q, e, and d. What is the meaning of each? Indicate which are secret, and which are public.

34. For RSA, suppose $p = 3$, $q = 11$, $e = 3$ and $m = 5$. What is the ciphertext?

35. For RSA, the following quantities are used: n, p, q, e, and d. Suppose that the message is m and $\gcd(m, n) = 1$. Prove that $m^{ed} \equiv m \pmod{n}$.

36. Suppose that $n = pq$ is a product of primes, and suppose that n and $\phi(n)$ (only) are known. Prove that n can be factored, and show how to do it.

37. For RSA, suppose that Alice uses $e = 1$. How can the system be attacked? Suppose that Bob uses $e = 2$. How can the system be attacked?

38. For RSA, Bob chooses n and two encryption exponents, e_1 and e_2. He asks Alice to encrypt her message m by first calculating the ciphertext c_1 using RSA with the exponent e_1 and then encrypting that with exponent e_2 to get the final ciphertext c_2 which is sent to Bob. Does this double encryption improve security? Why or why not?

39. State and prove the Basic Principle for primality testing.

40. State precisely the Miller–Rabin primality test.

41. Determine $L_{13}(18)$ for $p = 19$.

42. Let p be prime, and α a primitive root mod p. Prove that $\alpha^{(p-1)/2} \equiv -1 \pmod{p}$.

43. It can be shown that 5 is a primitive root for the prime 1223. You want to solve the discrete logarithm problem $5^x \equiv 3 \pmod{1223}$. You know $3^{611} \equiv 1 \pmod{1223}$. Is x even or odd? Prove it.

44. State precisely all of the steps in Diffie–Hellman key exchange.

45. Alice and Bob use Diffie-Hellman to agree on a key. They use the prime 19, with $\alpha = 14$. Alice chooses the secret $x = 4$ and Bob chooses the secret $y = 11$. What key do they use?

46. State precisely all of the steps in an ElGamal public key cryptosystem.

47. Alice and Bob use the ElGamal public key cryptosystem with $p = 19$, and $\alpha = 3$. Bob chooses the secret $x = 4$. What is β? Alice sends the ciphertext $(2, 3)$. What is the message?

48. The points $(3, \pm 5)$ lie on the elliptic curve $y^2 = x^3 + 2$. Find another point with rational coordinates on this curve.

49. For the elliptic curve $y^2 = x^3 - 2 \pmod 7$, calculate $(3, 2) + (5, 5)$.

50. Let $P = (x, 0)$ be a point on an elliptic curve. Find $P + P$.

51. Explain how the elliptic curve version of the Diffie–Hellman key exchange works.

0	1	2	3	4	5	6	7	8	9	10	11	12
a	b	c	d	e	f	g	h	i	j	k	l	m
13	14	15	16	17	18	19	20	21	22	23	24	25
n	o	p	q	r	s	t	u	v	w	x	y	z

Multiplication mod 26

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Addition mod 19

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
18	18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Multiplication mod 19

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	0	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	0	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	0	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	0	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	0	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	0	7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	5	12
8	0	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11
9	0	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	0	10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9
11	0	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8
12	0	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
13	0	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	0	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	0	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	0	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	0	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	0	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Exponentiation mod 19

^	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1