Introduction to cryptography with coding theory 3rd edition pdf

1 SOLUTIONS MANUAL for INTRODUCTION TO CRYPTOGRAPHY with Coding Theory, 2nd edition Wade Trappe Wireless Information Network Laboratory and the Electrical and Computer Engineering Department Rutgers University Lawrence C. Washington Department of Mathematics University of Maryland August 26, 2005 2 Contents Exercises Chapter 2 - Exercises 1 Chapter 3 - Exercises 6 Chapter 4 - Exercises 14 Chapter 5 - Exercises 17 Chapter 6 - Exercises 19 Chapter 7 - Exercises 23 Chapter 8 - Exercises 25 Chapter 9 - Exercises 27 Chapter 10 - Exercises 28 Chapter 11 - Exercises 29 Chapter 12 - Exercises 31 Chapter 13 - Exercises 33 Chapter 14 - Exercises 34 Chapter 15 - Exercises 36 Chapter 16 - Exercises 40 Chapter 17 - Exercises 44 Chapter 18 - Exercises 46-2 3 -1 Chapter 19 - Exercises 51 Mathematica problems Chapter 2 52 Chapter 3 63 Chapter 6 66 Chapter 7 72 Chapter 8 74 Chapter 9 75 Chapter Chapter Chapter Maple problems Chapter 2 84 Chapter 3 98 Chapter Chapter Chapter Chapter Chapter Chapter 4 0 MATLAB problems Chapter Chapter Chapter Chapter Chapter Chapter Chapter Chapter Chapter 5 Chapter 2 - Exercises 1. Among the shifts of EVIRE, there are two words: arena and river. Therefore, Anthony cannot determine where to meet Caesar. 2. The inverse of 9 mod 26 is 3. Therefore, the decryption function is x = 3(y 2) = 3y 2 (mod 26). Now simply decrypt letter by letter as follows. U = 20 so decrypt U by calculating (mod 26) = 2, and so on. The decrypted message is cat. 3. Changing the plaintext to numbers yields 7, 14, 22, 0, 17, 4, 24, 14, 20. Applying 5x+7 to each yields = (mod 26), = 77 25, etc. Changing back to letters yields QZNHOBXZD as the ciphertext. 4. Let mx + n be the encryption function. Since h = 7 and N = 13, we have m 7 + n 13 (mod 26). Using the second letters yields m 0 + n 14. Therefore n = 14. The first congruence now yields 7m 1 (mod 26). This yields m = 11. The encryption function is therefore 11x Let the decryption function be x = ay + b. The first letters tell us that 7 a 2 + b (mod 26). The second letters tell us that 0 a 17 + b.subtracting yields 7 a (15) 11a. Since (mod 26), we have a (mod 26). The first congruence now tells us that b, so b = 1. The decryption function is therefore x 3y + 1. Applying this to CRWWZ yields happy for the plaintext. 6. Let mx+n be one affine function and ax+b be another. Applying the first then the second yields the function a(mx + n) + b = (am)x + (an + b), which is an affine function. Therefore, successively encrypting with two affine functions is the same as encrypting with a single affine function. There is therefore no advantage of doing double encryption in this case. (Technical point: Since gcd(a,26) = 1 and gcd(m,26) = 1, it follows that gcd(am,26) = 1, so the affine function we obtained is still of the required form.) 7. For an affine cipher mx + n (mod 27), we must have gcd(27,m) = 1, and we can always take 1 m 27. So we must exclude all multiples of 3, which leaves 18 possibilities for m. All 27 values of n are possible, so we have = 486 keys. When we work mod 29, all values 1 m 28 are allowed, so we have = 812 keys. 8. (a) In order for α to be valid and lead to a decryption algorithm, we need gcd(α, 30) = 1. The possible values for α are 1, 7, 11, 13, 17, 19, 23, 29. (b) We need to find two x such that 10x (mod 30) gives the same value. There are many such possible answers, for example x = 1 and x = 4 will work. 1 6 2 This corresponds to the letters b and e. 9. If x 1 = x 2 +(26/d), then αx 1 +β = αx 2 +β+(α/d)26. Since d = gcd(α,26) divides α, the number α/26 is an integer. Therefore (α/d)26 is a multiple of 26, which means that αx 1 + β αx 2 + β (mod 26). Therefore x 1 and x 2 encrypt to the same ciphertext, so unique decryption is impossible. 10. (a) In order to find the most probable key length, we write the ciphertext down on two strips and shift the second strip by varying amounts. The shift with the most matches is the most likely key length. As an example, look at the shift by 1: B A B A B A A A B A B A B A B A A A B A * * This has a total of 2 matches. A shift by 2 has 6 matches, while a shift by 3 has 2 matches. Thus, the most likely key length is 2. (b) To decrypt, we use the fact that the key length is 2 and extract off every odd letter to get BBBAB, and then every even letter to get AAAAA. Using a frequency count on each of these yields that a shift of 0 is the most likely scenario for the first character of the Vigenere key, while a shift of 1 is the most likely case for the second character of the key. Thus, the key is AB. Decrypting each subsequence yields BBBAB and BBBBB. Combining them gives the original plaintext BBBBBBABBB. 11. If we look at shifts of 1, 2, and 3 we have 2, 3, and 1 matches. This certainly rules out 3 as the key length, but the key length may be 1 or 2. In the ciphertext, there are 3 A s, 5 B s, and 2 C s. If the key length were 1, this should approximate the frequencies.7,.2,.1 of the plaintext in some order, which is not the case. So we rule out 1 as the key length. Let s consider a key length of 2. The first, third, fifth,... letters are ACABA. There are 3 A s, 1 B, and 1C. These frequencies of.6,.2,.2 is a close match to.7,.2,.1 shifted by 0 positions. The first element of the key is probably A. The second, fourth,... letters of the ciphertext are BBBBC. There are 0 A s, 4 B s, and 1 C. These frequencies.0,.8,.2 and match.7,.2,.1 with a shift by 1. Therefore the second key element is probably B. Since the results for length 2 match the frequencies most closely, we conclude that the key is probably AB. 12. Since the entries of A i are the same as those in A 0 (shifted a few places) the two vectors have the same length. Therefore A 0 A i = A 0 A i cos θ = A 0 2 cos θ. Note that cos θ 1, and equals 1 exactly when θ = 0. But θ = 0 exactly when the two vectors are equal. So we see that the largest value of the cosine is when A 0 = A i. Therefore the largest value of the dot product is when i = Change YIFZMA(to pairs of numbers:) ((24, 8),)(5, 25), (12, 0). Invert the matrix to get N = (mod 26). Calculate (24,8)N = (4,20), (5,25)N = (17,4), (12,0)N = (10,0). Change back to letters: eureka. 7 ( ) a b 14. Suppose the encryption matrix M is. Change the ciphertext c d to numbers: (6, 4), (25, 23), (3, 18). Change the plaintext to numbers: (18, 14), (11, 21), (4,3). We know (18,14)M (6,4), etc. We ll use (11,21)M (25,23) and (4,3)M (3,18) to get equations for a,b,c,d, which are most ( )( ) a b easily put in matrix form: ( ) (4 3 c d of mod 26 is ( ) ( ) a b 12 3 M =. c d Suppose the matrix has the form ( ). The inverse). Multiply by this matrix to obtain (α β M = γ δ) Then the encryption of a plaintext x = (b,a) = (1,0) yields (α,β). We know this corresponds to HC, and hence α = 7 and β = 2. The second piece of information is that zz encrypts to GT. This corresponds to a plaintext of (25,25) or equivalently (1, 1). Using this yields α γ = 6 and β δ = 19. Thus, γ = 13 and δ = (a) (The plaintext) is ((3,14), (13,) 19). The ciphertext (is (4,11),) (13, 8) We have M. The inverse of mod 26 (13) ( ) is. Multiplying by this inverse yields M (3 14 (b) We have ( ) find M) (4 11 M). Proceeding as in part (a), we 17. Suppose the plaintext is of the form (x,y), then the ciphertext is of the form (x + 3y,2x + 4y) (mod 26). There will be many possible plaintexts that will map to the same ciphertext. We will try to make plaintexts that yield a ciphertext of the form (0,). To do so, we will have the relationship x = 3y (mod 26). Now we need to find two y values that produce the same 2(3y) + 4y = 2y (mod 26). If we take y = 4 and y = 17 then we get the same value for 2y (mod 26). Thus, (14,4) and (1,17) are two plaintexts that map to (0,18). 18. We will need to use three different plaintexts. First, choose (x,y) = (0,0). This will produce a ciphertext that is precisely (e,f). Next, try (x,y) = (1,0). This will produce a ciphertext that is (a,b) + (e,f). We may subtract off (e,f) to find (a,b). Finally, use (x,y) = (0,1) to get (c,d) + (e,f) as the ciphertext. We may subtract off (e,f) to get (c,d). 8 4 19. As is Section 2.11, set up the matrix equation c c c 2 0 This yields c 0 = 1,c 1 = 0,c 2 = 1, so the recurrence is k n+3 k n + k n+2. The next four terms of the sequence are 1, 0, 0, 1. ( )( ) 1 0 c0 20. The sequence is 1,0,1,0,1,0,1,.... The matrix equation is 0 1 c ( ) 1 1. This yields c 0 0 = 1,c 1 = 0, so k n+2 k n. 21. Set up the matrix equation ( ) ( ) ( ) xn x n+1 c0 xn+2 =. x n+1 x n+2 c 1 x n+3 Using the values provided, we obtain ( )(c0 c 1) = (0 2). The inverse of the matrix can be found to be ( ) (=) (mod 3) Multiplying both sides of by the inverse matrix, yields c 0 = 2 and c 1 = Use x 1, x 2 and x 3 to solve for c 1 by obtaining c (mod 5). Thus, c 1 = 4. Next, use x 2, x 3 and x 4 to solve for c 0. We get c 0 +c 1 +2 (mod 5) 0, and hence c 0 = The number of seconds in 120 years is Therefore you need to count /( ) numbers per second! 24. (a) The ciphertext will consist of one letter repeated. However, there is no way of deducing what the key is. (b) The ciphertext will consist of one letter repeated. However, there is no way of deducing what the key is. (c) The ciphertext will consist of a continuous stream of the letter A. This is easy to detect. However, there will be no way to tell what the key is. 25. (a) The ciphertext will correspond to a shifted version of the key word that is repeated many times. The periodic nature of the resulting ciphertext will cause Eve to suspect the plaintext is a single letter, while the period of the repeating ciphertext will correspond to the key length. (b) Using the fact that no English word of length six is the shift of another English word, simply treat the Vigenere key as if it were the plaintext and the 9 single character plaintext as if it were the shift in a shift cipher. Decrypting can be done by trying all possible shifts of the first six characters of the ciphertext. One of these shifts will be a word that corresponds to the Vigenere key. (c) If we use the method of displacement, then shifting by six will have the highest number of matches. In fact, every place will match up. This will be easy to detect. However, shifting the ciphertext by one place will just yield the amount of matches that occur when the repeated key is shifted by one place. In particular, the key word will most likely not have that many matches with itself when shifted over one place. Similarly for shifts of two, three, four, and five. As a result, other shifts will have a much smaller amount of matches. 5 10 Chapter 3 - Exercises 1. (a) Apply the Euclidean algorithm to 17 and 101: 101 = = Working back yields 1 = = 17 ( ) = (1) (b) Since = 1, we have (mod 101). Therefore (mod 101). 2. (a) Apply the Euclidean algorithm to 7 and 30: 30 = = Working backwards yields 1 = = 7 3 (30 4 7) = (3) 30. Therefore (mod 30), so d = 13. (b) Let c m 7 (mod 31) be the ciphertext. Claim: c 13 m (mod 31). Proof: c 1 3 (m 7) 13 m 91 (m 30) 3 m. If m 0 (mod 31) then m 30 1 (mod 31) by Fermat. Then c m m. If m 0 (mod 31), then c m 7 0, so c m. Therefore c 13 m for all m. Therefore decryption is performed by raising the ciphertext to the 13th power mod (a) gcd(12,236) = 4, so divide both sides by 4 to obtain 3x 7 (mod 59). The inverse of 3 mod 59 is 20, so multiply both sides by 20 to obtain x (mod 59). This yields x 22,81,140,199 (mod 236). (b) 30 is not divisible by 4 = gcd(12,236), so there are no solutions. 4. (a) = = = = = = = = 11 7 Therefore, gcd(30030, 257) = 1. (b) If 257 is composite, it is divisible by a prime p 257 = The primes satisfying this are exactly the prime factors of Since the gcd is 1, none of them divide 257, so 257 is prime. 5. (a) 4883 = = = Therefore, the gcd is 257. (b) We know that both numbers have 257 as a factor. This yields 4883 = and 4369 = (a) The first two steps of the Euclidean algorithm are It continues in this way until Therefore, the gcd is 1. (b) F n = 1 F n 1 + F n 2 F n 1 = 1 F n 2 + F n 3. 2 = = = = = = Therefore, the gcd is 1. (c) The first step of the Euclidean algorithm is a = 10 Fn 2 b + c, where c consists of F n 2 repeated 1 s. Continuing in this way, in each step we divide F j 1 repeated 1 s into F j repeated 1 s and get a remainder consisting of F j 2 repeated 1 s. Eventually, we get down to the computations of part (b), and then obtain that the gcd is (a) If ab 0 (mod p), then p ab. By the Corollary on page 64, since p is prime, either p a or p b. Therefore, either a 0 (mod p) or b 0 (mod p). (b) We follow the proof of the Corollary on page 64. Since gcd(a,n) = 1, there are integers x,y such that ax+ny = 1. Multiply by b to obtain abx+bny = b. Since n ab, both terms on the left are multiples of n. Therefore n b. 8. (x+1)(x 1) 0 (mod p) implies, by 3(a), that either x+1 0 (mod p) or x 1 0 (mod p). Therefore x ±1 (mod p). 12 8 9. One solution is to look at the numbers congruent to 3 (mod 10) until we find one that is 2 (mod 7): 3, 13 6, 23 2 (mod 7). Therefore x 23 (mod 70). 10. Suppose there are x people. Then x 1 (mod 3),x 2 (mod 4),x 3 (mod 5). The last two congruences combine to x 18 (mod 20). List the numbers that are 18 (mod 20) until you find one that is 1 (mod 3). The answer is x 58 (mod 60). 11. If a 0 (mod p), then Fermat says that a p 1 1 (mod p). Multiply by a to get a p a (mod p). If a 0 (mod p), then a p 0 p 0 a (mod). Therefore a p a (mod p) for all a. 12. By Fermat s theorem, (mod 101). Therefore, (2 100) Therefore, the remainder is Last two digits means we work mod 100. Since φ(100) = 40, Euler s theorem says that (mod 100). Therefore, ( ) The last two digits are (a) 7 7 (1) (mod 4). (b) 7 7 = 3 + 4k for some k. By Euler s theorem, (mod 10). Therefore, 7 77 = 7 3 (7 4) k k (mod 10). The last digit is (a) φ(1) = 1,φ(2) = 1,φ(5) = 4,φ(10) = 4. The sum is 10. (b) φ(1) = 1,φ(2) = 1,φ(3)2,φ(4) = 2,φ(6) = 2,φ(12) = 4. The sum is 12. (c) The sum of φ(d), for all of the divisors d of n, equals n. 16. (a) Since p a, Fermat says that a p 1 1 (mod p). For p = 7, we have a 6 1 (mod 7), so a (a 6) (mod 7). Since 1728 = and 1728 = 18 96, a similar argument works for p = 13 and for p = 19. (b) If p a, then multiply the result of (a) by a to get a 1729 a (mod p). If p a, then a 1729 and a are both 0 (mod p), so a 1729 a in this case, too. (c) Fix a number a. The Chinese Remainder Theorem says that x a 1729 (mod 7),x a (mod 13),x a 1729 (mod 19) has a unique solution x (mod 1729), since 1729 = We know two such solutions: x = a (from part (b) and x = a (trivially). Since x is unique mod 1729, we must have a a 1729 (mod 1729). 17. (a) The powers of 2 mod 11 are 2,4,8,5,10,9,7,3,6,1. This gives all nonzero congruence classes mod 11, so 2 is a primitive root mod 11. (b) The inverse of 3 (mod 10) is 7. We obtain 8 7 (2 3) ((mod 11). Therefore, x = 7. (c) This can be done directly, but here is another way. If c 0 (mod 11), then c 2 j for some j. Therefore, c (8 7) j 8 7j (mod 11), so c is a power of 8. (d) Write xy = 1 + (p 1)k. Then h x (g y) x g (g p 1) k g 1 k g (mod p). 13 9 (e) Let c be nonzero mod p. Then c g j (mod p) for some j, so c (h x) j h xj (mod p). Since every nonzero congruence class is a power of h, we have that h is a primitive root mod p. 18. (a) The determinant is = 5 21 (mod 26). The inverse of the determinant is 5 (mod 26). The inverse of the matrix is therefore 1 21 ( ) 5 ( ) ((b) The determinant is 1 b. The matrix is invertible mod 26 exactly when gcd(1 b,26) = 1. This happens when 1 b is odd and not 0 mod 13, so b 0,2,4,6,8,10,12,16,18,20,22,24 (mod 26). 19. The determinant is 9 35 = 26. This is divisible by 2 and by 13, so these are the two primes for which the matrix is not invertible mod p. 20. (a) We know a φ(n) 1 (mod n), by Euler. Since r is smallest, r φ(n). (b) Since a r 1, we have a m (a r) k 1 k 1 (mod n). (c) By (b), a qr 1. Therefore, 1 (by assumption)a t a qr a s 1 a s a s. (d) Since a s 1 and r is the smallest positive integer with a r 1, we must have s = 0. Therefore t = qr, so r t. (e) By Euler, a φ(n) 1 (mod n). From part (d) with t = φ(n), we obtain ord n (a) φ(n). 21. (a) If r divides 600, then r = 2 a 3 b 5 c with a 3,b 1,c 2. If r < 600, then we cannot have a = 3,b = 1,c = 2. If a 2, then r = 300. If b = 0 then r = 200. If c 1 then r = 120. (b) From 9(e), we know that ord 601 (7) 600. If ord 601 (7) < 600, then it divides 300, 200, or 120, by (a). (c) Suppose ord 601 (7) 300. By 9(b), we must have (mod 601), which is not the case. Therefore, ord 601 (7) 300. Similarly, ord 601 (7) 200 and ord 601 (7) 120. (d) From (b) and (c), we cannot have ord 601 (7) < 600. Since ord 601 (7) 600 from 9(a), we must have ord 601 (7) = 600. Therefore the numbers 7 j (mod 601), for j = 0,1,...,599 are distinct, so there are 600 of them. This implies that 7 is a primitive root mod 601. (e) Calculate g (p 1)/qi (mod p) for i = 1,2,...,s. If each of these is 1 (mod p), then g is a primitive root mod p. (Of course, perhaps we should check first that p g.) 22. (a) We have 3 16k 2 k 1 (mod 65537) and 3 32k (mod 65537). Therefore k and k. Write 32k = 65536l for some l. Divide by 32 to obtain k = 2048l, so 2 11 = 2048 k. If 2 12 = 4096 k, then 16k is a multiple of = 65536, which we showed doesn t happen. Therefore k is a multiple of 2048, but is not a multiple of (b) From (a), we see that k is an odd multiple of We also know that 0 k < 65536, since every nonzero number mod can be written as a power of 3 with exponent in this range. There are 65536/2048=32 multiples of 2048 in this range. Of these, 16 are multiples of The remaining 16 are possibilities for k. We now calculate m (mod 65537) for m = 1,3,5,. We find (with the help of a computer) that m = 27 works. So k = =). 14 (a) We claim that after the kth step 2, we have r k y b1b2 b k (mod n). This is easily seen to be the case for k = 1. Assume it is true for k 1. We ll show it s true for k. We have s k rk 1 2 y2 b1b2 b k 1. Then r k s k y b k rk 2yb k y 2 b1...b k 1+b k y b1 b k 1b k. Therefore, when k = w we have r w y x, as desired. (b) Write x = b 1...b w in binary as in (a). We assume b 1 = 1. The algorithm is easily seen to work when x = 0, so we may assume w 1. We claim that after step 2, a = b 1...b w k, b y b w k+1...b w and c y 2k for some value of k. When we start, we have k = 0. Suppose we arrive at step 2 with a = b 1...b w k, b y b w k+1...b w, and c y 2k. If a is odd, then the output of step 2 is the same as the input, hence of the desired form. If a is even, then b w k = 0. We obtain the new a = b 1...b w k 1, b y b w kb w k+1...b w (we may include the extra bit at the beginning since it is 0), and c y 2k+1. Therefore the output has a,b,c in the desired form with k + 1 in place of k. Now let s look at what happens in step 3. The output of step 2 is of the form a = b 1...b w j, b y bw j+1...bw and c y 2j for some value of j. If a is even, step 3 does nothing, so the output still has the desired form. If a is odd, then the last bit b w j of a is 1. The new a is a = b 1...b w j 1 0. Also, the new b is y bw jbw j+1...bw y 2j y 1bw jbw j+1...bw y bw jbw j+1...bw. The new c is still y 2j. If the new a = 0, then j = w 1, so b y x. Therefore step 5 outputs y x, as desired. Otherwise, step 4 sends us to step 2, which outputs a = b 1...b w j 1, b y bw jbw j+1...bw, and c y 2j+1. This is of the desired form with k = j + 1. Therefore, the output of step 2 always has the desired form, as claimed. Since a gets smaller at each application of steps 2 and 3, eventually a = 0 and the algorithm stops. As pointed out above, the output of step 5 is then y x (mod n). 24. Since z j 0 (mod m i) when j i, we have x a i y i z i a i z 1 i z i a i (mod m i). 25. (a) Solve x (mod 11) to obtain x ±1 (mod 11). Now solve x (mod 13) to obtain x ±4 (mod 13). There are four ways to combine these via the Chinese Remainder Theorem: x 43, 56, 87, 100 (mod 143). (b) This reduces to x 2 77 (mod 11) and x 2 77 (mod 13). The solutions satisfy x 0 (mod 11) and x ±5 (mod 13). These combine to yield x 44, 99 (mod 143). 26. Suppose x 2 1 (mod p). Raise both sides to the (p 1)/2 power to obtain x p 1 (1) (p 1)/2 (mod p). By Fermat, x p 1 1. Since p 3]pmod4, the exponent (p 1)/2 is odd. Therefore (1) (p 1)/2 = 1. This yields 1 1 (mod p), which is a contradiction. Therefore x cannot exist. 27. (a) There are at most 4 square roots of x (mod n). Therefore, several random selections of these square roots should include the meaningful message m. (b) Being able to find square roots mod n is computationally equivalent to factoring n, which is presumed to be hard. 15 11 (c) Eve chooses a random number m and computes x m 2 (mod n). She gives x to the machine, which outputs a square root m of x. If gcd(m,n) = 1, there are four possible m, namely m, m, and two others. After a few tries, Eve should obtain m with m ±m (mod n). Since m 2 x m 2 (mod n), a nontrivial factor of n is given by gcd(m m,n). 28. (a) Since r 1 = a bq 1 and d a,b, we have d r 1. Since r 2 = b q 2 r 1 and d b,r 1, we have d r 2. (b) Suppose d r 1,...,r j. Since r j+1 = r j 1 q j+1 r j and d rj 1,r j, we have d r j+1. By induction, we have d r i for all i. (c) Since r k 1 = q k+1 r k, we have r k r k 1. Assume r k r k i for i = 1,2,...,j. Since r k j 1 = q k j+1 r k j + r k j+1 and d r k r k j,r k j+1 by assumption, we have r k r k j 1. By induction, r k r i for all i. (d) Since b = q 2 r 1 + r 2 and r k r 1,r 2, we have r k b. Since a = q 1 b + r 1 and r k a,r 1, we have r a. (e) Since d r k for each common divisor d, we have r k d for all common divisors d. Since r k is a common divisor, it is the largest. 29. (a) ( ) 123 = 401 Therefore, there is no solution. (b) ( ) 43 = 179 Therefore, there is a solution. (c) ( ) 1093 = ( ) ( ) ( ) = = = ( ) ( ) = = ( ) ( ) 43 1 = = ( ) ( )( ) ( ) ( ) = = = = Therefore, there is no solution. 30. (a) If a b 2 (mod n), then (a = n) ( ) 2 b = (±1) 2 = 1. n Therefore, if (a n) = 1, then a cannot be a square mod n. (b)) (3 35 = ( ) 35 = 3 ( ) 2 = 1. 3 (c) Since 3 is not a square mod 5, it cannot be a square mod (2 15) = 1, but (mod 15). 32. (a) ( ) ( ) ( ) = = 16 12 (b) Since is prime, 3 ( )/2 ( ) = 1 (mod 65537). (c) The order of 3 mod divides = 2 16, hence is a power of 2. If the order is not 2 16, then it divides 2 15 = 32768, so (mod 65537). But part (b) says that this is not the case. Therefore, the order of 3 must be 2 16, and 3 is a primitive root mod (a) The only polynomials of degree 1 are X and X + 1, and they are irreducible. The only polynomials of degree 2 are X 2,X 2 +1,X 2 +X,X 2 +X+1. But X 2 and X (X + 1) 2 are reducible, and so is X 2 + X X(X + 1). Only X 2 + X + 1 remains. If it factors, it must be divisible by a degree one polynomial. Clearly X does not divide it. A simple calculation shows that X +1 does not divide it either. Therefore X 2 + X + 1 is irreducible. (b) If X 4 +X +1 factors, it must have an irreducible factor of degree at most 2. Since none of the polynomials from part (a) divide it, it must be irreducible. (c) X 4 (X + 1) X + 1, since we are working with coefficients mod 2. Square both sides to obtain X 8 (X + 1) 2 X Square again to obtain X 16 (X 2 + 1) 2 X (X + 1) + 1 X. (d) Since X 4 + X + 1 is irreducible, polynomials mod X 4 + X + 1 form a field. Since X 0 (mod X 4 +X +1), it has a multiplicative inverse. Therefore, we can divide X 16 X by X to obtain X (a) If X is reducible, it must factor as a product of two degree one polynomials. But none of the polynomials X, X +1, X +2 divides X 2 +1 mod 3. Therefore it is irreducible. (b) Apply the Euclidean algorithm to 2X + 1 and X 2 + 1: X = (2X)(2X + 1) + (X + 1) 2X + 1 = (2)(X + 1) + 2 X + 1 = (2X + 2)(2) + 0. Working backwards, we obtain 2 = (2X+1) 2(X+1) = (2X+1) 2((X 2 +1) (2X)(2X+1)) = (2)(X 2 +1)+(X+1)(2X+1). Therefore, (X+1)(2X+1) 2 (mod X 2 + 1). Multiply by 2 to obtain (2X + 2)(2X + 1) 1 (mod X 2 + 1). Therefore, 2X + 2 is the multiplicative inverse of 1 + 2X. 35. a = q 1 b + r 1 with 0 r 1 < b. This means that a b = q 1 + r 1 b with 0 r 1 /b < 1. Therefore, a 0 = q 1. Similarly, at each step of the algorithm, in the notation of page 67, we have r j 2 r j 1 = q j + r j r j 1, which yields a j 1 = q j. 36. (a) The values of a 0,a 1,a 2,... for 3 are 1,1,2,1,2,1,2,. For 7, they are 2,1,1,1,4,1,1,1,4,. The first keeps repeating 1,2. The second keeps repeating 1, 1, 1, 4. 17 13 (b) For d = 3: n = 1, and p 1 /q 1 = 1 + 1/1 = 2/1. We have = 1. For d = 7: n = 3, and p 3 1 = 2 + q = We have = 1. (c) The continued fraction for 19 starts with a 0,a 1,a 2,a 3,a 4,a 5,a 6 equal to 4,2,1,3,1,2,8. We have n = 5. A calculation yields p 5 = 170 and q 5 = 39. We have = 1. (Note: this method sometimes yields x 2 dy 2 = 1. In this case x 1 = x 2 + dy 2 and y 1 = 2xy satisfy x 2 1 dy 2 1 = +1.) 37. Use a decimal approximation for e to obtain a 0,a 1,a 2,a 3, = 2,1,2,1,1,4,1,1,6,1,1,8,1,1,10,1,1,12,1,1,14,.... After the initial 2, we get blocks of 1,2n,1 for n = 1,2,3, The continued fraction has a 0,a 1,a 2, equal to 1,1,1,. We have p n = F n+2 and q n = F n+1, where F n is the nth Fibonacci number (see Exercise 6). 39. (a) The multiples of p are p,2p,3p,,(q 1)p. There are q 1 of them. Similarly for the multiples of q. (b) The only factors of pq are 1,p,q,pq. If gcd(m,pq) > 1, then the gcd must be p, q, or pq. Therefore, m is a multiple of p, q, or pq, hence a multiple of p or of q (possibly both). (c) If m is a multiple of both p and q, then it is a multiple of pq, hence m pq. If 1 m < pq, this is impossible. (d) We have pq numbers m with 1 m pq. Remove m = pq, which is the only number satisfying gcd(m.pq) = pq. Remove the q 1 multiples of p and the p 1 multiples of q. By part (c), these two sets of numbers do not overlap. We have therefore removed 1 + (q 1) + (p 1) numbers. There are pq 1 (q 1) (p 1) = (p 1)(q 1) numbers remaining. These are exactly the m with gcd(m,pq) = (a) x 1 (mod 4), x 2 (mod 6) has no solution. (b) x 2 (mod 4), x 4 (mod 6) has the solution x = 10 (in fact, x 10 (mod 12) gives all solutions). 18 Chapter 4 - Exercises 1. (a) Switch left and right halves and use the same procedure as encryption. The switch the left and right of the final output. Verification is the same as that on pages (b, c) 1st round: M 0 M 1 M 1 [M 0 K M 1] 2nd round: [M 0 K M 1][M 1 M 0 K M 1 K] = [M 0 K M 1][M 0] 3rd round: [M 0][M 0 K M 1 K M 0] = [M 0][M 1], which is the plaintext. Therefore 3 rounds is very insecure! After 2 rounds, the ciphertext alone lets you determine M 0 and therefore M 1 K, but not M 1 or K individually. If you also know the plaintext, you know M 1 are therefore can deduce K. 2. If someone discovers the fixed key and obtains the encrypted password file, this person can easily decrypt by the usual decryption procedure. However, knowing the ciphertext and the plaintext does not readily allow one to deduce the key. 3. CBC: We have D K (C j) C j 1 = D K (E K (P j C j 1)) C j 1 = P j C j 1 C j 1 = P j. CFB: C j L 8 (E K (X j)) = (P j L 8 (E K (X j))) L 8 (E K (X j)) = P j. 4. Let I denote the string of all 1 s. Note that the expansion E(R i 1) = E(R i 1) = E(R i 1) I. Therefore E(R i 1) K i = E(R i 1) I K i I = E(R i 1) K i, so the input to the S-boxes doesn t change. Therefore the output doesn t change. But L i 1 = L i 1 I, so the resulting right side is L i 1 f(r i 1,K i) = R i I = R i. Also, clearly the new left side is the complementary string. So each round of DES gives the complementary string, so this is true for the final result. 5. (a) The keys K 1,...,K 16 are all the same (all 1 s). Decryption is accomplished by reversing the order of the keys to K 16,...,K 1. Since the K i are all the same, this is the same as encryption, so encrypting twice gives back the plaintext. (b) The key of all 0 s, by the same reasoning. 6. Let (m,c) be a plaintext-ciphertext pair. Make one list of E K (E K (m)), where K runs through all possible keys. Make another list of D K (c), where K runs through all possible keys. A match between the two lists is a pair K,K of keys with E K (E K (E K (m))) = c. There should be a small number of such pairs. For each such pair, try it on another plaintext and see if it produces the corresponding ciphertext. This should eliminate most of the incorrect pairs. 14 19 15 Repeating a few more times should yield the pair K 1,K (a) To perform the meet in the middle attack, you need a plaintext m and ciphertext c pair (its a known plaintext attack). So, make two lists. The left list consists of encryptions using the second encryption E 2 with different choices for K 2. Similarly, the right side contains decryptions using different keys for the first encryption algorithm. Thus, the lists look like: E1(m) 2 = y 1 E2(m) 2 = y 2. E788(m) 2 = y 788. z 1 = D1(c) 1 z 2 = D2(c) 1. z 788 = D788(c) 1. Note: The two lists need not be the same size, as the different algorithms might have different key lengths, and hence different amount of keys (see part b). Now, look for matches between y j and z l. A match using K 2 for E 2 and K 1 for D 1 indicates E 2 K 2 (m) = y = D1 K 1 (c) and hence E 1 K 1) (EK 2 (m) = c. 2 (b) Observe that there are 26 possibilities for β and 12 possibilities for α. Let Eα(x) 2 = αx (mod 26) and let Eβ 1 (x) = x + β (mod 26). The composition of these two gives the affine cipher. The total computation needed involves producing 26 encryptions for E 2 and 12 decryptions for E 1. The total is It suffices to look at an arbitrary round of the encryption process. Suppose we look at the ith round, which involves L i = R i 1, M i = L i 1 and R i = f(k i,r i 1) M i 1. To undo this round, that is to go from {L i,m i,r i } to {L i 1,M i 1,R i 1 } we do the following: L i 1 = M i M i 1 = f(k i,r i 1) R i = f(k i,l i) R i R i 1 = L i. This is of the form of the decryption algorithm specified in the problem. 9. (a) At the decryption side, the decryptor has {C 1,C 2, } and the initial X 1. To decrypt, the decryptor starts with j = 1 and calculates P j = C j L 32 (E K (X j)) X j+1 = R 32 (X j) C j. (b) To solve this problem, it is easiest to step through registers step by step. We start with X 1 and a sequence of ciphtertext C 1,C 2,C 3,. To decrypt the first block, we calculate: P 1 = C 1 L 32 (E K (X 1)) 20 16 X 2 = R 32 (X 1) C 1. Observe that the decrypted plaintext P 1 is corrupted because it has the corrupted C 1 as part of it, and also that X 2 X 2 since it has the corrupted C 1 as part of it. The next couple steps of decryption proceed as P 2 = C 2 L 32 (E K (X 2)) X 3 = R 32 (X 2) C 2 = C 1 C 2 P 3 = C 3 L 32 (E K (X 3)) X 4 = R 32 (X 3) C 3 = C 2 C 3. At this point, we have three corrupted plaintexts P 1, P 2, and P 3. However, note that by the end of the third round, the register X 4 is no longer corrupted. The subsequent decryption step is P 4 = C 4 L 32 (E K (X 4)) X 5 = R 32 (X 4) C 4. Thus, the fourth step of decryption is uncorrupted. All subsequent decryption steps also will be free of errors. 10. In CBC, suppose that an error occurs (perhaps during transmission) in block C j to produce the corrupted C j, and that the subsequent blocks C j+1 and C j+2 are ok. Now start decrypting. If we try to decrypt to get P j we get P j = D K (C j) C j 1 which is corrupted because the decryption of Cj will be junk. Next, try to decrypt to get P j+1 : P j+1 = D K (C j+1) C j which, although D K (C j+1) is correct, when we add the corrupted C j we get a corrupted answer. Now proceed to try to decrypt C j+2 to get P j+2 : P j+2 = D K (C j+2) C j+1 which is uncorrupted since each of the components are D K (C j+2) and C j+1 are uncorrupted. 11. Let K be the key we wish to find. Use the hint. Then C 1 = E K (M 1) and C 2 = E K (M 1). Now, suppose we start a brute force attack by encrypting M 1 with different keys. If, when we use K j we get E Kj (M 1) = C 1 then we are done and the key we desire is K = K j. However, when we use K j we can eliminate another key. Here is how. If E Kj (M 1) = C 2 then we know (by complementation property) that E Kj (M 1) = C 2. Hence, if this happens, we know the key is K j since K j would decrypt C 2 to get M 1. We are effectively testing two keys for the price of one! Hence, the key space is cut in half and we only have to search an average of 2 54. 21 Chapter 5 - Exercises 1. (a) We have W(4) = W(0) T(W(0)) = T(W(0)). In the notation in Subsection 5.2.5, a = b = c = d = 0. The S-box yields e = f = g = h = 99 (base 10) = (binary). The round constant is r(4) = = We have e r(4) = Therefore, W(4) = T(W(0)) = We have W(5) = W(1) W(4) = W(4), and similarly W(7) = W(6) = W(5) = W(4). (b) We have W(9) = W(5) W(8) W(8), since W(5) 0. But W(10) = W(6) W(9) = W(6) W(5) W(8) = W(8), since W(6) = W(5). Also, W(11) = W(7) W(10) = W(7) W(6) W(9) = W(9), since W(7) = W(6). 2. (a) We have W(4) = W(0) T(W(0)) = T(W(0)). In the notation in Subsection 5.2.5, a = b = c = d = The S-box yields e = f = g = h = 22 (decimal) = (binary). The round constant is r(4) = = We have e r(4) = Therefore, W(4) = T(W(0)) = We have W(5) = W(1) W(4) = W(4). Also, W(6) = W(2) W(5) = W(2) W(1) W(4) = W(4), since W(1) = W(2). Finally, W(7) = W(3) W(6) = W(3) W(2) W(5) = W(5), since W(2) = W(3). (b) W(10) = W(6) W(9) = W(6) W(5) W(8) = W(8), since the entries of W(5) W(6) are strings of all 1 s. Finally, W(11) = W(7) W(10) = W(7) W(6) W(9) = W(9). 3. (a) Since addition in GF(2 8) is the same as, we have f(x 1) f(x 2) = α(x 1 + x 2) = α(x 3 + x 4) = f(x 3) f(x 4). (b) The ShiftRow transformation permutes the entries of the matrix, which has the effect of permuting the results of the XOR. If x 1 x 2 = x 3 x 4, then this still holds after permuting the entries. The MixColumn transformation has the form f(x) = Mx, where M 17.. 22 18 is a fixed matrix and x is a binary string represented as a matrix. Therefore, f(x 1) f(x 2) = Mx 1 Mx 2 = Mx 1 + Mx 2, since addition in GF(2 8) is XOR. This yields M(x 1 +x 2) = M(x 1 x 2). If x 1 x 2 = x 3 x 4, then we can reverse the above steps to obtain f(x 3) f(x 4). The RoundKey Addition has the form f(x) = x K. We have f(x 1) f(x 2) = x 1 x 2 = x 3 x 4 = f(x 3) f(x 4). 4. (a) It is easy to see that if functions f and g have the equal difference property, then the composition f g has the equal difference property. Since all steps in this modified AES algorithm have the equal difference property, the composition of all the steps has the property. (b) The steps in E involve permuting, multiplying by a matrix, and adding a matrix. Let E j (x) represent the result after j steps (there are 30 such steps). Let F j denote the similar encryption, but where nothing is done (that is, F j (x) = F j 1 (x)) in the jth step if the E j algorithm ends with AddRoundKey. We start with x 1 and x 2. Suppose that E j 1 (x 1) E j 1 (x 2) = F j 1 (x 1 x 2) for some j 1. If the jth step is ShiftRow, then the entries of all matrices are given the same permutation, so we have E j (x 1) E j (x 2) = F j (x 1 x 2). If the jth step is MixColumn, then everything is multiplied on the left by a matrix M. This again yields the relation with j in place of j 1. Finally, if the jth step is AddRoundKey, then a matrix K is XORed with E j 1 (x 1) and with E j 1 (x 2). These K s cancel each other. So E j (x 1) E j (x 2) = E j 1 (x 1) E j 1 (x 2). Since F j 1 = F j in this case, we obtain E j (x 1) E j (x 2) = F j (x 1 x 2). Therefore, this relation holds for all j (the case j = 0 represents no encryption, so it holds trivially). In particular, since E = E 30, and since F 30 is encryption with the AddRoundKey steps also removed, we have E(x 1) E(x 2) = F(x 1 x 2), as desired. (c) Eve uses part (b). She computes E(x 1) E(x 2). This is the encryption of x 1 x 2 using only ShiftRow and MixColumn, and is independent of the key. These steps are easily reversed to yield x 1 x 2. By XORing with x 1, Eve obtains x BS(x 1) = 99 = and BS(x 2) = 124 = , so BS(x 1) BS(x 2) = But BS(x 3) = 119 = and BS(x 4) = 123 = , so BS(x 3) BS(x 4) = Therefore, BS does not satisfy the equal difference property. By 3(a), affine maps satisfy this property, so BS is not affine. 23 Chapter 6 - Exercises 1. We have φ(n) = (p 1)(q 1) = = A quick calculation shows that (mod 11200). We have (mod 11413), so the plaintext was 1415 = no. 2. (a) Here φ(n) = 4 10 = 40. We are looking for a number d such that ed = 1 (mod 40). Thus, we want to solve for d in 3d = 1 (mod 40). Observe that d = 27 gives 3 27 = 81 = 1 (mod 40). Hence d = 27. (b) Here, you use Euler s Theorem. d is such that 3d = 1 + kφ(n) for some k. Then, c d = m 3d = m 1+kφ(n) = m (mod n) by Euler s Theorem. 3. The two possible plaintexts are 8 and 9. Encrypt each to get 8 3 (mod 437) = 75 and 9 3 (mod 437) = 292. Hence, the correct plaintext is Here, we want a number d such that (m 3) d (mod 101) = m 3d = m (mod 101). By Fermat s Little Theorem, we need to find d such that 3d = 1 (mod 100). Solving, we get d = 67 and thus decryption is accomplished by c 67 (mod 101). 5. Choose d with de 1 (mod p 1). Then y d x de x 1 x (mod p), since we work mod p 1 in the exponent. 6. The number e is m aba1 (mod n). Since aa 1 1 (mod φ(n)), and we work mod φ(n) in the exponent, we have e m b (mod n). Therefore Bob finds b 1 with bb 1 1 (mod φ(n)) and computes e b1. This will be m. 7. Nelson decrypts 2 e c to get 2 ed c d 2c d 2m (mod n), and therefore sends 2m to Eve. Eve divides by 2 mod n to obtain m. 8. We have c 2 c e2 1 (mod n). Therefore, this double encryption is mc1c2 the same as single encryption with encryption exponent e 1 e 2. So the security is at the same level as single encryption. 9. (a) x 1 2 φ(n) (x p 1) (q 1)/2 1 (q 1)/2 1 (mod p), and similarly for q. Note that since q is odd, the exponent (q 1)/2 is an integer. The following proof doesn t work: (x 1/2) φ(n) 1 (mod n) by Euler. The problem is that x 1/2 might not make sense mod n. Fractional exponents must be avoided. (b) Use the Chinese Remainder Theorem to combine the two congruences from (a). (c) If ed 1 (mod 1 2 φ(n)), then ed = φ(n)k for some integer k. Therefore x ed x (x 1 2 φ(n)) k x 1 k x (mod n), where the middle congruence used part (b). 19 24 e = 1 means that the ciphertext is the same as the plaintext, so there is no encryption. The exponent e = 2 does not satisfy gcd(e,(p 1)(q 1)) = 1, so it is not allowed in RSA (no d will exist). 11. Since n 1 n 2, and since they are not relatively prime, we have gcd(n 1,n 2) must be a nontrivial common factor of n 1 and n 2. Therefore, we can factor n 1 and n 2 and break the systems. 12. We have ( ) 2 (2 7) 2 (mod n). Compute gcd(,) = Therefore, = Let a = , b = , and c = Then (abc) 2 = (mod). Next, we need to check that abc ±6. After that, factoring is accomplished by just calculating gcd(x y,n). The information = 77 (mod) was just trick information. 14. Use the Chinese remainder theorem to solve x 7 (mod p), x 7 (mod q). Then x 2 49 (mod p) and also (mod q), hence (mod pq). 15. (a) Note, if n were prime, then k 2 2 n 1 1 (mod n). This would contradict the assumption in part (a), and hence n must not be prime. (b) Suppose k 2 1 (mod n), then we have a case of the form x 2 y 2 (mod n) yet x y (mod n), and hence may factor by calculating gcd(x y,n). Here, x = k and y = 1. Thus, to factor, we just calculate gcd(k 1, n). 16. Since gcd(e a,e B) = 1, there are integers x and y with e A x + e B y = 1. Therefore, m = m 1 = (m ea) x (m eb) y c x A cy B (mod n). Since Eve can calculate this last quantity, she can calculate m. 17. Make a list of 1 e,2 e,...,26 e (mod n). For each block of ciphertext, look it up on the list and write down the corresponding letter. The message given is hello. 18. Let d = gcd(x + y,n). If d = n, then n x + y, hence x y, contradiction. If d = 1, then Exercise 3.3(b) implies that n x y, so x y (mod n), contradiction. Since d 1,n, we find that d is a nontrivial factor of n. 19. (a) m is a multiple of (p 1)(q 1), hence a multiple of (p 1). Note that gcd(a,n) = 1 implies that gcd(a,p) = 1. Since a p 1 1 (mod p), we also have a m 1 (mod p). Similarly, a m 1 (mod q). (b) If a 0 (mod p), then a m 1 (mod p), from (a). Multiply by a to get a m+1 a (mod p). If 0 (mod p), then this congruence still holds, since both sides are 0 mod p. Similarly, a m+1 a (mod q). The Chinese Remainder Theorem allows us to combine these to get a m+1 a (mod pq). (c) Let m = ed 1, which is a multiple of φ(n). From (b), we have a ed = a m a (mod n). (d) If p and q are large, then the probability is only 1/p that a is a multiple of p and 1/q that a is a multiple of q. Both 1/p and 1/q are small, so the probability that gcd(a,n) 1 is small (1/p + 1/q (1/(pq), to be precise). 20. We would need ed 1 (mod (p 1)(q 1)(r 1)). The verification is the same as the one for RSA. 21. Note that d = e, so Alice sends m e2 m ed m 25 (a) Note that gcd(e,24) = 1 leaves only 1,5,7,11,13,17,19, and 23 as possibilities. These may be paired into e and e (mod 24) pairs. Note that e 2 (e) 2 (mod 24). Hence, it suffices to check just 1,5,7, and 11 to see that e 2 1 (mod 24). This can be easily verified by hand. (b) The encryption exponents e are precisely those e such that gcd(e,24) = 1. In RSA, we seek to find a d such that ed 1 (mod 24). We already know that e e 1 (mod 24) from part (a). Since gcd(e,24) = 1, inverses are unique and hence d = e. 23. The spy tells you that m (mod n). Hence ψ = acts like φ(n) (in the sense of Euler s Theorem). Now, if we can find a δ such that eδ 1 (mod ψ), then we have that eδ = kψ + 1 for some k, and thus c δ = m eδ = (m ψ) k m (mod n) = m. Therefore, all that is needed to decrypt is to use the publicly available e and solve eδ = 1 (mod 12345), and then use δ as the decryption exponent. 24. (a) Write de = k for some integer k. Then m de m (m 1000) k m 1 k m (mod n). (b) There are 1000 solutions to x (mod p) and 1000 solutions to x (mod q). There are = 10 6 ways to combine them using the Chinese Remainder Theorem. So there are 10 6 solutions to m (mod n). 25. Since ed 1 (mod) we have ed = k for some integer k. Then c d (mod) m ed (m) k m = m (mod). 26. Let c A and c B be the outputs of the two machines. Then c A c B 0 (mod p) but c B c A 1 (mod q). Therefore gcd(c a c b,n) = p, and q = n/p. 27. (a) The new ciphertext is c e m e. Eve makes two lists: 1. c 1 x e for all x with 1 x 10 9, and 2. (100y) e for all y with 1 y A match gives c 1 (100xy) e, so m = xy. Another way: Eve divides c 1 by e (mod n) and then uses the short message attack from Section 6.2. (b) Suppose the length of m is k. Then m m = (10 k + 1)m. Therefore, the encrypted message is (10 k +1) e m e. Eve simply divides this by (10 k +1) e (mod n) and then uses the short message attack. 28. (a) Suppose 0 x < (2 1) n 1 and s = n. Then x + s < (2 1) n 1 + s < (2 1) n 1 + n + 1 = 2n. (b) Suppose p f(x), then (x+s) 2 n = kp for some integer k. Thus (x+s) 2 kp = n. Operating modulo p gives n (x + s) 2 (mod p). (c) From (b), n is a square mod p, so n a 2. Since p n, we have a 0 (mod n). We obtain f(x) (x + s) 2 a 2 (x + s + a)(x + s a) (mod p). Since p is prime, either x + s + a 0 or x + s a 0 (mod p). This yields x ±a s (mod p). Since p is odd and a 0, these two values of x are distinct mod p. (d) We subtract log p exactly for those p for which f(x) 0 (mod p), so we subtract once for each prime factor of f(x). Since we are assuming that f(x) = 26 22 p 1 p 2 p r is a product of distinct primes, we have log f(x) log p 1 log p r = 0. (e) If f(x) has a large prime factor p, then the register will be at least log p, which is large. If all of the factors of f(x) are in B, then the register is 0 if the prime factors are distinct. In general, the register will contain a sum of logs of some primes from B. These will tend to be small. Moreover, the multiple prime factors of f(x) will tend to be the small primes in the factor base (for example, it is much more likely that 2 2 or 3 2 divides f(x) than divides f(x)). Therefore, the register will tend to be small. (f) The procedure in d only works with 2 out of each p values of x, rather than with each x, which is what would happen with trial division. Subtracting is a much faster operation than dividing. Also, the subtraction can be done in floating point, while the division is done with large integer arithmetic. 27 Chapter 7 - Exercises 1. (a) Perhaps the easiest way to do this is to list the powers of 2 mod 13 until we get 3: 2,2 2 4,2 3 8, (mod 13). Therefore L 2 (3) = 4. (b) 2 7 = (mod 13), which implies that L 2 (11) = (a) (mod 11), , (b) Since 2 is a primitive root, 2 5 = 2 (11 1)/2 1 (mod 11). Therefore, (2 x) 5 (1) x, so x is odd. 3. Since 5 is a primitive root, (mod 1223). Therefore, x (1) x, so x is even. 4. p 1 = First we compute L = L 2 (14) mod 2: We have 14 (p 1)/2 1 (mod 19), so L 1 (mod 2). Now compute L mod 3: We have 14 (p 1)/3 7 (mod 19). Since (mod 19), we have L 1 (mod 3). Now write L = 1+3x 1. Let β (mod 19). Then β (p 1)/ (2 (p 1)/3) 2, so x 1 = 2. Therefore L = 7 (mod 9). Since L 1 (mod 2) from above, we use the Chinese Remainder Theorem to obtain L = (a) Let x = L α (β 1), y = L α (β 2), and z = L α (β 1 β 2). Then α x+y α x α y α z (mod p). By the proposition in Section 3.7, we have x + y z (mod p 1), which is what we wanted to prove. (b) First, we need the fact that α u α v (mod p) if and only if u v (mod ord p (α)). This is proved by rewriting the congruence as α u v 1 (mod p) and using Exercise 3.9(d), which says that α u v 1 (mod p) if and only if u v 0 (mod ord p (α). Now use the proof of part (a) above, with p 1 replaced by ord p (α). Instead of using the proposition in Section 3.7, use the fact just proved (about u and v). 6. (a) L 2 (24) 3L 2 (2) + L 2 (3) (mod 100). Therefore, L 2 (24) = 72. (b) L 2 (24) 3L 2 (5) (mod 100). Therefore, L 2 (24) = Since 11 = 44/2 2, and since (mod 137), we have 3 x Therefore, x = (a) If someone knows 2 x (mod p), it is difficult to find x since this is the discrete logarithm problem. (b) If p has only 5 digits, it is easy to compute 2 k (mod p) for k = 1,2,...p 1 until the number 2 x (mod p) is found. Then k = x is the password. 9. (a, b) We have p 1 = = Note that (mod p), and 23 28 (mod p). We have 2 (p 1)/ (1) 0 (mod p), so x 0 = 1. Therefore β 1 β 2 (mod p). Then β (p 1)/ (mod p), so x 1 = 0 and β 2 = 2. Continuing in this manner, we get x 3 = = x 10 = 0 and β 2 = = β 11 = 2. Then so x 11 = 1. Therefore β (p 1)/ = (mod p), β 12 β 11 α x (mod p). We have so x 12 = 1. Then β (p 1)/ (mod p), β (mod p). We have so x 13 = 0 and β 14 = β 13 = 256. Then so x 14 = 1 and Then so x 15 = 1 and β (p 1)/ (mod p), β (p 1)/ (mod p), β β (p 1)/ (mod p), β This means we can stop. We have (mod p). (mod p). L 3 (2) = x x 15 = = Eve computes b 1 with bb 1 1 (mod p 1). Then x b1 2 αbb1 α 1 α (mod p). 11. m tr a (mod 17). 12. (a) Write d in base N, so d = a 0 + a 1 N with 0 a i < N. Then m c d c a0+a1n implies that mc a1n c a0. Therefore, there is a match for j = a 0 and k = a 1. This gives a 0 + a 1 N as a candidate for d. (b) c = m = 1 gives a match for every j,k, so it is unlikely that the first match yields the correct d. (c) The lists are of length approximately N. This is approximately the time required to factor n by dividing by all the primes up to N. 29 Chapter 8 - Exercises 1. It is easy to construct collisions: h(x) = h(x+p 1), for example. (However, it is fairly quickly computed (though not fast enough for real use), and it is preimage resistant.) 2. (a) Finding a preimage is the same as finding a square root mod pq. This is computationally equivalent to factoring (see page 88). (b) h(x) h(n x) for all x, so it is easy to find collisions. 3. h can be computed quickly, so (1) is satisfied. However, h(x 0 0) = x, so it is not preimage resistant. Taking different numbers of 0-blocks yields collisions, so it is not strongly collision-free. 4. The probability that no two have birthdays in the same month is ( )( ) ( ) = (a) f (x) = 1/(1 x) + 1 = x/(1 x) 0 when 0 x < 1. Also, g (x) = 1/(1 x) x = x(1 2x)/(1 x) 0 when 0 x 1/2. (b) f is decreasing and f(0) = 0, so ln(1 x) + x = f(x) 0 for 0 x 1/2. Therefore, ln(1 x) x. The other inequality follows similarly. (c) From (b), we have j (N j2 N 2 ln 1 j) j N N. Summing for 1 j r 1 yields (r 1)r (r 1)r(2r 1) r 1 (2N 6N 2 ln 1 j) (r 1)r N N. Since (r 1)r(2r 1) < (r)r(2r) = 2r 3, the result follows. (d) Exponentiate the result in (c) and rearrange the exponents. (e) As N, we have c/ N 0, so e c/ N e 0 = 1. Therefore, both ends of the inequalities in (d) are close to e λ. 6. (a) The probability is (1/2) j that we succeed on the jth try, so the expected number of tries is 1(1/2)+2(1/4)+3(1/8)+. To evaluate this sum S, consider S 1 S = ( ) ( ) 2 25 j=1