

INSTRUCTOR'S
SOLUTIONS MANUAL

INTRODUCTION TO CRYPTOGRAPHY
WITH CODING THEORY
THIRD EDITION

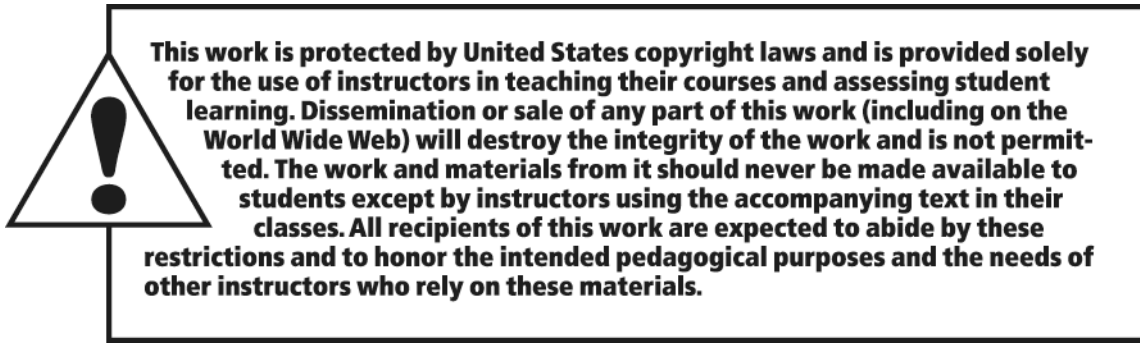
Wade Trappe

Rutgers University

Lawrence C. Washington

University of Maryland





The author and publisher of this book have used their best efforts in preparing this book. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness. The author and publisher make no warranty of any kind, expressed or implied, with regard to these programs or the documentation contained in this book. The author and publisher shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of these programs.

Reproduced by Pearson from electronic files supplied by the author.

Copyright © 2021, 2006 by Pearson Education, Inc. 221 River Street, Hoboken, NJ 07030. All rights reserved.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. Printed in the United States of America.



ISBN-13: 978-0-13-487691-7

ISBN-10: 0-13-487691-1

Contents

Exercises

Chapter 2 - Exercises	1
Chapter 3 - Exercises	4
Chapter 4 - Exercises	10
Chapter 5 - Exercises	12
Chapter 6 - Exercises	14
Chapter 7 - Exercises	17
Chapter 8 - Exercises	18
Chapter 9 - Exercises	19
Chapter 10 - Exercises	23
Chapter 11 - Exercises	24
Chapter 12 - Exercises	26
Chapter 13 - Exercises	28
Chapter 14 - Exercises	30
Chapter 15 - Exercises	31
Chapter 16 - Exercises	32
Chapter 17 - Exercises	33
Chapter 18 - Exercises	35

Chapter 19 - Exercises	36
Chapter 20 - Exercises	37
Chapter 21 - Exercises	39
Chapter 22 - Exercises	42
Chapter 23 - Exercises	44
Chapter 24 - Exercises	45
Chapter 25 - Exercises	48

Mathematica problems

Chapter 2	49
Chapter 3	54
Chapter 5	58
Chapter 6	60
Chapter 9	62
Chapter 10	66
Chapter 12	67
Chapter 13	68
Chapter 17	71
Chapter 21	73
Chapter 24	75

Maple problems

Chapter 2	78
Chapter 3	84
Chapter 5	90

Chapter 6	90
Chapter 9	91
Chapter 10	95
Chapter 12	96
Chapter 13	97
Chapter 17	99
Chapter 21	100
Chapter 24	102

MATLAB problems

Chapter 2	104
Chapter 3	112
Chapter 5	117
Chapter 6	120
Chapter 9	122
Chapter 10	127
Chapter 12	128
Chapter 13	129
Chapter 17	131
Chapter 21	133
Chapter 24	136

Sage problems

Chapter 2	139
Chapter 3	142

Chapter 5	145
Chapter 6	146
Chapter 9	147
Chapter 10	149
Chapter 12	150
Chapter 13	151
Chapter 17	152
Chapter 21	153
Chapter 24	155

Chapter 2 - Exercises

1. Among the shifts of *EVIRE*, there are two words: *arena* and *river*. Therefore, Anthony cannot determine where to meet Caesar.

3. The inverse of $9 \pmod{26}$ is 3. Therefore, the decryption function is $x = 3(y - 2) = 3y - 6 \pmod{26}$. Now simply decrypt letter by letter as follows. $U = 20$ so decrypt U by calculating $3 * 20 - 6 \pmod{26} = 2$, and so on. The decrypted message is 'cat'.

5. Changing the plaintext to numbers yields 7, 14, 22, 0, 17, 4, 24, 14, 20. Applying $5x + 7$ to each yields $5 \cdot 7 + 7 = 42 \equiv 16 \pmod{26}$, $5 \cdot 14 + 7 = 77 \equiv 25$, etc. Changing back to letters yields *QZNHOBXZD* as the ciphertext. The decryption function is $21x + 9$.

7. Let $mx + n$ be the encryption function. Since $h = 7$ and $N = 13$, we have $m \cdot 7 + n \equiv 13 \pmod{26}$. Using the second letters yields $m \cdot 0 + n \equiv 14$. Therefore $n = 14$. The first congruence now yields $7m \equiv -1 \pmod{26}$. This yields $m = 11$. The encryption function is therefore $11x + 14$.

9. Let the decryption function be $x = ay + b$. The first letters tell us that $7 \equiv a \cdot 2 + b \pmod{26}$. The second letters tell us that $0 \equiv a \cdot 17 + b$. Subtracting yields $7 \equiv a \cdot (-15) \equiv 11a$. Since $11^{-1} \equiv 19 \pmod{26}$, we have $a \equiv 19 \cdot 7 \equiv 3 \pmod{26}$. The first congruence now tells us that $7 \equiv 3 \cdot 2 + b$, so $b = 1$. The decryption function is therefore $x \equiv 3y + 1$. Applying this to *CRWWZ* yields *happy* for the plaintext.

11. 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.)

13. For an affine cipher $mx + n \pmod{27}$, we must have $\gcd(27, m) = 1$, and we can always take $1 \leq m \leq 27$. So we must exclude all multiples of 3, which leaves 18 possibilities for m . All 27 values of n are possible, so we have $18 \cdot 27 = 486$ keys. When we work mod 29, all values $1 \leq m \leq 28$ are allowed, so we have $28 \cdot 29 = 812$ keys.

15. (a) In order for α to be valid and lead to a decryption algorithm, we need $\gcd(\alpha, 30) = 1$. The possible values for α are 1, 7, 11, 13, 17, 19, 23, 29.

(b) We need to find two x such that $10x \pmod{30}$ gives the same value.

There are many such possible answers, for example $x = 1$ and $x = 4$ will work. This corresponds to the letters 'b' and 'e'.

17. If $x_1 = x_2 + (26/d)$, then $\alpha x_1 + \beta = \alpha x_2 + \beta + (\alpha/d)26$. Since $d = \gcd(\alpha, 26)$ divides α , the number $\alpha/26$ is an integer. Therefore $(\alpha/d)26$ is a multiple of 26, which means that $\alpha x_1 + \beta \equiv \alpha x_2 + \beta \pmod{26}$. Therefore x_1 and x_2 encrypt to the same ciphertext, so unique decryption is impossible.

19. (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	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 BBBB. Combining them gives the original plaintext BBBBABB.

21. 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 1 C . 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 .

23. Since the entries of \mathbb{A}_i are the same as those in \mathbb{A}_0 (shifted a few places) the two vectors have the same length. Therefore

$$\mathbb{A}_0 \cdot \mathbb{A}_i = |\mathbb{A}_0||\mathbb{A}_i| \cos \theta = |\mathbb{A}_0|^2 \cos \theta.$$

Note that $\cos \theta \leq 1$, and equals 1 exactly when $\theta = 0$. But $\theta = 0$ exactly when the two vectors are equal. So we see that the largest value of the cosine is when $\mathbb{A}_0 = \mathbb{A}_i$. Therefore the largest value of the dot product is when $i = 0$.

25. (a) The ciphertext will be one letter repeated a few hundred times, so the plaintext must also be a repeated letter. But the plaintext could be the shift of any letter, so the key and the plaintext cannot be deduced.

(b) The ciphertext will be one letter repeated a few hundred times, so the plaintext must also be a repeated letter. But the plaintext could be the encryption of any letter, so the key and the plaintext cannot be deduced.

(c) The ciphertext will be a sequence of letters repeated many times. This means that the plaintext consists of a pattern of letters that is repeated (for example, if the key length is 6, then three letters repeated many times would cause the ciphertext to repeat every 6 letters). If the key is a word, then the ciphertext is this word repeated several times. But Eve cannot be sure of this, so the key and the plaintext cannot be deduced with certainty.

27. EK IO IR NO AN HF YG BZ YB LF GM ZN AG ND OD VC MK

29. AAXFFGDGAFAX

31. (a) Since $2^{128} = 2^{64} \cdot 2^{64}$, it will take 2^{64} days, which is approximately 5×10^{16} years.

(b) It will take around 5×10^{14} years (the offset by 10 years is insignificant), which is much less than the time in part (a).