Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

SKU: 9780134859064-SOLUTIONS

INSTRUCTOR'S SOLUTIONS MANUAL

INTRODUCTION TO CRYPTOGRAPHY WITH CODING THEORY

THIRD EDITION

Wade Trappe

Rutgers University

Lawrence C. Washington

University of Maryland

Pearson

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

This work is protected by United States copyright laws and is provided solely for the use of instructors in teaching their courses and assessing student learning. Dissemination or sale of any part of this work (including on the World Wide Web) will destroy the integrity of the work and is not permitted. The work and materials from it should never be made available to students except by instructors using the accompanying text in their classes. All recipients of this work are expected to abide by these restrictions and to honor the intended pedagogical purposes and the needs of other instructors who rely on these materials.

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

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

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

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

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

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

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

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

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

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

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 mod 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.

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

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  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.

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 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.

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.

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

(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 that the time in part (a).

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

Chapter 2 - Mathematica

Problem 1. Let's call up the ciphertext, then try all shifts of it.

In[1]:= **allshifts[ycve]**

```
ycvejqwvhqtdtwvwu
zdwfkrxwirueuxwxv
aexglsyxjsvfvyxyw
bfyhmtzyktwgwzyzx
cgzinuazluxhxazay
dhajovbamvyiybabz
eibkpwcbnwzjzcbca
fjclqxdcoxakadcdb
gkdmryedpyblbedec
hlenszfeqzcmcfefd
imfotagfradndgfge
jngpubhgsbeoehghf
kohqvcihtcfpfihig
lpirwdjiudgqgjijh
mqjsxekjvehrhkjki
nrktyflkwfisilklj
osluzgmlxgjtjmlmk
ptmvahnmyhkuknmnl
qunwbionzilvlonom
rvoxcjpoajmwmpopn
swpydkqpbknxnqpqo
txqzelrqcloyorqrp
uyrafmsrdmpzpsrsq
vzsbgntsenqaqtstr
watchoutforbrutus
xbudipvugpscsvuvt
```

The plaintext was "watch out for Brutus"

Problem 3.

In[1]:= **frequency[jidf]**

```
{a, 3}, {b, 6}, {c, 4}, {d, 3}, {e, 2}, {f,
```


Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

```
4}, {g, 4}, {h, 9}, {i, 8}, {j, 6}, {k, 0}, {l,
0}, {m, 0}, {n, 0}, {o, 1}, {p, 1}, {q, 0}, {r,
0}, {s, 8}, {t, 2}, {u, 4}, {v, 2}, {w, 0}, {x,
1}, {y, 0}, {z, 8}
```

Therefore, h is the encryption of e, and d and w encrypt to d and a, but not necessarily in that order. Solving for the decryption function shows that only $15x + 3$ is possible.

In[2]:= **affinecrypt[jidf, 15, 3]**

```
itwastwooclockintheafternoonandthestudentswereontheiripadsshoppingorsleeping
```

Problem 5. Solve y=3x+b mod 26 for x to obtain x=9y-9b mod 26. Therefore, the plaintext can be found by computing 9y, then trying all shifts:

In[1]:= **allshifts[affinecrypt[tcab,9,0]]**

```
psajpuoetlkooexehepeao
qtbkqvpfumlppfyfifqfbp
ruclrwqgvnmqqgzgjgrgcq
svdmsxrhwonrrhahkhshdr
twentysixpossibilities
uxfouztjyqpttjcjmjujft
vygpvaukzrquukdknkvkgu
wzhqwbvlasrvvlelolwlhv
xairxcwmbtswwmfmpmxmiw
ybjsydxncutxxngnqnynjx
zcktzeyodvuyyohorozoky
adluafzpewvzzpipspaplz
bemvbgaqfxwaaqjqtqbqma
cfnwchbrgyxbbrkrurcrnb
dgoxdicshzyccslsvsdsoc
ehpyejdtiazddtmtwtetpd
fiqzfkeujbaeeunuxufuqe
gjraglfvkcbffvovyvgvrf
hksbhmgwldcggwpwzwhwsg
iltcinhxmedhhxqxaxixth
jmudjoiynfeiiyrybyjyui
knvekpjzogfjjzszczkzvj
lowflqkaphgkkatadalawk
mpxgmrlbqihllbubebmbxl
nqyhnsmcrjimmcvcfcncym
orziotndskjnndwdgdodzn
```

Therefore the plaintext is "twentysixpossibilities". (The encryption function was y=3x+14 mod 26.)

Copyright © 2021 Pearson Education. Inc.

Problem 7. Look at the program and extract the relevant commands, then modify
the commands and command names (to avoid changing the existing commands):

In[1]:= **alphabetDNA="ACGT";**

```
keyDNA[n_]:=
  Table[StringTake[alphabetDNA,{i}] ->
    StringTake[alphabetDNA,{Mod[i-1+n,4]+1}],{i,1,4}];
shiftDNA[plaintext_,n_]:=
  StringReplace[plaintext,keyDNA[n]];
affkeyDNA[m_,n_]:=
  Table[StringTake[alphabetDNA,{i}] ->
    StringTake[alphabetDNA,{Mod[m*(i-1)+n,4]+1}], {i,1,4}];
affinecryptDNA[plaintext_,m_,n_]:=
  StringReplace[plaintext, affkeyDNA[m,n]];
```

Part(a): Shift the plaintext by 1 (the plaintext has been stored as DNA):

In[2]:= **shiftDNA[DNA,1]**

```
TCCAAGTGTTGGTGCCAACCGGGAGCGACCCTTTCAGAGACTCCGA
```

Part (b): Let the affine function be y=mx+n. Then we need
gcd(m,4)=1.

Here is an affine encryption:

In[3]:= **affinecryptDNA[DNA,3,2]**

```
AGGTTCACAACCACGGTTGGCCCTCGCTGGGAAAGTCTCTGAGGCT
```

Here is what could happen if gcd(m,4) is not 1:

In[4]:= **affinecryptDNA[DNA,2,1]**

```
CCCTTTCTCCTTCTCCTTCCTTTTTCTTCCCCCCCTTTTTCCCCTT
```

Notice that only C and T appear in the ciphertext. Both A and G are encrypted to C.

Problem 9. Find the key length:

In[1]:= **coinc[ocwy,1]**

13

In[2]:= **coinc[ocwy,2]**

13

In[3]:= **coinc[ocwy,3]**

11

In[4]:= **coinc[ocwy,4]**

Copyright © 2021 Pearson Education. Inc.

6

In[5]:= **coinc[ocwy,5]**

15

In[6]:= **coinc[ocwy,6]**

23

In[7]:= **coinc[ocwy,7]**

13

We guess that the key length is 6.
Now, perform the following calculations:

In[8]:= **vigvec[ocwy,6,1]**

```
{0.0417308,0.0452115,0.0372308,0.0451731,0.0294615,0.0301731,0.0419808,
0.0560577,0.038,0.0398654,0.0351731,0.0366538,0.0316731,
0.0392308,0.0411154,0.0388654,0.0409808,0.0322115,0.0350769,
0.0384423,0.0475577,0.0323846,0.0448846,0.0393654,0.033,0.0295}
```

In[9]:= **Max [%]**

0.0560577

This occurs in the 8th position.

In[10]:= **corr[ocwy,6,2]**

```
{0.0360577,0.0435192,0.0398846,0.03825,0.0359423,0.0313269,0.0271538,
0.0385,0.0441154,0.0411346,0.0473077,0.0308462,0.0300769,
0.0466154,0.0641923,0.0341923,0.0263269,0.0384231,0.0416538,
0.0361154,0.0362308,0.0365577,0.0325962,0.04275,0.0442308,0.037}
```

In[11]:= **Max [%]**

0.0641923

This occurs in the 15th position.

In[12]:= **corr[vigvec[ocwy,6,3]]**

```
{0.0474231,0.0376731,0.0362885,0.0412692,0.0347885,0.0285192,0.0333462,
0.0411731,0.0326154,0.0307885,0.0447115,0.0608269,0.0389231,
0.0308654,0.03975,0.0458077,0.0332308,0.0335,0.0406154,
0.0319423,0.0270769,0.0443846,0.0481538,0.0370962,0.0356731,0.0445577}
```

In[13]:= **Max [%]**

0.0608269

This occurs in the 12th position.

In[14]:= **vigvec[ocwy,6,4]**

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

```
{0.0461346,0.0405,0.03875,0.0313654,0.0392692,0.0342885,0.0341154,0.0291154,
0.0478269,0.0391346,0.0355769,0.0348077,0.0608846,0.0437885,
0.0291731,0.0347115,0.0438846,0.0282692,0.0314615,0.0426154,
0.0351538,0.0313846,0.0409231,0.0447885,0.0410577,0.0420192}
```

In[15]:= **max** [%]

0.0608846

This occurs in the 13th position.

In[16]:= **corr[vigvec[ocwy,6,5]**

```
{0.0506346,0.0364423,0.032,0.0352692,0.0602308,0.0388846,0.0328077,
0.0376731,0.0451154,0.0265385,0.0355769,0.0444615,0.0360577,
0.0361154,0.0383654,0.0446154,0.0360192,0.0417308,0.0380769,
0.0432692,0.0394038,0.0364038,0.0366346,0.03375,0.0353846,0.0295385}
```

In[17]:= **max** [%]

0.0602308

This is in the 5th position.

In[18]:= **vigvec[ocwy,6,6]]**

```
{0.03125,0.0328654,0.0522885,0.0472308,0.0258077,0.0328654,0.0490577,
0.03925,0.0310192,0.0324808,0.0397885,0.0301154,0.0384038,0.0357692,
0.0403846,0.0394808,0.0348269,0.0372115,0.0636923,0.0385962,
0.0274423,0.0348269,0.0485385,0.0293846,0.0417115,0.0467115}
```

In[19]:= **max** [%]

0.0636923

This is in the 19th position.
Since the 1st position corresponds to a shift of 0, etc., we find that the shifts were by 7, 14, 11, 12, 4, 18. The key word was "holmes". Decrypt:

In[20]:= **vigenere[ocwy,-{7,14,11,12,4,18}]**

```
holmeshadbeenseatedforsomehoursinsilencewithhislongthinbackcurved
overachemicalvesselinwhichhewasbrewingaparticularly
malodorousproducthisheadwassun
kuponhisbreastandhelookedfrommypointofviewlikeastrange
lankbirdwithdullgreyplumageandablacktopknot
sowatsonsaidhesuddenlyyoudonotproposetoinvesti
nsouthafricansecurities
```

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

Chapter 2 - Maple

```
> Problem 1.  Let's call up the ciphertext:
> ycve
```

"ycvejqwvhqtdtwvwu"

```
> Try all shifts and see which is an English text:
> allshifts(ycve)
```

"ycvejqwvhqtdtwvwu"
"zdwfkrxwirueuxwxv"
"aexglsyxjsvfvyxyw"
"bfyhmtzyktwgwzyzx"
"cgzinuazluxhxazay"
"dhajovbamvyiybabz"
"eibkpwcbnwzjzcbca"
"fjclqxdcoxakadcdb"
"gkdmryedpyblbedec"
"hlenszfeqzcmcfefd"
"imfotagfradndgfge"
"jngpubhgsbeoehghf"
"kohqvcihtcfpfihig"
"lpirwdjiudgqgjijh"
"mqjsxekjvehrhkjki"
"nrktyflkwfisilklj"
"osluzgmlxgjtjmlmk"
"ptmvahnmyhkuknmnl"
"qunwbionzilvlonom"
"rvoxcjpoajmwmpopn"
"swpydkqpbknxnqpqo"
"txqzelrqcloyorqrp"
"uyrafmsrdmpzpsrsq"
"vzsbgntsenqaqtstr"
"watchoutforbrutus"
"xbudipvugpscsvuvt"

```
> The plaintext was  "watch out for Brutus"

> Problem 3.
```


Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

```
> frequency(jidf)
```

[3, 6, 4, 3, 2, 4, 4, 9, 8, 6, 0, 0, 0, 0, 1, 1, 0, 0, 8, 2, 4, 2, 0, 1, 0, 8]

```
> Therefore, h in the ciphertext correponds to e in the plaintext
> and a and d correspond to d and w in some order.
> Only a corresponding to d yields a permissible decryption function,
> which is 15x+3.
> affinecrypt(jidf,15,3)
```

"itwastwooclockintheafternoonandthestudentswereontheiripadsshoppingorsleeping"

```
> Problem 5.
> Solve y=3x+b mod 26 for x to obtain  x=9y-9b mod 26.  Therefore,
the
> plaintext
> can be found by computing 9y, then trying all shifts:
> allshifts(affinecrypt(tcab,9,0))
```

"psajpuoetlkooexehepeao"
"qtbkqvpfumlppfyfifqfbp"
"ruclrwqgvnmqqgzgjgrgcq"
"svdmsxrhwonrrhahkhshdr"
"twentysixpossibilities"
"uxfouztjyqpttjcjmjujft"
"vygpvaukzrquukdknkvkgu"
"wzhqwbvlasrvvlelolwlhv"
"xairxcwmbtswwmfmpmxmiw"
"ybjsydxncutxxngnqnynjx"
"zcktzeyodvuyyohorozoky"
"adluafzpewvzzpipspaplz"
"bemvbgaqfxwaaqjqtqbqma"
"cfnwchbrgyxbbrkrurcrnb"
"dgoxdicshzyccslsvsdsoc"
"ehpyejdtiazddtmtwtetpd"
"fiqzfkeujbaeeunuxufuqe"
"gjraglfvkcbffvovyvgvrf"
"hksbhmgwldcggwpwzwhwsg"
"iltcinhxmedhhxqxaxixth"
"jmudjoiynfeiiyrybyjyui"
"knvekpjzogfjjzszczkzvj"
"lowflqkaphgkkatadalawk"
"mpxgmrlbqihllbubebmbxl"

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

"nqyhnsmcrjimmcvcfcncym"

"orziotndskjnndwdgdodzn"

```
> Therefore the plaintext is "twentysixpossibilities".
> (The encryption function was y=3x+14 mod 26.)


> Problem 7. Look at the program and extract the relevant commands,
> then modify the commands and command names (to avoid changing
the
> existing commands):
> numbDNA:=table([" "=0,"A"=1, "C"=2, "G"=3, "T"=4]):
> alphDNA:=table([0=" ",1="A",2="C",3="G",4="T"]):
> shiftDNA:=proc(txt,n)
> local i, z;
> z :=NULL
> for i from 1 while i<= length(txt) do
> z:=cat(z,(alphDNA[(numbDNA[substring(txt,i)]+n-1 mod 4)+1]))
> end do
> return(z)
> end:
> affinecryptDNA:= proc(txt,m,n)
> local i,z
> z:=NULL
> for i from 1 while i<=length(txt) do
> z:=cat(z,(alphDNA[((numbDNA[substring(txt,i)]-1)*m+n mod
> 4)+1]))
> end do
> return(z)
> end:
> Part (a): Shift the plaintext by 1 (the plaintext has been stored
as
> DNA):
> shiftDNA(DNA,1)
```

"TCCAAGTGTTGGTGCCAACCGGGAGCGACCCTTTCAGAGACTCCGA"

```
> Part (b) Let the affine function be y=mx+n. Then we need
> gcd(m,4)=1.
> Here is an affine encryption:
> affinecryptDNA(DNA,3,2)
```

"AGGTTCACAACCACGGTTGGCCCTCGCTGGGAAAGTCTCTGAGGCT"

```
> Here is what could happen if gcd(m,4) is not 1:
> affinecryptDNA(DNA,2,1)
```


Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

"CCCTTTCTCCTTCTCCTTCCTTTTTCTTCCCCCCCTTTTTCCCCTT"

```
> Notice that only C and T appear in the ciphertext.Both A and
G are
> encrypted to C.

> Problem 9.  Find the key length:
> coinc(ocwy,1)
                                13
> coinc(ocwy,2)
                                13
> coinc(ocwy,3)
                                11
> coinc(ocwy,4)
                                 6
> coinc(ocwy,5)
                                15
> coinc(ocwy,6)
                                23
> coinc(ocwy,7)
                                 8
> We guess that the key length is 6.
> Now, perform the same calculations as in Problem 7:
> corr(vigvec(ocwy,6,1))
```

0.04173076921, 0.04521153846, 0.03723076924, 0.04517307693, 0.02946153846, 0.03017307693, 0.04198076922, 0.05605769227, 0.03799999999, 0.03986538462, 0.03517307692, 0.03665384615, 0.03167307692, 0.03923076923, 0.04111538460, 0.03886538463, 0.04098076924, 0.03221153848, 0.03507692307, 0.03844230769, 0.04755769229, 0.03238461538, 0.04488461539, 0.03936538462, 0.03300000001, 0.02950000002

```
> max(%)
                        0.05605769227
> This occurs in the 8th position.
> corr(vigvec(ocwy,6,2))
```


Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

0.03605769230, 0.04351923078, 0.03988461538, 0.03825000001, 0.03594230769, 0.03132692308, 0.02715384617, 0.03850000000, 0.04411538461, 0.04113461539, 0.04730769231, 0.03084615384, 0.03007692308, 0.04661538462, 0.06419230766, 0.03419230770, 0.02632692308, 0.03842307693, 0.04165384614, 0.03611538461, 0.03623076922, 0.03655769233, 0.03259615385, 0.04275000000, 0.04423076922, 0.03700000000

```
> max(%)
```

0.06419230766

```
> This occurs in the 15th position.
> corr(vigvec(ocwy,6,3))
```

0.04742307692, 0.03767307693, 0.03628846154, 0.04126923077, 0.03478846153, 0.02851923077, 0.03334615385, 0.04117307691, 0.03261538463, 0.03078846153, 0.04471153843, 0.06082692306, 0.03892307692, 0.03086538463, 0.03974999999, 0.04580769233, 0.03323076924, 0.03349999999, 0.04061538460, 0.03194230768, 0.02707692308, 0.04438461537, 0.04815384616, 0.03709615386, 0.03567307693, 0.04455769231

```
> max(%)
```

0.06082692306

```
> This occurs in the 12th position.
> corr(vigvec(ocwy,6,4))
```

0.04613461538, 0.04050000000, 0.03875000000, 0.03136538462, 0.03926923078, 0.03428846153, 0.03411538462, 0.02911538462, 0.04782692310, 0.03913461539, 0.03557692310, 0.03480769231, 0.06088461538, 0.04378846153, 0.02917307694, 0.03471153847, 0.04388461540, 0.02826923077, 0.03146153847, 0.04261538460, 0.03515384615, 0.03138461538, 0.04092307692, 0.04478846153, 0.04105769231, 0.04201923077

```
> max(%)
```

0.06088461538

```
> The max is in the 13th position.
> corr(vigvec(ocwy,6,5))
```

0.05063461539, 0.03644230769, 0.03200000000, 0.03526923078, 0.06023076924, 0.03888461539, 0.03280769234, 0.03767307693, 0.04511538463, 0.02653846153, 0.03557692309, 0.04446153845, 0.03605769231, 0.03611538462, 0.03836538462, 0.04461538460, 0.03601923077, 0.04173076923, 0.03807692308, 0.04326923076, 0.03940384617, 0.03640384616, 0.03663461540, 0.03375000001, 0.03538461539, 0.02953846155

```
> max(%)
```


Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual

0.06023076924

```
> This is in the 5th position.
> corr(vigvec(ocwy,6,6))
```

0.03125000000, 0.03286538462, 0.05228846153, 0.04723076924, 0.02580769230, 0.03286538461, 0.04905769229, 0.03924999998, 0.03101923078, 0.03248076923, 0.03978846156, 0.03011538460, 0.03840384616, 0.03576923075, 0.04038461539, 0.03948076925, 0.03482692308, 0.03721153846, 0.06369230769, 0.03859615385, 0.02744230769, 0.03482692308, 0.04853846154, 0.02938461540, 0.04171153847, 0.04671153845

```
> max(%)
```

0.06369230769

```
> This is in the 19th position.
> Since the 1st position corresponds to a shift of 0, etc, we find
that
> the shifts were by 7, 14, 11, 12, 4, 18.  The key word was "holmes".
> Decrypt:
> vigenere(ocwy,-[7,14,11,12,4,18])
```

"holmeshadbeenseatedforsomehoursinsilencewithhislongthinbackcurvedoverache \
micalvesselinwhichhewasbrewingaparticularlymalodorousproducthishead \
wassunkuponhisbreastandhelookedfrommypointofviewlikeastrangelankbir \
dwithdullgreyplumageandablacktopknotsowatsonsaidhesuddenlyyoudonot \
proposetoinvestinsouthafricansecurities"

Copyright © 2021 Pearson Education. Inc.

Introduction to Cryptography with Coding Theory 3rd edition Trappe Solutions Manual