1 Exercises

1. Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the ciphertext *EVIRE*. However, Antony does not know the key, so he tries all possibilities. Where will he meet Caesar? (*Hint:* This is a trick question.)

2. The ciphertext UCR was encrypted using the affine function $9x + 2$ mod 26. Find the plaintext.

3. Encrypt *howareyou* using the affine function $5x + 7$ (mod 26). What is the decryption function? Check that it works.

4. Consider an affine cipher (mod 26). You do a chosen plaintext attack using *hahaha*. The ciphertext is *NONONO*. Determine the encryption function.

5. The following ciphertext was encrypted by an affine cipher mod 26:

CRWWZ.

The plaintext starts *ha*. Decrypt the message.

6. Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod 26). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?

7. Suppose we work mod 27 instead of mod 26 for affine ciphers. How many keys are possible? What if we work mod 29?

8. Suppose that you want to encrypt a message using an affine cipher. You let $a = 0$, $b = 1$, $\ldots$, $z = 25$, but you also include $? = 26$, $; = 27$, $" = 28$, $! = 29$. Therefore, you use $x \mapsto \alpha x + \beta$ (mod 30) for your encryption function, for some integers α and β.

- **(a)** Show that there are exactly eight possible choices for the integer α (that is, there are only eight choices of α (with $0 < \alpha < 30$) that allow you to decrypt).
- **(b)** Suppose you try to use $\alpha = 10$, $\beta = 0$. Find two plaintext letters that encrypt to the same ciphertext letter.

9. You want to carry out an affine encryption using the function $\alpha x + \beta$, but you have $\gcd(\alpha, 26) = d > 1$. Show that if $x_1 = x_2 + (26/d)$, then $\alpha x_1 + \beta \equiv \alpha x_2 + \beta \pmod{26}$. This shows that you will not be able to decrypt uniquely in this case.

10. Suppose there is a language that has only the letters a and b. The frequency of the letter a is .1 and the frequency of b is .9. A message is encrypted using a Vigenère cipher (working mod 2 instead of mod 26). The ciphertext is BABABAAABA.

(a) Show that the key length is probably 2.

(b) Using the information on the frequencies of the letters, determine the key and decrypt the message.

11. Suppose you have a language with only the 3 letters *a, b, c*, and they occur with frequencies .7, .2, .1, respectively. The following ciphertext was encrypted by the Vigenère method (shifts are mod 3 instead of mod 26, of course):

ABCBABBBAC.

Suppose you are told that the key length is 1, 2, or 3. Show that the key length is probably 2, and determine the most probable key.

12. If $\mathbf{v}$ and $\mathbf{w}$ are two vectors in n-dimensional space, $\mathbf{v} \cdot \mathbf{w} = |\mathbf{v}||\mathbf{w}| \cos\theta$, where θ is the angle between the two vectors (measured in the two-dimensional plane spanned by the two vectors), and $|\mathbf{v}|$ denotes the length of $\mathbf{v}$. Use this fact to show that, in the notation of Section 2.3, the dot product $\mathbf{A}_0 \cdot \mathbf{A}_i$ is largest when $i = 0$.

13. The ciphertext *YIFZMA* was encrypted by a Hill cipher with matrix $\begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix}$. Find the plaintext.

14. The ciphertext text *GEZXDS* was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is *solved*. Find the encryption matrix M.

15. Eve captures Bob's Hill cipher machine, which uses a 2-by-2 matrix M mod 26. She tries a chosen plaintext attack. She finds that the plaintext *ba* encrypts to *HC* and the plaintext *zz* encrypts to *GT*. What is the matrix M.

16. **(a)** The ciphertext text *ELNI* was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is *dont*. Find the encryption matrix.

(b) Suppose the ciphertext is *ELNK* and the plaintext is still *dont*. Find the encryption matrix. Note that the second column of the matrix is changed. This shows that the entire second column of the encryption matrix is involved in obtaining the last character of the ciphertext (see the end of Section 2.7).

17. Suppose the matrix $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is used for an encryption matrix in a Hill cipher. Find two plaintexts that encrypt to the same ciphertext.

18. Let a, b, c, d, e, f be integers mod 26. Consider the following combination of the Hill and affine ciphers: Represent a block of plaintext as a pair (x, y) mod 26. The corresponding ciphertext (u, v) is

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \end{pmatrix} \equiv \begin{pmatrix} u & v \end{pmatrix} \pmod{26}.$$

Describe how to carry out a chosen plaintext attack on this system (with the goal of finding the key a, b, c, d, e, f). You should state explicitly what plaintexts you choose and how to recover the key.

19. A sequence generated by a length three recurrence starts 001110. Find the next four elements of the sequence.

20. Consider the sequence starting $k_1 = 1, k_2 = 0, k_3 = 1$ and defined by the length three recurrence $k_{n+3} = k_n + k_{n+1} + k_{n+2}$. This sequence can also be given by a length two recurrence. Determine this length two recurrence by setting up and solving the appropriate matrix equations.

21. Suppose we build an LFSR machine that works mod 3 instead of mod 2. It uses a recurrence of length 2 of the form

$$x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} \pmod{3}$$

to generate the sequence 1, 1, 0, 2, 2, 0, 1, 1. Set up and solve the matrix equation to find the coefficients c_0 and c_1.

22. Suppose you modify the LFSR method to work mod 5 and you use a (not quite linear) recurrence relation

$$x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} + 2 \pmod{5},$$

$$x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0.$$

Find the coefficients c_0 and c_1.

23. In the mid-1980s, a recruiting advertisement for NSA had 1 followed by one hundred 0s at the top. The text began “You’re looking at a ‘googol.’ Ten raised to the 100th power. One followed by 100 zeroes. Counting 24 hours a day, you would need 120 years to reach a googol. Two lifetimes. It’s a number that’s impossible to grasp. A number beyond our imagination.” How many numbers would you have to count each second in order to reach a googol in 120 years? (This problem is not related to the cryptosystems in this chapter. It is included to show how big 100-digit numbers are from a computational viewpoint. Regarding the ad, one guess is that the advertising firm assumed that the time it took to factor a 100-digit number back then was the same as the time it took to count to a googol.)

24. Alice is sending a message to Bob using one of the following cryptosystems. In fact, Alice is bored and her plaintext consists of the letter a repeated a few hundred times. Eve knows what system is being used, but not the key, and intercepts the ciphertext. For systems (a), (b), and (c), state how Eve will recognize that the plaintext is one repeated letter and decide whether or not Eve can deduce the letter and the key. (*Note:* For system (c), the solution very much depends on the fact that the repeated letter is a, rather than $b, c, \ldots$.)

(a) Shift cipher

(b) Affine cipher

(c) Hill cipher (with a 2×2 matrix)

25. The operator of a Vigenère encryption machine is bored and encrypts a plaintext consisting of the same letter of the alphabet repeated several hundred times. The key is a six-letter English word. Eve knows that the key is a word but does not yet know its length.

(a) What property of the ciphertext will make Eve suspect that the plaintext is one repeated letter and will allow her to guess that the key length is six?

(b) Once Eve recognizes that the plaintext is one repeated letter, how can she determine the key? (*Hint:* You need the fact that no English word of length six is a shift of another English word.)

(c) Suppose Eve doesn't notice the property needed in part (a), and therefore uses the method of displacing then counting matches for finding the length of the key. What will the number of matches be for the various displacements? In other words, why will the length of the key become very obvious by this method?

2 Computer Problems

1. The following ciphertext was encrypted by a shift cipher:

```
ycvejqwvhqtdtwvwu
```

Decrypt. (The ciphertext is stored in the downloadable computer files (see the Appendices) under the name *ycve*.)

2. The following ciphertext was the output of a shift cipher:

```
lcllewljazlnnzmvyiylhrmhza
```

By performing a frequency count, guess the key used in the cipher. Use the computer to test your hypothesis. What is the decrypted plaintext? (The ciphertext is stored in the downloadable computer files (see the Appendices) under the name *lcll*.)

3. The following ciphertext was encrypted by an affine cipher:

```
edsgickxhuklzveqzvkxwkzukcvuh
```

The first two letters of the plaintext are *if*. Decrypt. (The ciphertext is stored in the downloadable computer files (see the Appendices) under the name *edsg*.)

4. The following ciphertext was encrypted by an affine cipher using the function $3x + b$ for some b:

```
tcabtiqmfheqqmrmvmtmaq
```

Decrypt. (The ciphertext is stored in the downloadable computer files (see the Appendices) under the name *tcab*.)

5. Experiment with the affine cipher $y \equiv mx + n \pmod{26}$ for values of $m > 26$. In particular, determine whether or not these encryptions are the same as ones obtained with $m < 26$.

6. In this problem you are to get your hands dirty doing some programming. Write some code that creates a new alphabet $\{A, C, G, T\}$. For example, this alphabet could correspond to the four nucleotides adenine, cytosine, guanine, and thymine, which are the basic building blocks of DNA and RNA codes. Associate the letters A, C, G, T with the numbers $0, 1, 2, 3$, respectively.

- **(a)** Using the shift cipher with a shift of 1, encrypt the following sequence of nucleotides which is taken from the beginning of the thirteenth human chromosome:

  $GAATTCGCGGCCGCAATTAACCCTCACTAAAGGGATCT$
  $CTAGAACT.$

- **(b)** Write a program that performs affine ciphers on the nucleotide alphabet. What restrictions are there on the affine cipher?

7. The following was encrypted using by the Vigenère method using a key of length at most 6. Decrypt it and decide what is unusual about the plaintext. How did this affect the results?

```
hdsfgvmkoowafweetcmfthskucaqbilgjofmaqlgspvatvxqbiryscpcfr
mvswrvnqlszdmgaoqsakmlupsqforvtwvdfcjzvgsoaoqsacjkbrsevbel
vbksarlscdcaarmnvrysywxqgvellcyluwwveoafgclazowafojdlhssfi
ksepsoywxafowlbfcsocylngqsyzxgjbmlvgrggokgfgmhlmejabsjvgml
nrvqzcrggcrghgeupcyfgtydycjkhqluhgxgzovqswpdvbwsffsenbxapa
sgazmyuhgsfhmftayjxmwznrsofrsoaopgauaaarmftqsmahvqecev
```

(The ciphertext is stored in the downloadable computer files (see the Appendices) under the name *hdsf*. The plaintext is from *Gadsby* by Ernest Vincent Wright.)

8. The following was encrypted by the Vigenère method. Find the plaintext.

```
ocwyikoooniwugpmxwktzdwgtssayjzwyemdlbnqaaavsuwdvbrflauplo
oubfgqhgcscmgzlatoedcsdeidpbhtmuovpiekifpimfnoamvlpqfxejsm
xmpgkccaykwfzpyuavtelwhrhmwkbbvgtguvtefjlodfefkvpxsgrsorvg
tajbsauhzrzalkwuowhgedefnswmrciwcpaaavogpdnfpktdbalsisurln
```

```
psjyeatcuceesohhdarkhwotikbroqrdfmzghgucebvgwcdqxgpbgqwlpb
daylooqdmuhbdqgmyweuik
```

(The ciphertext is stored in the downloadable computer files (see the Appendices) under the name *ocwy*. The plaintext is from *The Adventure of the Dancing Men* by Sir Arthur Conan Doyle.)

9. The following was encrypted by the Vigenère method. Decrypt it. (The ciphertext is stored in the downloadable computer files (see the Appendices) under the name *xkju*.)

```
xkjurowmllpxwznpimbvbqjcnowxpcchhvvfvsllfvxhazityxohulxqoj
axelxzxmyjaqfstsrulhhucdskbxknjqidallpqslluhiaqfpbpcidsvci
hwhwewthbtxrljnrsncihuvffuxvoukjljswmaqfvjwjsdyljogjxdboxa
jultucpzmpliwmlubzxvoodybafdskxgqfadshxnxehsaruojaqfpfkndh
saafvulluwtaqfrupwjrszxgpfutjqiynrxnyntwmhcukjfbirzsmehhsj
shyonddzzntzmplilrwnmwmlvuryonthuhabwnvw
```

10. The following is the ciphertext of a Hill cipher

```
zirkzwopjjoptfapuhfhadrq
```

using the matrix

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 11 & 2 & 4 & 6 \\ 2 & 9 & 6 & 4 \end{pmatrix}.$$

Decrypt.

11. The following sequence was generated by a linear feedback shift register. Determine the recurrence that generated it.

```
1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0,
0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0,
0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1,
1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0,
1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1,
1, 1, 1, 1, 1
```

(It is stored in the downloadable computer files (see the Appendices) under the name *L101*.)

12. The following are the first 100 terms of an LFSR output. Find the coefficients of the recurrence.

```
1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0,
0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1,
1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0,
1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1,
0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0,
1, 0, 0, 0, 0
```

(The sequence is stored in the downloadable computer files (see the Appendices) under the name *L100*.)

13. The following ciphertext was obtained by XORing an LFSR output with the plaintext.
`0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0,`
`1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0,`
`1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1`
Suppose you know the plaintext starts
`1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0`
Find the plaintext. (The ciphertext is stored in the downloadable computer files (see the Appendices) under the name *L011*.)