sends d to e (namely, A sends d to x and then D sends x to v). The unknown x has been eliminated. Similarly, the second intercepted text tells us that AD sends v to p, and the third tells us that AD sends p to f. We have therefore determined that

\[ AD = (dvpf) \] 

In the same way, the second and fifth letters of the three messages tell us that

\[ BE = (oumb) \] 

and the third and sixth letters tell us that

\[ CF = (enpy) \] 

With enough data, we can deduce the decompositions of AD, BE, and CF into products of cycles. For example, we might have

\[ AD = (dvpf/kxgzpe/cejmgunhlu/bc)(rw)(ea)(e) \]
\[ BE = (kt/ffouemv/h/jjwuvlvrj/tx)(eqy)/(d/lk) \]
\[ CF = (aboiktj/pflnypj/j/dz/ehizp/arn) \]

This information depends only on the daily settings of the plugboard and the rotors, not on the message key. Therefore, it relates to every machine used on a given day.

Let's look at the effect of the plugboard. It introduces a permutation \( S \) at the beginning of the process and then adds the inverse permutation \( S^{-1} \) at the end. We need another fact about permutations: Suppose we take a permutation \( P \) and another permutation of the form \( SPS^{-1} \) for some permutation \( S \) (where \( S^{-1} \) denotes the inverse permutation of \( S \); in our case, \( S = S^{-1} \)) and decompose each into cycles. They will usually not have the same cycles, but the lengths of the cycles in the decompositions will be the same. For example, \( AD \) has cycles of length 10, 10, 2, 2, 1, 1. If we decompose \( SADS^{-1} \) into cycles for any permutation \( S \), we will again get cycles of lengths 10, 10, 2, 2, 1, 1. Therefore, if the plugboard settings are changed, but the initial positions of the rotors remain the same, then the cycle lengths remain unchanged.

You might have noticed that in the decomposition of \( AD, BE, \) and \( CF \) into cycles, each cycle length appears on even number of times. This is a general phenomenon. For an explanation, see Appendix E of the aforementioned book by Kozaczuk.

Rejewski and his colleagues compiled a catalog of all 105,456 initial settings of the rotors along with the set of cycle lengths for the corresponding three permutations \( AD, BE, CF \). In this way, they could take the ciphertexts for a given day, deduce the cycle lengths, and find the small number of corresponding initial settings for the rotors. Each of these substitutions could be tried individually. The effect of the plugboard (when the correct setting was used) was then merely a substitution cipher, which was easily broken. This method worked until September 1938, when a modified method of transmitting message keys was adopted. Modifications of the above technique were again used to encrypt the messages. The process was also mechanized, using machines called "bombes" to find daily keys, each in around two hours. These techniques were extended by the British at Bletchley Park during World War II and included building more sophisticated "bombes." These machines, designed by Alan Turing, are often considered to have been the first electronic computers.

### 2.13 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 homogram 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 hubba. The ciphertext is NONO. Determine the encryption function.

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

   The plaintext starts with. 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 \( T = 26, :, = 27, ! = 29 \). Therefore, you use \( x \rightarrow ax + b \pmod{29} \) for your encryption function, for some integers \( a \) and \( b \).

(a) Show that there are exactly eight possible choices for the integer \( a \) (that is, there are only eight choices of \( a \) (with \( 0 < a < 26 \)) that allow you to decrypt).

(b) Suppose you try to use \( a = 10, b = 0 \). Find two plaintext letters that encrypt to the same ciphertext letter.

9. You want to carry out an affine encryption using the function \( ax + b \), but you have gcd\((a, 26) = d > 1 \). Show that if \( x_1 = x_2 + (26/d) \), then \( ax_1 + b \equiv ax_2 + b \pmod{26} \). 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 BABAABABB.

(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): ABCBBABBAC.

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

12. If \( v \) and \( w \) are two vectors in \( n \)-dimensional space, \( v \cdot w = |v||w| \cos \theta \), where \( \theta \) is the angle between the two vectors (measured in the two-dimensional plane spanned by the two vectors), and \( |v| \) denotes the length of \( v \). Use this fact to show that, in the notation of Section 2.3, the dot product \( A_0 A_1 \) 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 \( 2 \times 2 \) matrix. The plaintext is solved. Find the encryption matrix \( M \).

2.13 Exercises

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 be encrypted to HC and the plaintext 2z encrypts to GT. What is the matrix \( M \)?

16. (a) The ciphertext text ELNI was encrypted by a Hill cipher with a \( 2 \times 2 \) matrix. The plaintext is don't. Find the encryption matrix.

(b) Suppose the ciphertext is ELNK and the plaintext is still don't. 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

\[
\begin{pmatrix} x \\ y \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} u \\ v \end{pmatrix} \pmod{26}
\]

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 000110. 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 \( k_{n+2} = k_n + k_{n+1} + k_{n+3} \). 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

\[
x_{n+2} \equiv q_0 x_n + q_1 x_{n+1} \pmod{3}
\]

to generate the sequence 1, 1, 0, 2, 0, 0, 1, 1. Set up and solve the matrix equation to find the coefficients \( q_0 \) and \( q_1 \).
22. Suppose you modify the LFSR method to work mod 5 and you use a (not quite linear) recurrence relation

\[ x_{n+2} = c_0 x_n + c_1 x_{n+1} + 2 \pmod{5}, \]

\[ x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0. \]

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 \( b, c \).)

(a) Shift cipher
(b) Affine cipher
(c) Hill cipher (with a \( 2 \times 2 \) matrix)

25. The operator of a Vigenère encryption machine is bored and encrypts a plaintext consisting of the same letter of the alphabet 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?