CHAPTER 3

Traditional Symmetric-Key Ciphers

(Solution to Odd-Numbered Problems)

Review Questions

1. Symmetric-key encipherment uses a single key for both encryption and decryption. In addition, the encryption and decryption algorithms are inverse of each other.

3. Substitution ciphers can be divided into two broad categories: monoalphabetic ciphers and polyalphabetic ciphers. In monoalphabetic substitution, the relationship between a character in the plaintext and the characters in the ciphertext is one-to-one. In polyalphabetic substitution, the relationship between a character in the plaintext and the characters in the ciphertext is one-to-many.

5. A stream cipher is a monoalphabetic cipher if the value of k_i does not depend on the position of the plaintext character in the plaintext stream; otherwise, the cipher is polyalphabetic.

7. The additive ciphers, multiplicative ciphers, affine ciphers, and monoalphabetic substitution cipher are some examples of monoalphabetic ciphers.

9. The rail fence cipher and double transposition cipher are examples of transposition ciphers.

Exercises

11.

a. The number of keys = $n \times (n - 1) / 2 = (100 \times 99) / 2 = 4950$.

b. Only 100 keys are needed: There should be one secret key between the president and each member.

c. Only 100 keys are needed: There should be one secret key between the president and each member to create the session secret key. After the session key is established, the two members can use the one-time session key.

13. Double encryption here does not help. Encryption with k_1 followed by encryption with k_2 is the same as encryption with $k = (k_1 + k_2) \bmod 26$.

$$C = [(P + k_1) \bmod 26) + k_2] \bmod 26 = (P \bmod 26 + k_1 \bmod 26 + k_2) \bmod 26$$
$$C = (P \bmod 26) \bmod 26 + (k_1 \bmod 26) \bmod 26 + k_2 \bmod 26$$
$$C = P \bmod 26 + k_1 \bmod 26 + k_2 \bmod 26 = (P + k_1 + k_2) \bmod 26$$
$$C = (P + k) \bmod 26, \text{ where } k = (k_1 + k_2) \bmod 26$$

15.

a. The size of the key domain is 26 + 10 = 36. The modulus is also 36. Alice needs to use the set $\mathbf{Z}_{36}$.

b. The size of the key domain is 12; the domain is (1, 5, 7, 11, 13, 17, 19, 23, 25, and 29). The modulus is 36. Alice needs to use the set $\mathbf{Z}_{36}$*.

c. The key domain is $36 \times 12 = 432$. The modulus is still 36. However, Alice needs to use $\mathbf{Z}_{36}$ for addition and $\mathbf{Z}_{36}$* for multiplication.

17.

a. Random switching between substitution and transposition is as difficult for Alice and Bob as it is for Eve to discover which method is being used. If Alice and Bod do not have a secure channel to inform each other which method they are using (which is normally the case), they need to toss a coin. Eve can do the same. However, Alice and Bob can use a pattern (for example, three substitutions and two transpositions), but using any pattern is a kind of weakness in secrecy.

b. The same argument used in part *a* can be used here. However, if Eve knows that cipher is a substitution, she can use more tools to find out the which type. For example, if she can easily break the code using brute-force attack on the key, she knows that they are using either additive or multiplicative cipher.

c. The same argument used in part *a* can be used here. However, if Eve knows that the cipher is transposition, she can use the pattern attack to find the size of the section.

19.

a. Single transposition only reorders the characters. If one character is changed in the plaintext, it affects only one character in the ciphertext.

b. Double transposition only reorders the characters. If one character is changed in the plaintext, it affects only one character in the ciphertext.

c. In the Playfair cipher, encryption is two characters at a time. If one character in the plaintext is changed, it normally changes one or two characters in the ciphertext. However, if the changed character is the same as the previous or next character, we need to add one bogus character in the plaintext that may change several characters in the ciphertext.

21.

Cipher	Plaintext	Ciphertext
Additive, key = 20	**This is an exercise**	**NBCMCMUHYRYLWCMY**
Multiplicative, key = 15	**This is an exercise**	**ZBQKQKANIHIVEQKI**
Affine, key = (15, 20)	**This is an exercise**	**TVKEKEUHCBCPYKEC**

23.

Plaintext	Ciphertext
Life is full of surprise	**SMFPBZMYLWHMZYPPKPZI**

25. We add the bogus character, "z" to the end of the plaintext to make the number of characters multiple of 2. The plaintext matrix, the key matrix, and ciphertext matrix are shown below:

$$\underset{\mathbf{C}}{\begin{bmatrix} 8 & 20 \\ 21 & 0 \\ 5 & 18 \\ 11 & 3 \\ 13 & 13 \\ 11 & 3 \\ 22 & 12 \\ 2 & 14 \\ 19 & 10 \\ 6 & 12 \\ 2 & 7 \\ 4 & 25 \end{bmatrix}} = \underset{\mathbf{P}}{\begin{bmatrix} 22 & 4 \\ 11 & 8 \\ 21 & 4 \\ 8 & 13 \\ 0 & 13 \\ 8 & 13 \\ 18 & 4 \\ 2 & 20 \\ 17 & 4 \\ 22 & 14 \\ 17 & 11 \\ 3 & 25 \end{bmatrix}} \times \underset{\mathbf{K}}{\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}}$$

The ciphertext is then "IUVAFSLDNNLDWMCOTKGMCHEZ", in which the last character is a bogus character.

27.

a. Eve is launching a chosen-plaintext attack.

b. The length of the message is 10. Since $10 = 2 \times 5$, The number of columns can be 1, 2, 5 or 10. The first or the last guess is unlikely, so the number of columns is either 2 or 5.

29. We know that "ab" $\rightarrow$ "GL". This means that

$$00 \rightarrow 06 \quad \text{and} \quad 01 \rightarrow 11$$

We can construct two equations from these two pieces of information:

$$00 \times k_1 + k_2 \equiv 06 \pmod{26} \qquad 01 \times k_1 + k_2 \equiv 11 \pmod{26}$$

Solving these two equations give us $k_1 = 5$ and $k_2 = 6$. This means,

$$P = ((C - k_2) \times k_1^{-1}) \bmod 26 = ((C + 20) \times 21) \bmod 26$$

Ciphertext: XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

Plaintext: the best of a fight is making up afterwards

31.

a. Since each entry can be one of the 29 characters, the total number of potential keys are $29^4 = 707{,}281$.

b. Out of these 707,281 keys, only 682,080 of them are usable.

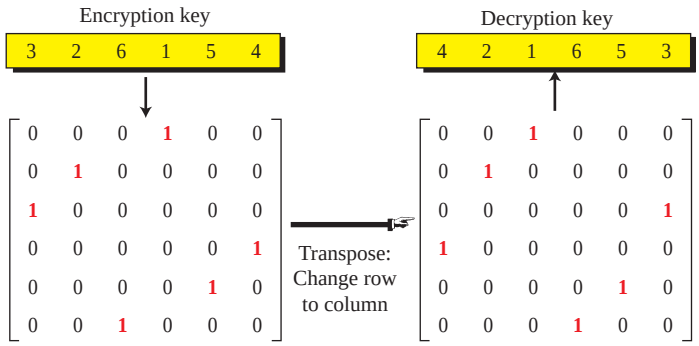
33. This is an example that Kasiski test cannot help us. The reason is that the plaintext has been encrypted line by line. The ciphertext is also created line by line, but each line is too short for Kasiski test. The encryption algorithm uses a 5-character word "*a poet*" to encrypt the text without adding any padding at the end of the last segment.

```
maken oment ionof rough times forge tabou teven tspas t
MPYIG OBSRM IDBSY RDIKA TXAIL FDFKX TPPSN TTJIG THDEL T
timey ettoc omeis unrev ealed andbe ingre veale dwill notla st
TXAIR EIHSV OBSML UCFIO EPZIW ACRFX ICUVX VTOPX DLWPE NDHPT SI
dontd wello ndays ofyou rnorb uildo nhere after
DDBXW WTZPH NSOCL OUMSN RCCVU UXZHH NWSVX AUHIK
lifet otoda yandt histo owill whisk awaya sblas t
LXTIM OICHT YPBHM HXGXH OLWPE WWWWD ALOCT SQZEL T
```

After adding the punctuation, we get another English translation of a poem by Khayyam, the Persian poet, philosopher, and mathematician of the twelve century.

Make no mention of rough times, forget about events past.
Time yet to come is unrevealed, and being revealed will not last,
Don’t dwell on days of your, nor build on here after,
Life to today and this too will whisk away as blast.

35. We follow the idea shown in Figure 3.24 of the text.



37. We can use a row matrix of size *m* for addition matrix, but we need to use a square matrix for multiplication (to be reversible).

a. For the additive cipher we have

$$\underset{C}{[\ 1 \times m\ ]} = \underset{P}{[\ 1 \times m\ ]} + \underset{k}{[\ 1 \times m\ ]}$$

$$\underset{P}{[\ 1 \times m\ ]} = \underset{C}{[\ 1 \times m\ ]} - \underset{k}{[\ 1 \times m\ ]}$$

b. For the affine cipher we have

$$\underset{C}{[\ 1 \times m\ ]} = \underset{P}{[\ 1 \times m\ ]} \times \underset{k_1}{\left[\ m \times m\ \right]} + \underset{k_2}{[\ 1 \times m\ ]}$$

$$\underset{P}{[\ 1 \times m\ ]} = \left(\underset{C}{[\ 1 \times m\ ]} - \underset{k_2}{[\ 1 \times m\ ]}\right) \times \underset{k_1}{\left[\ m \times m\ \right]}^{-1}$$

39. In the Hill cipher, $\mathbf{C} = \mathbf{P} \times \mathbf{K}$. If the plaintext is the identity matrix **I**, then we have $\mathbf{C} = \mathbf{K}$. This means that if can access to the Alice computer and launch a chosen plaintext attack using the trivial identity matrix, Eve can find the key. This shows that the Hill cipher is very vulnerable to the chosen-plaintext attack.

41. We use the following key:

	1	**2**	**3**	**4**	**5**
1	z	q	p	f	e
2	y	r	o	g	d
3	x	s	n	h	c
4	w	t	m	i / j	b
5	v	u	l	k	a

The plaintext and ciphertext are shown below:

Plaintext	Ciphtertext
an exercise	(5, 5), (3, 3), (1, 5), (3, 1), (1, 5), (2, 2), (3, 5), (4, 4), (3, 2), (1, 5)