
CHAPTER 3

Traditional Symmetric-Key Ciphers

(Solution to Practice Set)

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.
2. Traditional symmetric-key ciphers can be divided into two broad categories: substitution ciphers and transposition ciphers. A substitution cipher replaces one character with another character. A transposition cipher reorders the symbols.
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.
4. Symmetric-key ciphers can also be divided into two broad categories: stream ciphers and block ciphers. In a stream cipher, encryption and decryption are done one symbol at a time. In a block cipher, symbols in a block are encrypted together.
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.
6. In a block cipher, each character in a ciphertext block depends on all characters in the corresponding plaintext block. The cipher, therefore, is a polyalphabetic.
7. The additive ciphers, multiplicative ciphers, affine ciphers, and monoalphabetic substitution cipher are some examples of monoalphabetic ciphers.
8. The autokey cipher, Playfair cipher, Vigenere cipher, Hill cipher, rotor cipher, one-time pad, and Enigma machine are some examples of polyalphabetic ciphers.
9. The rail fence cipher and double transposition cipher are examples of transposition ciphers.

10. Brute-force attack, statistical attack, pattern attack, and Kasiski test are examples of attacks on traditional 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.

12. The sentence in the tablet and its translation serves as a known plaintext/ciphertext pair. This is a *known-plaintext* attack.

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

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

14.

- a. The compression in general creates a text which is not in the source language (English for example). This means that the compressed plaintext does not preserve the frequency of characters. It helps Alice in this case.
- b. Compression before encryption can be more efficient because encryption is normally time consuming if the message is very long.

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.

16.

- a. The size of the key domain is 29.
- b. The size of the key domain is 28 because 29 is a prime number.
- c. The size of the key domain is $29 \times 28 = 812$.

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 Bob 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.

18.

- a. In additive cipher, $C_i = (P_i + K) \bmod 26$. This means that if one character in the plaintext is changed only one character in the ciphertext is changed. C_i depends only P_i .
- b. In multiplicative cipher, $C_i = (P_i \times K) \bmod 26$. This means that if one character in the plaintext is changed only one character in the ciphertext is changed. C_i depends only P_i .
- c. In affine cipher, $C_i = (P_i \times k_1 + k_2) \bmod 26$. This means that if one character in the plaintext is changed only the corresponding character in the ciphertext is changed. C_i depends only P_i .
- d. In Vigenere cipher, $C_i = (P_i + K_j) \bmod 26$. Although, the value of K_j may change, but the change does not depend on the previous or next characters; the change depends only on position of the plaintext character. If only one character in the plaintext is changed, only one character in the ciphertext will be changed.
- e. In autokey cipher, $C_i = (P_i + K_i) \bmod 26 = (P_i + P_{i-1}) \bmod 26$. This means each ciphertext character (except the first) depends on the corresponding plaintext character and the previous plaintext character. Therefore, changing one single character in the plaintext will change all characters in the ciphertext which comes after that character. In other words, if we change character 21 in the plaintext, characters 22, 23, 24, ... will be changed.
- f. In one-time pad, the key stream is used only once. Each ciphertext character, however, depends only the corresponding plaintext ciphertext. If only one character in the plaintext is changed, only one character in the ciphertext will be changed.
- g. The rotor cipher is a kind of monoalphabetic substitution cipher, in which the mapping table will be changed from one character to the next. Each ciphertext character, however, depends only the corresponding plaintext character. If only

one character in the ciphertext is changed, only one character in the plaintext will be changed.

- h.** The Enigma machine is based on the rotor cipher. Therefore, If only one character in the plaintext is changed, only one character in the ciphertext will be changed.

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.

20.

- a.** The Playfair is a block cipher; encryption is done two character at a time.
- b.** The autokey cipher is a stream cipher; encryption is done one character at a time.
- c.** The one-time pad cipher is a stream cipher; encryption is done one character at a time.
- d.** The rotor cipher is a stream cipher; encryption is done one character at a time.
- e.** The Enigma machine is a is a stream cipher; encryption is done one character at a time.

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

22.

Cipher	Plaintext	Ciphertext
Vigenere	The house is being sold tonight	WVPSOLKHWDMEZFJGZWDKGQWRST
Autokey	The house is being sold tonight	AALLVIMWMATFMVTYGGZOWHBBVONA
Playfair	The house is being sold tonight	WECEXIOHNOEIFIHKXBBWSIRBEW

23.

Plaintext	Ciphertext
Life is full of surprise	SMFPBZMYLWHMZYPKPZI

24. We use the following key:

G	U	I / J	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

We need to add three bogus character, x's, to separate two d's and two o's and one at the end to make the number of characters even. The transformed plaintext is actually "th ek ey is hi dx de nu nd er th ed ox or pa dx".

Plaintext	Ciphertext
The key is hidden under the door pad	POKLBXDRLGIYIBCGBGLXPOBILZTLGTIY

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:

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

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

- 26.** This is known-plaintext attack. John knows a plaintext/ciphertext pair (yes → CIW). He knows that the algorithm is shift cipher and the key = 4. When he gets access to the ciphertext "XVIEWYVT", he decrypts it as "treasure".

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.

28. We can try the keys 13, 12, 14, 11, 15 which are close to Alice's birthday. When we use the key = 11, the plaintext makes sense.

Key = 11

Ciphertext: NCJAEZRCLASJLYODEPRLYZRCLASJLCPEHZDZTOPDZQLNZTY

Plaintext: cryptography and steganography are two sides of a coin

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:

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

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

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

Ciphertext: XPALASXYFGFUKPXUSOGEUTKCDGFXANMGVNS

Plaintext: the best of a fight is making up afterwards

30. We can find the single-character frequency of letters in this ciphertext as shown below:

Character	O	H	B	G	W	N	V	E	J	C	U	L	R
Frequency	4	4	4	4	3	2	2	2	1	1	1	1	1

This statistic, however, is not very useful because of several reasons:

- The length of the ciphertext is very short for this analysis (only 30 characters).
- Only 10 out of 26 characters in the alphabet is used. When monoalphabetic substitution is used, we need to have all or most of the characters to be present in the ciphertext.
- The frequencies are not distributed. We have only four 4's, one 3, three 2's, and five 1's.

With some more guessing, we can find the mapping as:

O	N	H	O	V	E	J	H	W	O	B	E	V	G	W	O	C	B	W	H	N	U	G	B	L	H	G	B	G	R
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
o	n	e	o	f	t	h	e	m	o	s	t	f	a	m	o	u	s	m	e	n	w	a	s	c	e	a	s	a	r

This gives us the plaintext that makes sense:

Plaintext: One of the most famous men was Ceasar.

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.

32. We can find the single-character frequency of letters in this ciphertext as shown below:

Character	B	Q	M	A	V	L	Z	I	T	W	P
Frequency	18	15	14	12	11	10	10	9	9	9	7
Character	E	G	N	C	O	U	X	J	S	K	D
Frequency	6	6	5	5	4	4	3	2	1	1	1

Although "B" and "Q" have the highest frequencies, if we assume that "B" or "Q" are the decryption of "e", the plaintext does not make sense. We assume that "M" is the decryption of "e". In this case 12 is decrypted as 04 so the key = 8. Using this key the plaintext is

Plaintext:

Glow of youth is tarnished, by rolling time's heavy rust
Winter draped spring, in deep snow and dark frost,
Bird of delight named youth, swiftly left the nest
Alas, couldn't tame it, while it was in my trust.

It is the English translation of a poem by Khayyam, the Persian poet, philosopher, and mathematician of the twelve century.

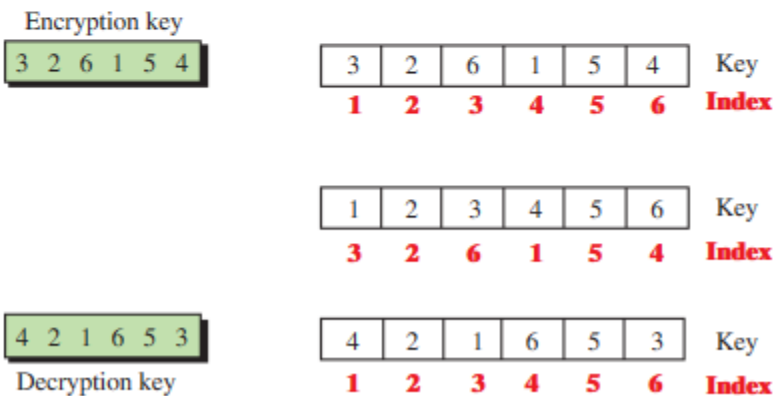
33. This is an example that Kasiski test cannot help us. The reason is that the plaintext has been encrypted line by line. The ciphertext is also created line by line, but each line is too short for Kasiski test. The encryption algorithm uses a 5-character word "a poet" to encrypt the text without adding 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 TDEL T
timey ettoc omeis unrev ealed andbe ingre veale dwill notla st
TXAIR EIHSV OBSML UCFIO EPZIW ACRFX ICUVX VTOPX DLWPE NDHPT SI
dondt 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 OLVPE WWWWD ALOCT SQZEL T
```

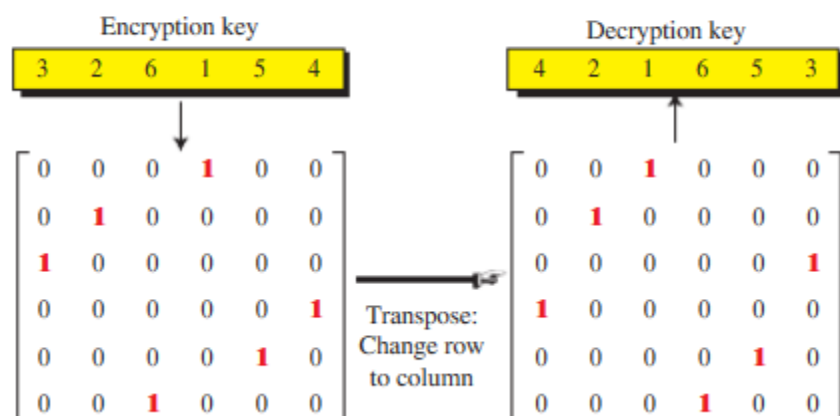
After adding the punctuation, we get another English translation of a poem by Khayyam, the Persian poet, philosopher, and mathematician of the twelve century.

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.

34. We follow the process shown in Figure 3.23 of the text.



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



36. The length of the message is 12. The size of the block needs to divide 12. This means that the size of the block can be 1, 2, 3, 4, 6, 12. Since the first and the last size is trivial, we can ignore them. We need to try the block sizes 2, 3, 4, and 6.

However, the size of message (12) does not allow us to test for the matrices of size 4 or 16. If the size of the key matrix is 4, we need at least the plaintext/ciphertext of size 16. If the size of the key matrix is 6, we need to have a plaintext/ciphertext of size 36. Our only choices are to test for the key matrices of size 2 and 3.

- a.** Let us first try the block size 2. Following Example 3.21 in the text, we can make a plaintext/ciphertext pair of the first four of the given plaintext and given ciphertext (letu $\rightarrow$ HBCD). In this case the plaintext matrix and ciphertext are

$$P = \begin{bmatrix} 11 & 04 \\ 19 & 08 \end{bmatrix} \quad C = \begin{bmatrix} 07 & 01 \\ 02 & 03 \end{bmatrix}$$

Since P is not invertible in modulo 26 arithmetic, we can not proceed.

- b.** Let us now try the block size 3. Following Example 3.21 in the text, we can make a plaintext/ciphertext pair of the first nine character of the given plaintext and given ciphertext (let usm eet $\rightarrow$ HBCDFNOPI). In this case the plaintext and ciphertext matrices are

$$P = \begin{bmatrix} 11 & 04 & 19 \\ 20 & 18 & 12 \\ 04 & 04 & 19 \end{bmatrix} \quad C = \begin{bmatrix} 07 & 01 & 02 \\ 03 & 05 & 13 \\ 14 & 15 & 08 \end{bmatrix}$$

Since P is not invertible in modulo 26 arithmetic, we can not proceed. This means that we cannot solve the problem with the information given.

- 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

$$\begin{array}{c} \begin{bmatrix} 1 \times m \end{bmatrix} \\ C \end{array} = \begin{array}{c} \begin{bmatrix} 1 \times m \end{bmatrix} \\ P \end{array} + \begin{array}{c} \begin{bmatrix} 1 \times m \end{bmatrix} \\ k \end{array}$$

$$\begin{array}{c} \begin{bmatrix} 1 \times m \end{bmatrix} \\ P \end{array} = \begin{array}{c} \begin{bmatrix} 1 \times m \end{bmatrix} \\ C \end{array} - \begin{array}{c} \begin{bmatrix} 1 \times m \end{bmatrix} \\ k \end{array}$$

b. For the affine cipher we have

$$\begin{bmatrix} 1 \times m \\ C \end{bmatrix} = \begin{bmatrix} 1 \times m \\ P \end{bmatrix} \times \begin{bmatrix} m \times m \\ k_1 \end{bmatrix} + \begin{bmatrix} 1 \times m \\ k_2 \end{bmatrix}$$

$$\begin{bmatrix} 1 \times m \\ P \end{bmatrix} = \left(\begin{bmatrix} 1 \times m \\ C \end{bmatrix} - \begin{bmatrix} 1 \times m \\ k_2 \end{bmatrix} \right) \times \begin{bmatrix} m \times m \\ k_1 \end{bmatrix}^{-1}$$

38. The following shows the encryption process. The position and the value of each character in the plaintext (P. Text) is found. The multiplication and addition keys (k_1 and k_2) are listed. The numeric result of encryption for each character is calculated ($P \times k_1 + k_2$), and finally the ciphertext characters (C. Text) are determined and listed.

P. Text	c	r	y	p	t	o	g	r	a	p	h	i	s	f	u	n
Position	0	1	2	3	4	5	6	7	8	9	10	11	0	1	2	3

Values	2	17	24	15	19	14	6	17	0	15	7	8	18	5	20	13
k_1	1	3	5	7	9	11	15	17	19	21	23	25	1	3	5	7
k_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

results	2	0	18	4	19	3	18	10	8	12	15	3	4	2	10	4
C. Text	C	A	S	E	T	D	S	K	I	M	P	D	E	C	K	E

39. In the Hill cipher, $C = P \times K$. If the plaintext is the identity matrix **I**, then we have $C = K$. 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.
40. The relationship between the plaintext and ciphertext is $P + C = 25$ or $C = (25 - P) \text{ mod } 26$.

Plaintext	Ciphertext
<i>an exercise</i>	ZMVCVIXRHV

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	Ciphertext
<i>an exercise</i>	(5, 5), (3, 3), (1, 5), (3, 1), (1, 5), (2, 2), (3, 5), (4, 4), (3, 2), (1, 5)