Problems

1.1. The ciphertext below was encrypted using a substitution cipher. Decrypt the ciphertext without knowledge of the key.

```
  lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk
lmird jk xjubt trmui jx ibndt

  wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi
iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m
vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh
mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd
wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb
```

1. Compute the relative frequency of all letters `A...Z` in the ciphertext. You may want to use a tool such as the open-source program CrypTool [82] for this task. However, a paper and pencil approach is also doable.
2. Decrypt the ciphertext with the help of the relative letter frequency of the English language (see Table 1.1 in Section 1.2.2). Note that the text is relatively short and that the letter frequencies in it might not perfectly align with that of general English language from the table.
3. Who wrote the text?

1.2. We received the following ciphertext which was encoded with a shift cipher:

```
  xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpit
ghlxiwiwtxgqadds.
```

1. Perform an attack against the cipher based on a letter frequency count: How many letters do you have to identify through a frequency count to recover the key? What is the cleartext?
2. Who wrote this message?

1.3. We consider the long-term security of the Advanced Encryption Standard (AES) with a key length of 128 bits with respect to exhaustive key-search attacks. AES is perhaps the most widely used symmetric cipher at this time.

1. Assume that an attacker has special-purpose hardware chips (also known as ASICs, or application-specific integrated circuits) that check $5 \cdot 10^8$ keys per

second, and she has a bu
sume 100% overhead for i
boards, power supply, co
with the given budget? H
time to the age of the Uni
2. We try now to take adva
the future tends to be tri
which states that the comp
of integrated circuits stay
a key-search machine can
search time of 24 hours?
inflation into account).

1.4. We now consider the rel
we consider a cryptosystem

1. Assume a password consi
ASCII code (7 bits per ch
of the key space which ca
2. What is the correspondin
3. Assume that most users u
stead of the full 7 bits o
length in bits in this case?
4. At least how many chara
key length of 128 bits in

a. 7-bit characters?
b. 26 lowercase letters fr

1.5. In case of a brute-force a
To prevent such a search fro
large. It is crucial to observ
length in bits. With this pro
exponential growth.
According to an anecdote, th
in the form of grains of rice
put one grain of rice, on the
grains etc.

1. How many grains of rice
2. A single grain of rice ha
weight of all grains on th
yield of approximately 4

Now, let us consider a piece
paper increases exponentiall
the thickness if folded twice
which is 0.1 mm thick.

ıtion cipher. Decrypt the ci-

```
jeryrkbi jx qmbm wi
riirkvr jx
t bj rhnvwdmbr bpr
 wkbrusurbmbwjk
```

```
mvp yjeryrkb mkd wbi
ashmwkrd bj ower m
j lr fnmhwxwrd mkd
nhd urmvp bpr ibmbr
wgwko ijnkdhrii
ry ytirhx bpr xwkmh
 pmi hrxb kj djnlb
wvmbwjk mkd
 bpr pjsr bpmb bpr
k wkbmvb
```

in the ciphertext. You may
CrypTool [82] for this task.

ter frequency of the English
t the text is relatively short
ly align with that of general

coded with a shift cipher:
`ipxciwtvgtpilpit`

tter frequency count: How
uency count to recover the

anced Encryption Standard
haustive key-search attacks.
at this time.

ware chips (also known as
that check $5 \cdot 10^8$ keys per

second, and she has a budget of \$1 million. One ASIC costs \$50, and we assume 100% overhead for integrating the ASIC (manufacturing the printed circuit boards, power supply, cooling, etc.). How many ASICs can we run in parallel with the given budget? How long does an average key search take? Relate this time to the age of the Universe, which is about 10^{10} years.
2. We try now to take advances in computer technology into account. Predicting the future tends to be tricky but the estimate usually applied is Moore's law, which states that the computing power doubles every 18 months while the costs of integrated circuits stay constant. How many years do we have to wait until a key-search machine can be built to break AES with 128 bits with an average search time of 24 hours? Again, assume a budget of \$1 million (do not take inflation into account).

1.4. We now consider the relation between passwords and key size. For this purpose we consider a cryptosystem where the user enters a key in the form of a password.

1. Assume a password consisting of 8 letters, where each letter is encoded with the ASCII code (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords?
2. What is the corresponding key length in bits?
3. Assume that most users use only the 26 lowercase letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?
4. At least how many characters are required for a password in order to generate a key length of 128 bits in case of letters consisting of

   a. 7-bit characters?
   b. 26 lowercase letters from the alphabet?

1.5. In case of a brute-force attack, we have to search the entire key space of a cipher. To prevent such a search from being successful, the key space must be sufficiently large. It is crucial to observe that the key space grows exponentially with the key length in bits. With this problem we want to get a better understanding of such an exponential growth.
According to an anecdote, the inventor of chess asked the king for a *humble* reward in the form of grains of rice: On the first field of the chess board, the king should put one grain of rice, on the second field two grains of rice, on the third field four grains etc.

1. How many grains of rice are on the last field of the chess board?
2. A single grain of rice has a weight of approximately 0.03 g. What is the total weight of all grains on the board? Compare the total weight with the worldwide yield of approximately 480 million tons per year.

Now, let us consider a piece of paper that is repeatedly folded. The thickness of the paper increases exponentially: It has twice the thickness if folded once, four times the thickness if folded twice etc. For the following tasks, we assume a piece of paper which is 0.1 mm thick.

3. How thick is the paper after 10 folding steps?
4. How often do we need to fold it to obtain a thickness of 1 km?
5. How often do we need to fold it to obtain the distance from the Earth to the Moon (384,400 km)?
6. How often do we need to fold it to obtain the distance of one light year, i.e., $9.46 \cdot 10^{15}$ km?

Remark: Obviously, folding a piece of paper that often will not work out very well in practice.

1.6. In this problem we consider the difference between end-to-end encryption (E2EE) and more classical approaches to encrypting when communicating over a channel that consists of multiple parts. E2EE is widely used, e.g., in instant messaging services such as WhatsApp or Signal. The idea behind this is that encryption and decryption are performed by the two users who communicate and all parties eavesdropping on the communication link cannot read (or meaningfully manipulate) the message.

In the following we assume that each individual encryption with the cipher $e()$ is secure, i.e., the cryptographic algorithm cannot be broken by an adversary. First we look at the communication between two smartphones *without* end-to-end encryption, shown in Figure 1.7. Encryption and/or decryption happen three times in this setting: Between Alice and base station A (air link), between base stations A and B (through the internet), and between base station B and Bob (again, air link).

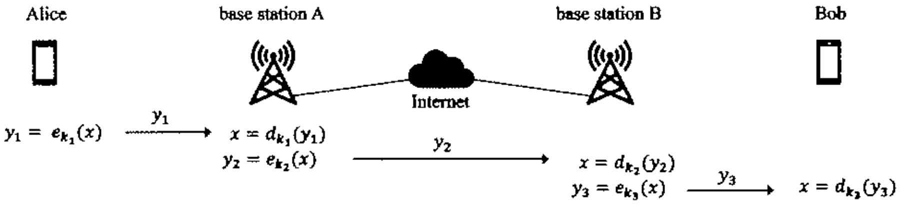


Fig. 1.7 Communication *without* E2EE

1. Describe which of the following attackers can read (and meaningfully manipulate) messages.
   a. A hacker who can listen to (and alter) messages on the air link between Alice and her base station.
   b. The mobile operator who runs and controls base station A.
   c. A national law enforcement agency that has power over the mobile operator and gains access to base station A or B.
   d. An intelligence agency of a foreign country that can wiretap any internet communication.
   e. The mobile operator who runs and controls base station B.

f. A hacker who can list
and his base station.

We now look at the same c
E2EE, cf. Figure 1.8

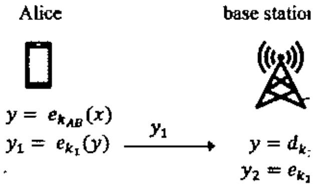


Fig.

2. Describe which of the fo
late) messages in the com
   a. A hacker who can list
   and her base station.
   b. The mobile operator v
   c. A national law enforc
   and gains access to ba
   d. An intelligence agency
   munication.
   e. The mobile operator v
   f. A hacker who can list
   and his base station.

1.7. As we learned in this
tosystems. We will now pro
modular computations.

Let's start with an easy o

1. $15 \cdot 29 \bmod 13$
2. $2 \cdot 29 \bmod 13$
3. $2 \cdot 3 \bmod 13$
4. $-11 \cdot 3 \bmod 13$

The results should be given
the relation between the dif

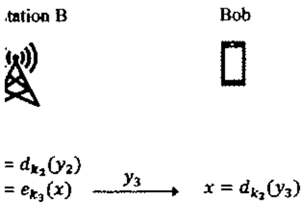
of 1 km?
from the Earth to the Moon

ınce of one light year, i.e.,

will not work out very well

een end-to-end encryption
hen communicating over a
sed, e.g., in instant messag-
d this is that encryption and
nicate and all parties eaves-
eaningfully manipulate) the

yption with the cipher $e()$ is
en by an adversary. First we
without end-to-end encryp-
ı happen three times in this
ween base stations A and B
Bob (again, air link).



E2EE

(and meaningfully manipu-

n the air link between Alice

tation A.
er over the mobile operator

n wiretap any internet com-

tation B.

f. A hacker who can listen to (and alter) messages on the air link between Bob and his base station.

We now look at the same communication system but this time Alice and Bob use E2EE, cf. Figure 1.8

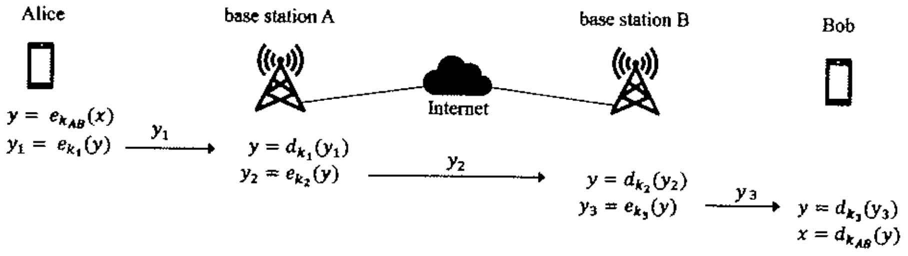


Fig. 1.8 Communication with E2EE

2. Describe which of the following attackers can read (and meaningfully manipulate) messages in the communication systems with E2EE.
   a. A hacker who can listen to (and alter) messages on the air link between Alice and her base station.
   b. The mobile operator who runs and controls base station A.
   c. A national law enforcement agency that has power over the mobile operator and gains access to base station A or B.
   d. An intelligence agency of a foreign country that can wiretap any internet communication.
   e. The mobile operator who runs and controls base station B.
   f. A hacker who can listen to (and alter) messages on the air link between Bob and his base station.

1.7. As we learned in this chapter, modular arithmetic is the basis of many cryptosystems. We will now provide a number of exercises that help us get familiar with modular computations.

Let's start with an easy one: Compute the following result without a calculator.

1. $15 \cdot 29 \bmod 13$
2. $2 \cdot 29 \bmod 13$
3. $2 \cdot 3 \bmod 13$
4. $-11 \cdot 3 \bmod 13$

The results should be given in the range from $0, 1, \ldots,$ modulus-1. Briefly describe the relation between the different parts of the problem.

1.8. Compute without a calculator:

1. $1/5 \bmod 13$
2. $1/5 \bmod 7$
3. $3 \cdot 2/5 \bmod 7$

1.9. We consider the ring $\mathbb{Z}_4$. Construct a table that describes the addition of all elements in the ring with each other in the following form:

+	0	1	2	3
0	0	1	2	3
1	1	2 ···		
2	···			
3				

1. Construct the multiplication table for $\mathbb{Z}_4$.
2. Construct the addition and multiplication tables for $\mathbb{Z}_5$.
3. Construct the addition and multiplication tables for $\mathbb{Z}_6$.
4. There are elements in $\mathbb{Z}_4$ and $\mathbb{Z}_6$ without a multiplicative inverse. Which elements are these? Why does a multiplicative inverse exist for all nonzero elements in $\mathbb{Z}_5$?

1.10. What is the multiplicative inverse of 5 in $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$, and $\mathbb{Z}_{13}$? You can do a trial-and-error search using a calculator or a PC.

With this simple problem we want now to stress the fact that the inverse of an integer in a given ring depends completely on the ring considered. That is, if the modulus changes, the inverse changes. Hence, it doesn't make sense to talk about an inverse of an element unless it is clear what the modulus is. This fact is crucial for the RSA cryptosystem, which is introduced in Chapter 7. The extended Euclidean algorithm, which can be used for computing inverses efficiently, is introduced in Section 6.3.

1.11. Compute x as far as possible without a calculator. Where appropriate, make use of a smart decomposition of the exponent as shown in the example in Section 1.4.1:

1. $x \equiv 3^2 \bmod 13$
2. $x \equiv 7^2 \bmod 13$
3. $x \equiv 3^{10} \bmod 13$
4. $x \equiv 7^{100} \bmod 13$
5. $7^x \equiv 11 \bmod 13$

The last problem is called a *discrete logarithm* and points to a hard problem which we discuss in Chapter 8. The security of many public-key schemes is based on the hardness of solving the discrete logarithm for large numbers, e.g., with more than 2000 bits.

1.12. Find all integers n wi
4, 5, 9, 26. We denote the *nu*
e.g., $\phi(3) = 2$. This functic
$m = 4, 5, 9, 26$?
More on Euler's phi func

1.13. This problem deals wi
$b = 22$.

1. Decrypt the text below:
`falszztysyjzyjkyw`
2. Who wrote the line?

1.14. We want to extend the
crypt and decrypt messages
alphabet consists of the Eng
the (even stranger) "sharp S'
to integers:

A ↔ 0	B ↔ 1
G ↔ 6	H ↔ 7
M ↔ 12	N ↔ 13
S ↔ 18	T ↔ 19
Y ↔ 24	Z ↔ 25

1. What are the encryption
2. How large is the key spa
3. The following ciphertext
the corresponding plainte

ä u ß w ß

4. From which village does

1.15. We consider an attack
Alice with a few pieces of pl
affine cipher by using two
is the condition for choosin
Remark: In practice, thi
the application, e.g., if Alic
are sent to her.

1.16. An obvious approach
apply the same cipher twice

As is often the case in cryp
ferent from the expected o

:scribes the addition of all
m:

'5.
'6.
icative inverse. Which ele-
:ist for all nonzero elements

12, and $\mathbb{Z}_{13}$? You can do a

: fact that the inverse of an
; considered. That is, if the
't make sense to talk about
lus is. This fact is crucial for
7. The extended Euclidean
efficiently, is introduced in

r. Where appropriate, make
wn in the example in Sec-

nts to a hard problem which
key schemes is based on the
mbers, e.g., with more than

1.12. Find all integers n with $0 \leq n < m$ that are relatively prime to m for $m = 4, 5, 9, 26$. We denote the *number* of integers n which fulfill the condition by $\phi(m)$, e.g., $\phi(3) = 2$. This function is called "Euler's phi function". What is $\phi(m)$ for $m = 4, 5, 9, 26$?

More on Euler's phi function will be said in Section 6.3.

1.13. This problem deals with the affine cipher where the key is given as $a = 7$ and $b = 22$.

1. Decrypt the text below:
   `falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj`
2. Who wrote the line?

1.14. We want to extend the affine cipher from Section 1.4.4 such that we can encrypt and decrypt messages written with the full German alphabet. The German alphabet consists of the English one together with the three umlauts, Ä, Ö, Ü, and the (even stranger) "sharp S" character ß. We use the following mapping from letters to integers:

A ↔ 0	B ↔ 1	C ↔ 2	D ↔ 3	E ↔ 4	F ↔ 5
G ↔ 6	H ↔ 7	I ↔ 8	J ↔ 9	K ↔ 10	L ↔ 11
M ↔ 12	N ↔ 13	O ↔ 14	P ↔ 15	Q ↔ 16	R ↔ 17
S ↔ 18	T ↔ 19	U ↔ 20	V ↔ 21	W ↔ 22	X ↔ 23
Y ↔ 24	Z ↔ 25	Ä ↔ 26	Ö ↔ 27	Ü ↔ 28	ß ↔ 29

1. What are the encryption and decryption equations for the cipher?
2. How large is the key space of the affine cipher for this alphabet?
3. The following ciphertext was encrypted using the key $(a = 17, b = 1)$. What is the corresponding plaintext?

   ä u ß w ß

4. From which village does the plaintext come?

1.15. We consider an attack scenario where the adversary Oscar manages to provide Alice with a few pieces of plaintext that she encrypts. Show how Oscar can break the affine cipher by using two pairs of plaintext–ciphertext, (x_1, y_1) and (x_2, y_2). What is the condition for choosing x_1 and x_2?

Remark: In practice, this chosen-plaintext attack is often possible depending on the application, e.g., if Alice is a web server that encrypts and returns messages that are sent to her.

1.16. An obvious approach to increase the security of a symmetric algorithm is to apply the same cipher twice, i.e.,

$$y = e_{k2}(e_{k1}(x))$$

As is often the case in cryptography, things can be tricky and results are often different from the expected or desired ones. In this problem we show that a double encryption with the affine cipher is only as secure as single encryption! Assume two affine ciphers $e_{k1} \equiv a_1 x + b_1 \bmod 26$ and $e_{k2} \equiv a_2 x + b_2 \bmod 26$.

1. Show that there is a single affine cipher $e_{k3} \equiv a_3 x + b_3 \bmod 26$ which performs exactly the same encryption (and decryption) as the combination $e_{k2}(e_{k1}(x))$.
2. Find the values for a_3, b_3 when $a_1 = 3, b_1 = 5$ and $a_2 = 11, b_2 = 7$.
3. To verify your solution, (1) encrypt the letter K with e_{k1} and the result with e_{k2}, and (2) encrypt the letter K with e_{k3}.
4. Briefly describe what happens if an exhaustive key-search attack is applied to a double-encrypted affine ciphertext. Is the effective key space increased?

Remark: The issue of multiple encryption is of great practical importance in the case of the Data Encryption Standard (DES), for which multiple encryption (in particular, triple encryption) does increase security considerably, cf. Section 5.3.2.

1.17. We already know that the substitution cipher and the shift cipher can easily be broken in little time. Let us now consider an extension of the shift cipher, namely the *Vigenère cipher* (named after *Blaise de Vigenère*). Instead of using a single key k for the shift, it uses l different shifts that are derived from a secret code word c. The code word consists of l letters and has the form $c = (c_0, c_1, \ldots, c_{l-1})$. Each letter c_i corresponds to a number $0, \ldots, 25$, which is given by its position in the alphabet. These numbers are the l shift positions, which we denote by $(k_0, k_1, \ldots k_{l-1})$.

Encryption (and decryption) work as follows: The first plaintext letter x_0 is cyclically shifted by k_0 positions, the second plaintext x_1 by k_1 positions and so on, until plaintext letter x_{l-1} is shifted by k_{l-1} positions. From now on, the shift sequence repeats, i.e., plaintext x_l is again shifted by k_0 positions, the next plaintext by k_1 positions and so on. This process is expressed as:

$$y_j \equiv x_j + k_{(j \bmod l)} \bmod 26$$

where x_j denotes the j-th letter of the plaintext $x = (x_0, x_1, \ldots)$.

Since the cipher uses many ciphertext alphabets, it is called a *polyalphabetic cipher*.

1. Assume the code word is given as $c =$ JAMAIKA of size $l = 7$. Transform the code word into the corresponding encryption keys k_i. You can use Table 1.4 for this task.
2. Use the table to encrypt the word $x =$ CODEBREAKERS with the Vigenère cipher. For each plaintext letter, choose the row with the corresponding shift value in the leftmost column # and look up the shifted version of the plaintext.
3. What do you think about the security of the Vigenère cipher? Propose an attack.

#	A	B	C	D	E	F	G	H
0	A	B	C	D	E	F	G	H
1	B	C	D	E	F	G	H	I
2	C	D	E	F	G	H	I	J
3	D	E	F	G	H	I	J	K
4	E	F	G	H	I	J	K	L
5	F	G	H	I	J	K	L	M
6	G	H	I	J	K	L	M	N
7	H	I	J	K	L	M	N	O
8	I	J	K	L	M	N	O	P
9	J	K	L	M	N	O	P	Q
10	K	L	M	N	O	P	Q	R
11	L	M	N	O	P	Q	R	S
12	M	N	O	P	Q	R	S	T
13	N	O	P	Q	R	S	T	U
14	O	P	Q	R	S	T	U	V
15	P	Q	R	S	T	U	V	W
16	Q	R	S	T	U	V	W	X
17	R	S	T	U	V	W	X	Y
18	S	T	U	V	W	X	Y	Z
19	T	U	V	W	X	Y	Z	A
20	U	V	W	X	Y	Z	A	B
21	V	W	X	Y	Z	A	B	C
22	W	X	Y	Z	A	B	C	D
23	X	Y	Z	A	B	C	D	E
24	Y	Z	A	B	C	D	E	F
25	Z	A	B	C	D	E	F	G

Table

.le encryption! Assume two
mod 26.

b_3 mod 26 which performs
ombination $e_{k2}(e_{k1}(x))$.
$= 11, b_2 = 7$.
e_{k1} and the result with e_{k2},

earch attack is applied to a
y space increased?

practical importance in the
nultiple encryption (in par-
rably, cf. Section 5.3.2.

ıe shift cipher can easily be
of the shift cipher, namely
stead of using a single key k
n a secret code word c. The
$c_0, c_1, \ldots, c_{l-1}$). Each letter
its position in the alphabet.
e by $(k_0, k_1, \ldots k_{l-1})$.
st plaintext letter x_0 is cycli-
k_1 positions and so on, until
now on, the shift sequence
ns, the next plaintext by k_1

$x_1, \ldots$).
. is called a *polyalphabetic*

of size $l = 7$. Transform the
$_i$. You can use Table 1.4 for

KERS with the Vigenère ci-
ne corresponding shift value
sion of the plaintext.
e cipher? Propose an attack.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table 1.4 Polyalphabetic substition table