CHAPTER 2 CLASSICAL ENCRYPTION TECHNIQUES

ANSWERS TO QUESTIONS

2.1 Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.

2.2 Permutation and substitution.

2.3 One key for symmetric ciphers, two keys for asymmetric ciphers.

2.4 A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

2.5 Cryptanalysis and brute force.

2.6 **Ciphertext only**. One possible attack under these circumstances is the brute-force approach of trying all possible keys. If the key space is very large, this becomes impractical. Thus, the opponent must rely on an analysis of the ciphertext itself, generally applying various statistical tests to it. **Known plaintext.** The analyst may be able to capture one or more plaintext messages as well as their encryptions. With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed. **Chosen plaintext.** If the analyst is able to choose the messages to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.

2.7 An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. An encryption scheme is said to be **computationally secure** if: (1) the cost of breaking the cipher exceeds the value of the encrypted information, and (2) the time required to break the cipher exceeds the useful lifetime of the information.

2.8 The **Caesar cipher** involves replacing each letter of the alphabet with the letter standing k places further down the alphabet, for k in the range 1 through 25.

2.9 A **monoalphabetic substitution cipher** maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet.

2.10 The **Playfair algorithm** is based on the use of a 5×5 matrix of letters constructed using a keyword. Plaintext is encrypted two letters at a time using this matrix.

2.11 A **polyalphabetic substitution cipher** uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.

2.12 **1.** There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

2.13 A **transposition cipher** involves a permutation of the plaintext letters.

2.14 Steganography involves concealing the existence of a message.

ANSWERS TO PROBLEMS

2.1 **a.** No. A change in the value of b shifts the relationship between plaintext letters and ciphertext letters to the left or right uniformly, so that if the mapping is one-to-one it remains one-to-one.
b. 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24. Any value of a larger than 25 is equivalent to a mod 26.
c. The values of a and 26 must have no common positive integer factor other than 1. This is equivalent to saying that a and 26 are relatively prime, or that the greatest common divisor of a and 26 is 1. To see this, first note that $E(a, p) = E(a, q)$ $(0 \leq p \leq q < 26)$ if and only if $a(p - q)$ is divisible by 26. **1.** Suppose that a and 26 are relatively prime. Then, $a(p - q)$ is not divisible by 26, because there is no way to reduce the fraction $a/26$ and $(p - q)$ is less than 26. **2.** Suppose

that a and 26 have a common factor $k > 1$. Then $E(a, p) = E(a, q)$, if $q = p + m/k \neq p$.

2.2 There are 12 allowable values of a (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25). There are 26 allowable values of b, from 0 through 25). Thus the total number of distinct affine Caesar ciphers is $12 \times 26 = 312$.

2.3 Assume that the most frequent plaintext letter is e and the second most frequent letter is t. Note that the numerical values are e = 4; B = 1; t = 19; U = 20. Then we have the following equations:

$1 = (4a + b) \bmod 26$
$20 = (19a + b) \bmod 26$

Thus, $19 = 15a \bmod 26$. By trial and error, we solve: $a = 3$.
Then $1 = (12 + b) \bmod 26$. By observation, $b = 15$.

2.4 A good glass in the Bishop's hostel in the Devil's seat—twenty-one degrees and thirteen minutes—northeast and by north—main branch seventh limb east side—shoot from the left eye of the death's head— a bee line from the tree through the shot fifty feet out. (from *The Gold Bug*, by Edgar Allan Poe)

2.5 **a.** The first letter t corresponds to A, the second letter h corresponds to B, e is C, s is D, and so on. Second and subsequent occurrences of a letter in the key sentence are ignored. The result

```
ciphertext:  SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA
plaintext:   basilisk to leviathan blake is contact
```

b. It is a monoalphabetic cipher and so easily breakable.
c. The last sentence may not contain all the letters of the alphabet. If the first sentence is used, the second and subsequent sentences may also be used until all 26 letters are encountered.

2.6 The cipher refers to the words in the page of a book. The first entry, 534, refers to page 534. The second entry, C2, refers to column two. The remaining numbers are words in that column. The names DOUGLAS and BIRLSTONE are simply words that do not appear on that page. Elementary! (from *The Valley of Fear*, by Sir Arthur Conan Doyle)

2.7 a.

2	8	10	7	9	6	3	1	4	5
C	R	Y	P	T	O	G	A	H	I
B	E	A	T	T	H	E	T	H	I
R	D	P	I	L	L	A	R	F	R
O	M	T	H	E	L	E	F	T	O
U	T	S	I	D	E	T	H	E	L
Y	C	E	U	M	T	H	E	A	T
R	E	T	O	N	I	G	H	T	A
T	S	E	V	E	N	I	F	Y	O
U	A	R	E	D	I	S	T	R	U
S	T	F	U	L	B	R	I	N	G
T	W	O	F	R	I	E	N	D	S

4	2	8	10	5	6	3	7	1	9
N	E	T	W	O	R	K	S	C	U
T	R	F	H	E	H	F	T	I	N
B	R	O	U	Y	R	T	U	S	T
E	A	E	T	H	G	I	S	R	E
H	F	T	E	A	T	Y	R	N	D
I	R	O	L	T	A	O	U	G	S
H	L	L	E	T	I	N	I	B	I
T	I	H	I	U	O	V	E	U	F
E	D	M	T	C	E	S	A	T	W
T	L	E	D	M	N	E	D	L	R
A	P	T	S	E	T	E	R	F	O

```
ISRNG  BUTLF  RRAFR  LIDLP  FTIYO  NVSEE  TBEHI  HTETA
EYHAT  TUCME  HRGTA  IOENT  TUSRU  IEADR  FOETO  LHMET
NTEDS  IFWRO  HUTEL  EITDS
```

b. The two matrices are used in reverse order. First, the ciphertext is laid out in columns in the second matrix, taking into account the order dictated by the second memory word. Then, the contents of the second matrix are read left to right, top to bottom and laid out in columns in the first matrix, taking into account the order dictated by the first memory word. The plaintext is then read left to right, top to bottom.

c. Although this is a weak method, it may have use with time-sensitive information and an adversary without immediate access to good cryptanalysis (e.g., tactical use). Plus it doesn't require anything more than paper and pencil, and can be easily remembered.

2.8 SPUTNIK

2.9 PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION

2.10 a.

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

b.

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

2.11 a. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

b. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

c. A cyclic rotation of rows and/or columns leads to equivalent substitutions. In this case, the matrix for part a of this problem is obtained from the matrix of Problem 2.10a, by rotating the columns by one step and the rows by three steps.

2.12 a. $25! \approx 2^{84}$

b. Given any 5x5 configuration, any of the four row rotations is equivalent, for a total of five equivalent configurations. For each of these five configurations, any of the four column rotations is equivalent. So each configuration in fact represents 25 equivalent configurations. Thus, the total number of unique keys is 25!/25 = 24!

2.13 A mixed Caesar cipher. The amount of shift is determined by the keyword, which determines the placement of letters in the matrix.

2.14 **a.** We need an even number of letters, so append a "q" to the end of the message. Then convert the letters into the corresponding alphabetic positions:

M	e	e	t	m	e	a	t	t	h	e	u	s	u	a	l
13	5	5	20	13	5	1	20	20	8	5	21	19	21	1	12
P	l	a	c	e	a	t	t	e	n	r	a	t	h	e	r
16	12	1	3	5	1	20	20	5	14	18	1	20	8	5	18
T	h	a	n	e	i	g	h	t	o	c	l	o	c	k	q
20	8	1	14	5	9	7	8	20	15	3	12	15	3	11	17

The calculations proceed two letters at a time. The first pair:

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 13 \\ 5 \end{pmatrix} \bmod 26 = \begin{pmatrix} 137 \\ 100 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 22 \end{pmatrix}$$

The first two ciphertext characters are alphabetic positions 7 and 22, which correspond to GV. The complete ciphertext:

GVUIGVKODZYPUHEKJHUZWFZFWSJSDZMUDZMYCJQMFWWUQRKR

b. We first perform a matrix inversion. Note that the determinate of the encryption matrix is (9 × 7) – (4 × 5) = 43. Using the matrix inversion formula from the book:

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = \blacksquare \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \bmod 26 = 23 \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \bmod 26 = \begin{pmatrix} 161 & -92 \\ -115 & 9 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$$

Here we used the fact that $(43)^{-1} = 23$ in Z_{26}. Once the inverse matrix has been determined, decryption can proceed. Source: [LEWA00].

2.15 Consider the matrix **K** with elements k_{ij} to consist of the set of column vectors K_j, where:

$$\mathbf{K} = \begin{pmatrix} k_{11} & \cdots & k_{1n} \\ \vdots & \vdots & \vdots \\ k_{n1} & \cdots & k_{nn} \end{pmatrix} \quad \text{and} \quad \mathbf{K}_j = \begin{pmatrix} k_{1j} \\ \vdots \\ k_{nj} \end{pmatrix}$$

The ciphertext of the following chosen plaintext *n*-grams reveals the columns of **K**:

$$\begin{aligned} &(B, A, A, \ldots, A, A) \leftrightarrow K_1 \\ &(A, B, A, \ldots, A, A) \leftrightarrow K_2 \\ &\qquad\qquad\qquad\qquad\quad \vdots \\ &(A, A, A, \ldots, A, B) \leftrightarrow K_n \end{aligned}$$

2.16 **a.** 7×13^4
b. 7×13^4
c. 13^4
d. 10×13^4
e. $2^4 \times 13^2$
f. $2^4 \times \quad (13^2 - 1) \times 13$
g. 37648
h. 23530
i. 157248

2.17 **a.** $(80 - 10) \bmod 26 = 18$
b. $[(1 \times 9 \times 5) + (7 \times 2 \times 1) + (22 \times 4 \times 2) - (22 \times 9 \times 1) - (2 \times 2 \times 1) - (5 \times 7 \times 4)] \bmod 26$
$= (45 + 14 + 176 - 198 - 4 - 140) \bmod 26$
$= (-107) \bmod 26 = 23$

2.18 We label the matrices as **A** and **B**, respectively.
a. $\det(\mathbf{A}) = (44 - 3) \bmod 26 = 15$
$(\det(\mathbf{A}))^{-1} = 7$, using Table E.1 of Appendix E

$$\mathbf{A}^{-1} = \left(\det(\mathbf{A})\right)^{-1} \begin{pmatrix} \text{cof}_{11}(\mathbf{A}) & \text{cof}_{21}(\mathbf{A}) \\ \text{cof}_{12}(\mathbf{A}) & \text{cof}_{22}(\mathbf{A}) \end{pmatrix} =$$

$$7 \times \begin{pmatrix} 22 & -3 \\ -1 & 2 \end{pmatrix} \bmod 26 = \begin{pmatrix} 154 & -21 \\ -7 & 14 \end{pmatrix} \bmod 26 = \begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}$$

b. det(**B**) =[(6 × 16 × 15) + (24 × 10 × 20) + (1 × 13 × 17) – (1 × 16 × 20) – (10 × 17 × 6) – (15 × 24 × 13)] mod 26
= (1440 + 4800 + 221 – 320 – 1020 – 4680) mod 26
= 441 mod 26 = 25
We use the formulas from Appendix E

$$\frac{\text{cof}_{ji}(\mathbf{K})}{\det(\mathbf{K})} \bmod 26 = 17 \times \text{cof}_{ji}(\mathbf{K}) \bmod 26$$

$$b_{11} = \begin{vmatrix} 16 & 10 \\ 17 & 15 \end{vmatrix} \times 25 \bmod 26 = (16 \times 15 - 10 \times 17) \times 25 \bmod 26 = 5100 \bmod 26 = 8$$

$$b_{12} = -\begin{vmatrix} 24 & 1 \\ 17 & 15 \end{vmatrix} \times 25 \bmod 26 = -(24 \times 15 - 1 \times 17) \times 25 \bmod 26 = -8575 \bmod 26 = 5$$

$$b_{13} = \begin{vmatrix} 24 & 1 \\ 16 & 10 \end{vmatrix} \times 25 \bmod 26 = (24 \times 10 - 1 \times 16) \times 25 \bmod 26 = 5600 \bmod 26 = 10$$

$$b_{21} = -\begin{vmatrix} 13 & 10 \\ 20 & 15 \end{vmatrix} \times 25 \bmod 26 = -(13 \times 15 - 10 \times 20) \times 25 \bmod 26 = 125 \bmod 26 = 21$$

$$b_{22} = \begin{vmatrix} 6 & 1 \\ 20 & 15 \end{vmatrix} \times 25 \bmod 26 = (6 \times 15 - 1 \times 20) \times 25 \bmod 26 = 1750 \bmod 26 = 8$$

$$b_{23} = -\begin{vmatrix} 6 & 1 \\ 13 & 10 \end{vmatrix} \times 25 \bmod 26 = -(6 \times 10 - 1 \times 13) \times 25 \bmod 26 = -1175 \bmod 26 = 21$$

$$b_{31} = \begin{vmatrix} 13 & 16 \\ 20 & 17 \end{vmatrix} \times 25 \bmod 26 = (13 \times 17 - 16 \times 20) \times 25 \bmod 26 = -2475 \bmod 26 = 21$$

$$b_{32} = -\begin{vmatrix} 6 & 24 \\ 20 & 17 \end{vmatrix} \times 25 \bmod 26 = -(6 \times 17 - 24 \times 20) \times 25 \bmod 26 = 9450 \bmod 26 = 12$$

$$b_{33} = \begin{vmatrix} 6 & 24 \\ 13 & 16 \end{vmatrix} \times 25 \bmod 26 = (6 \times 16 - 24 \times 13) \times 25 \bmod 26 = -5400 \bmod 26 = 8$$

$$\mathbf{B}^{-1} = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$$

2.19 key: *legleglegle*
plaintext: explanation
ciphertext: PBVWETLXOZR

2.20 a.

s	e	n	d	m	o	r	e	m	o	n	e	y
18	4	13	3	12	14	17	4	12	14	13	4	24
9	0	1	7	23	15	21	14	11	11	2	8	9
1	4	14	10	9	3	12	18	23	25	15	12	7
B	E	C	K	J	D	M	S	X	Z	P	M	H

b.

c	a	s	h	n	o	t	n	e	e	d	e	d
2	0	18	7	13	14	19	13	4	4	3	4	3
25	4	22	3	22	15	19	5	19	21	12	8	4
1	4	14	10	9	3	12	18	23	25	15	12	7
B	E	C	K	J	D	M	S	X	Z	P	M	H

2.21 your package ready Friday 21st room three Please destroy this immediately.