Transposition Cipher Exercises

1. Assume that you are to cryptanalyze a ciphertext that you know was encrypted with a columnar transposition cipher using a full rectangular array. For each of the following message lengths, determine what row × column dimensions for the array are possible.

1a. 25
1b. 22
1c. 45
1d. 12
1e. 24

2. Use a columnar transposition cipher with a rectangular array and keyword *mathematician* to encrypt the following message:

    Sample the electronic environment of the east
    coast of North Korea. Emphasis is intercepting
    coastal radars.

3. The following message was encrypted with a columnar transposition cipher using a full rectangular array and keyword `mathematics`. Decrypt it.

    RIUGS   IPNCT   MSPAL   AUNCY   SOOCH   UEYSA
    RTE

4. Cryptanalyze the following message. It was encrypted with a columnar transposition cipher using a full rectangular array.

    NTDVC   ILRDT   LFNIT   AUEEE   UEOUA   OVSEN
    CIOTN   CCSLS   ATIPN   RNVA

5. A message is encrypted with a transposition cipher. What should we see if we do a frequency analysis of the message?

6. For columnar transposition, would it be easier to break a ciphertext of 65 letters if a 5×13 or a 13×5 rectangle were used for the encrypting? Explain.

7. Use a railfence cipher with 3 rails – removing the rails from top to bottom – to encrypt the message

    ```
    alan turing the enigma
    ```

8. Try decrypting this message that was encrypted by using a railfence cipher with two rails.

    ```
    TEETN   WRTRA   HNWSE   EOEBA   TUSHR   ISHBS   KONOO
    MCIEA   DVLPD   YRHRC   EBU
    ```

9. Try decrypting this message that was encrypted with a railfence cipher with four rails:

    ```
    TTTPT   QDSYP   RSHII   XEDOH   EIUNS   ESLDY   TEMES
    SERSE   NELSC   NEAUC   FLERE   GAMAE   BHDIH   SCUCD
    NG
    ```

10. Decrypt the following message that was encrypted with a columnar transposition with keyword *welchman*.

    ```
    LAOAE   CEDOS   EEOHN   NAHRE   FESSV   EGEGA   SCJMS
    WDPSD   OTIAS
    ```

11. Cryptanalyze the following message that was encrypted using columnar transposition.

    ```
    RTAEQ   DEHLR   CEERQ   SVMOT   HDDMQ   EIEFI
    ```

12. Encrypt the message

> If we have war with the United States, we will
> have no hope of winning unless the United
> States fleet in Hawaiian waters can be
> destroyed.

using the following transposition technique.

Fill in the grid below -- row by row from left to right. Do not place a letter in a cell containing a *.

10	2	8	1	5	3	7	4	6	9
			*						
	*	*						*	
				*	*	*			
			*					*	

Encrypt the message by reading down column one, then down column two, etc.

What problems would we face if we tried to cryptanalyze a message encrypted with this method?

13. Upon searching a room, the following were found on scraps of paper. Use the first to cryptanalyze the second.

On the first scrap

10	2	8	1	5	3	7	4	6	9
t	h	e	t	r	a	n	s	p	o
s	i	t	i	o	n	w	a	s	t
h	e	r	e	a	l	s	t	u	m
b	l	i	n	g	b	l	o	c	k

    THASR PNEOT IINAO SWTTS EELTA USRMH NLBOG CLIKB

On the second scrap

    ERMND LAIEF ETATW HYHRD HUHPT UEGRO SLAOH WDELP
    NAD

14. Transposition ciphers are often used to re-encrypt other ciphers. Here is a ciphertext that was first encrypted by a Caesar cipher and then encrypted again by a columnar transposition cipher using a full rectangle. Cryptanalyze it.

    AMXTX   HXXVH   HBXYA   BTGXT   TXTMM   KMVMF   UKKGX
    YFARX   MGAXD   FWKKL   KTTTZ   WUGBL   MEMRL

15a. Determine the eight routes that are obtained from the diagonal route transposition pattern.
15b. From the spiral route transposition pattern,
15c. From the orthogonal boustrophedon pattern.
15d. From the diagonal boustrophedon pattern.
15e. From the crab spiral pattern.

66. Enter the characters `ABCDEFGHIKLMNOPQRSTUVWXYZ` into a 5×5 array using the basic orthogonal boustophedon pattern, and remove the characters using the basic spiral pattern.

17. Construct a 6×6 turning grille that is different from the one given in the text. Describe a procedure for constructing a 6×6 turning grille. How many 6×6 turning grilles are possible?

18. Construct a 8×8 turning grille. Describe a procedure for constructing a 8×8 turning grille. How many 8×8 turning grilles are possible?