Columnar ciphers (subclass of transposition ciphers)

< Simple columnar cipher (rail fence, scytale) >

○ Encryption
  1. Set up k columns
     - k is the key.

  2. Write a plaintext (columnar cipher) in the columns.

  3. The text is transcribed column by column left to right to produce a ciphertext.

CMCEONIRLAPURH

○ Decryption

In-Class Exercise: If the number of columns is 4 and the ciphertext is

FUPETEWRI

find the plaintext.

Solution:

There are 10 = 4\cdot2 + 2 letters in the ciphertext. Thus there are 2 full rows, and the last row has 2 letters.

Hence

F E W B
U T R I → few, but ripe.
Encryption
1. Select a keyword; each letter defines a column.

```
apple
```

2. Write a plaintext in the columns.

```
apple
keyword
column
```

3. Rearrange the columns according to the alphabetical order of letters in the keyword.

```
aelp
kowey
rldoc
uramn
```

Decryption

In-Class Exercise: If the keyword is “banana,” decrypt the following ciphertext:

```
HPIOLNSDENRPOGWIHNNOBIE
```

Solution:

```
a_1 a_2 a_3 b_1 b_2
H L S P I 0
P Y E O H B
I S N G N I
O D R W NE
```

```
b_1 b_2 b_3
P H I L O S
P O PH Y B E
G I N S I N
W O N D E R
```