Transposition Ciphers

CMPUT 396

Transposition cipher: encryption

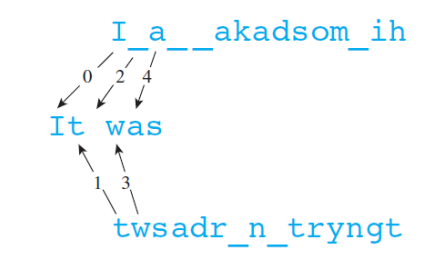
Original	It was a dark and stormy night
Even	I _ a _ _ a k a d s o m _ i h
Odd	t w s a d r _ n _ t r y n g t

Break up the plaintext into even and odd characters

twsadr_n_tryngt + I_a__akadsom_ih

Combine the even and odd parts to make the ciphertext

Transposition cipher: decryption



Transposition Algorithm

The transposition cipher rearranges the message's symbols. Each key (or shift) creates a different ordering.

1. Count the number of characters in the message.
2. Draw a row of a number of boxes equal to the key (e.g. 8).
3. Start filling in the boxes from left to right, entering one character per box.
4. When you run out of boxes, add another row of boxes.
5. When you reach the last character, shade in the unused boxes in the last row.
6. Starting from the top left and going down each column, write out the ciphertext.

Encrypting a message

Plaintext: *Common sense is not so common.*

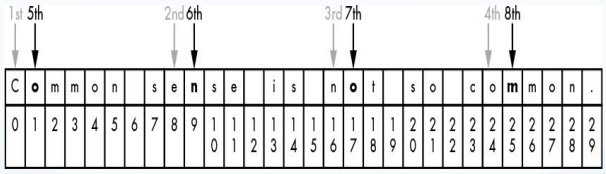
1st	2nd	3rd	4th	5th	6th	7th	8th
C	o	m	m	o	n	■	s
e	n	s	e	■	i	s	■
n	o	t	■	s	o	■	c
o	m	m	o	n	.		

Ciphertext: **Cenoonommstmme oo snnio. s s c**

Indexing the message

1st	2nd	3rd	4th	5th	6th	7th	8th
C 0+0=0	o 1+0=1	m 2+0=2	m 3+0=3	o 4+0=4	n 5+0=5	■ 6+0=6	s 7+0=7
e 0+8=8	n 1+8=9	s 2+8=10	e 3+8=11	■ 4+8=12	i 5+8=13	s 6+8=14	■ 7+8=15
n 0+16=16	o 1+16=17	t 2+16=18	■ 3+16=19	s 4+16=20	o 5+16=21	■ 6+16=22	c 7+16=23
o 0+24=24	m 1+24=25	m 2+24=26	o 3+24=27	n 4+24=28	. 5+24=29		

Creating ciphertext



At the end of the iteration, the ciphertext contains:
['Ceno', 'onom', 'mstm', 'me o', 'o sn', 'nio.', ' s ', 's c'].

Decrypting the ciphertext

	0	1	2	3
0	C 0	e 1	n 2	o 3
1	o 4	n 5	o 6	m 7
2	m 8	s 9	t 10	m 11
3	m 12	e 13	■ 14	o 15
4	o 16	■ 17	s 18	n 19
5	n 20	i 21	o 22	. 23
6	■ 24	s 25	■ 26	
7	s 27	■ 28	c 29	

Scytale

- pronounced /ˈskɪtəli/ [σ κ υ τ ά λ η] "cylinder" was a tool used by ancient Greeks to perform a transposition cipher. A message is written on a strip of parchment, which is then wound around a cylinder.

Anagrams

- **stop**, stpo, **spot**, spto, sopt, sotp
- **tops**, tosp, tsop, tspo, tpos, tpso
- **pots**, **post**, **psot**, psto, ptos, ptso
- opst, **opts**, otps, otsp, ostp, ospt
- **listen, silent, enlist, silent, tinsel, elints**

Counting transpositions

- **stop** (4 letters): 4! = 24
- **listen** (6 letters): 6! = 720
- **toboot** (b:1 t:2 o:3):
  - 6! / (2! * 3!) = 720 / (2 * 6) = 60
- **for example consider this short sentence**
  - 35 letters, distributed as a-z
  - **1** 0 **2** **1** **6** **1** 0 **2** **2** 0 0 **1** **1** **3** **3** **1** 0 **3** **4** **3** 0 0 0 **1** 0 0
  - number of **multiset** arrangements is
  - 35!/(1*2*1*720*2*2*1*1*6*6*1*6*24*6 * 1) = 5.7e31

Voynich Manuscript solution

- Original anagram:
  I put no trust in anagrammatic acrostic cyphers for they are of little real value - a waste – and may prove nothing. Finis.
- Guess #1:
  To arrive at a solution of the Voynich Manuscript, try these general tactics: a song, a punt, a prayer. William F. Friedman.
- Guess #2:
  This is a trap, not a trot. Actually I can see no apt way of unraveling the rare Voynich Manuscript. For me, defeat is grim.
- Actual message:
  The Voynich Manuscript was an early attempt to construct an artificial or universal language of the A-Priori type.—Friedman.