Transposition Cipher

Overview

A transposition cipher reorders the positions of the characters in a **m**essage but does not change the characters themselves.

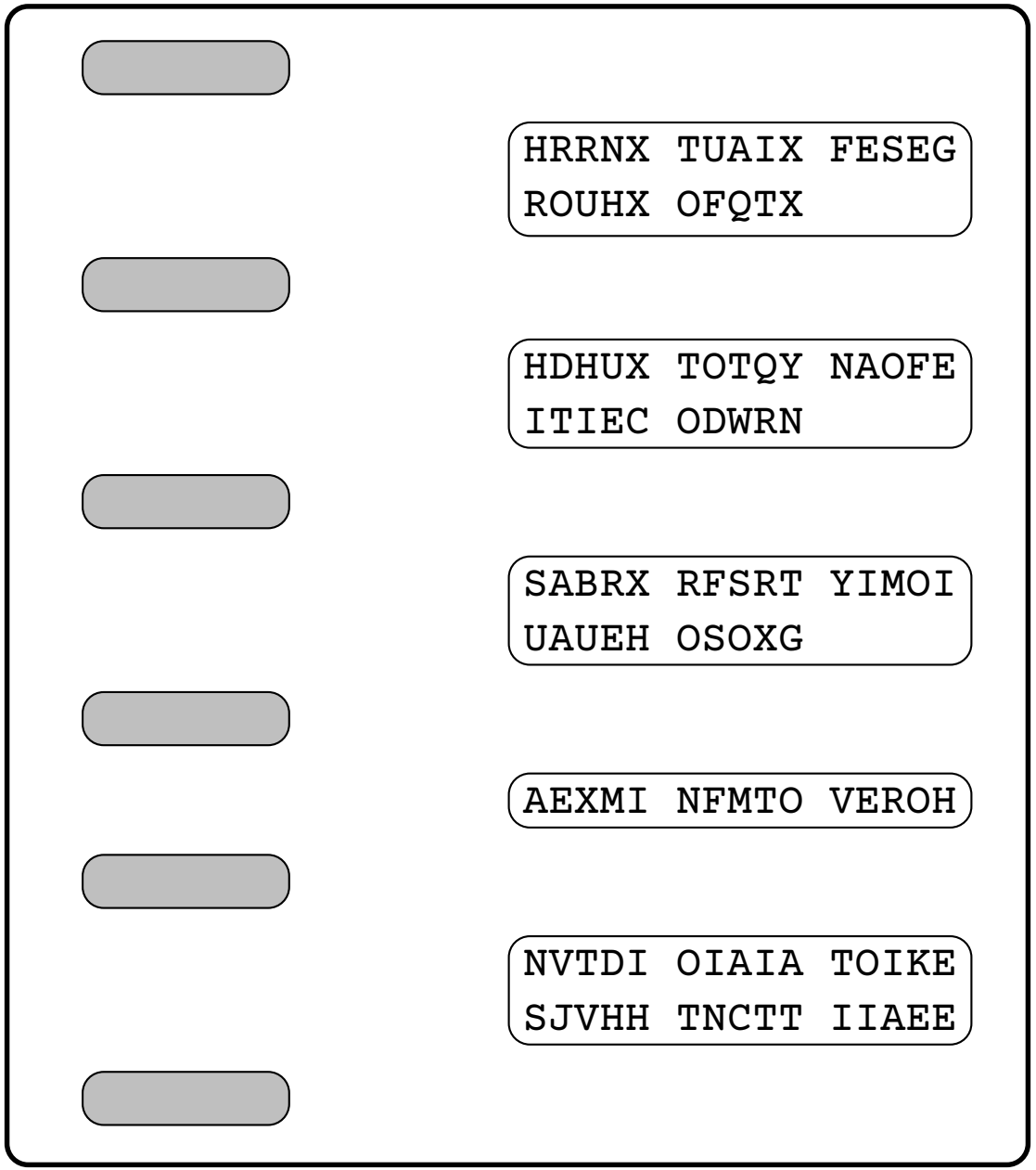
In a col**u**mnar transposition cipher, the message i**s** written out in rows of fixed length, and then read out column-by-column.

Both the w**i**dth of the rows and the ordering of the columns is determined by a se**c**ret keyword agreed upon ahead of time by the message's sender and receiver.

Encryption

To encrypt a message with a keyword of length *n*:

1. Write the message in a grid with *n* columns.
2. Number the columns of the resulting grid according to the alphabetical ordering of the letters of the keyword.
3. Read down the columns of the grid in increasing order of the numbers assigned to the columns in step 2.



Example

Use the keyword `GOBLIN` to encrypt the message:

`HOW QUICKLY DAFT JUMPING ZEBRAS VEX`

1. Write the message in a grid with $n = 6$ columns.

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

2. Number the columns of the resulting grid according to the alphabetical ordering of the letters of the keyword.

2	6	1	4	4	5
G	O	B	L	I	N

3. Read down the columns in increasing order of the numbers assigned in the previous step.

This yields the ciphertext:

`WLJGS HCFIR UDMEE QYUZV IAPBX OKTNA`