Playfair Cipher:

- **Construct a 5x5 Key Square**:

  Create a 5x5 matrix of letters using a keyword. Remove duplicates, then fill the remaining spaces with the other letters of the alphabet (typically combining 'I' and 'J' to fit 25 letters in the 5x5 square).

- **Prepare the Plaintext**:

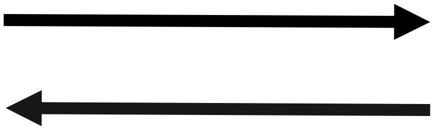
  Divide the plaintext into pairs of letters (digraphs). If a pair has the same letter (e.g., "LL"), insert a filler letter, usually 'X'. If the message has an odd number of letters, add an 'X' at the end.

- **Encrypt the Digraphs**:

  Same Row: If both letters are in the same row, replace each with the letter immediately to its right, wrapping around if needed.

  Same Column: If both letters are in the same column, replace each with the letter immediately below, wrapping around if needed.

  Rectangle Formation: If the letters form a rectangle, replace each letter with the one in the same row but in the column of the other letter.



Keyword:

- **Memorability**: The keyword should be something that is easy for both the sender and receiver to remember.
- **Complexity**: The more complex the keyword, the harder it will be for someone to crack the cipher without knowing it. A longer keyword or a word without common letters (like 'e' or 'a') adds complexity.
- **Avoid Predictability**: Keywords that are common or easy to guess, like "password" or "secret," should be avoided. More obscure words or phrases make the cipher more secure.

  Lets, the keyword is monarchy.

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

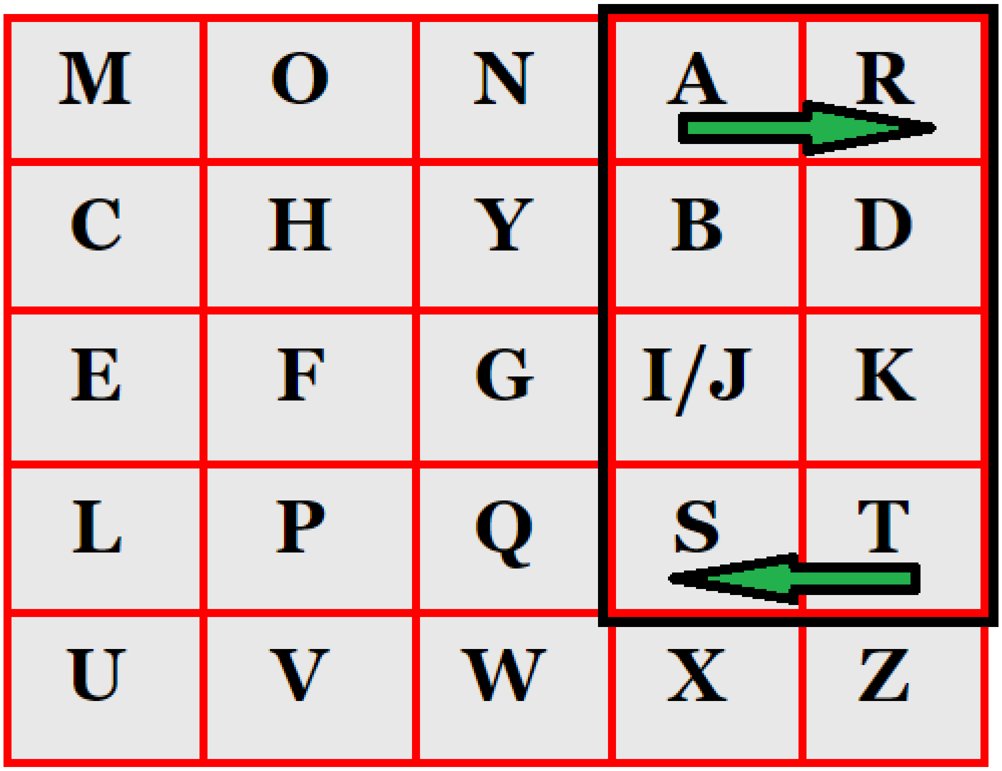
P.T: ATTACK

Diagrams: AT TA CK

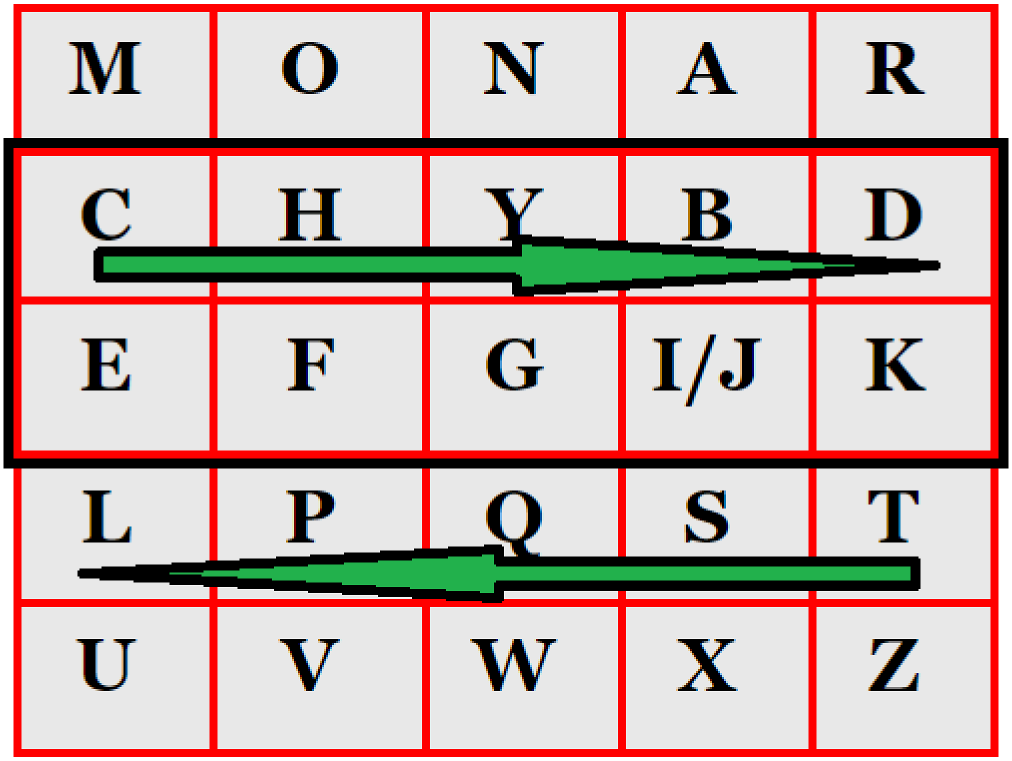
Diagrams: AT TA CK

Ciphertext: RS SR DE

AT:



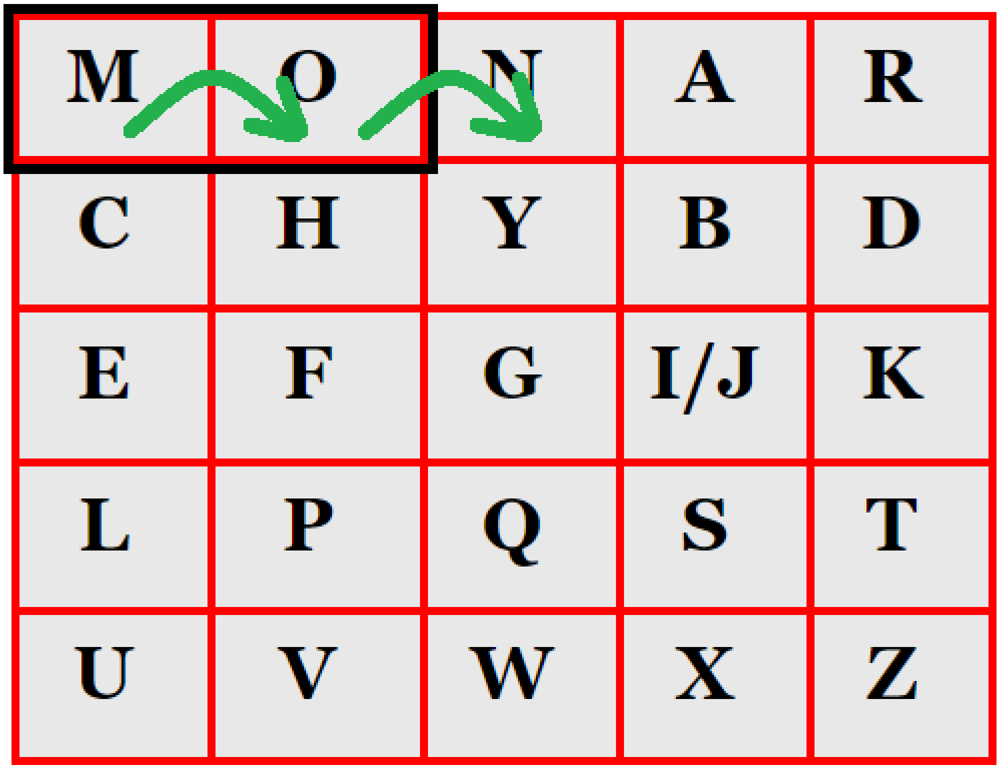
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z



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

Plaintext: mosque

Diagrams: mo sq ue

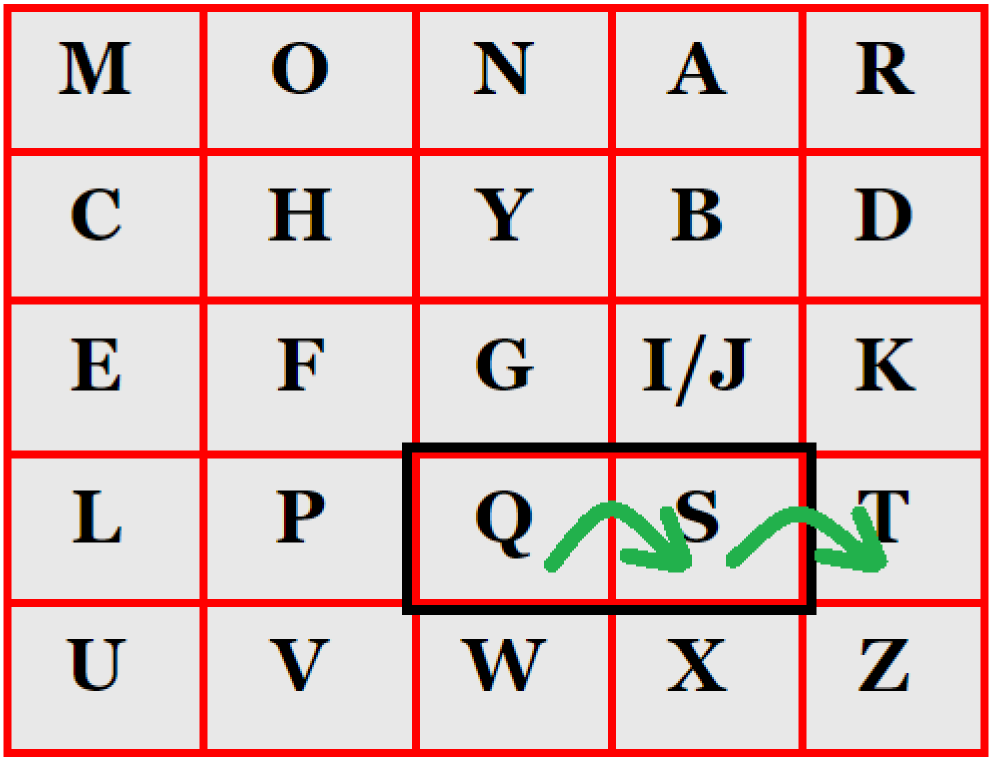


M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Cipher:

Cipher of M is O

Cipher of O is N

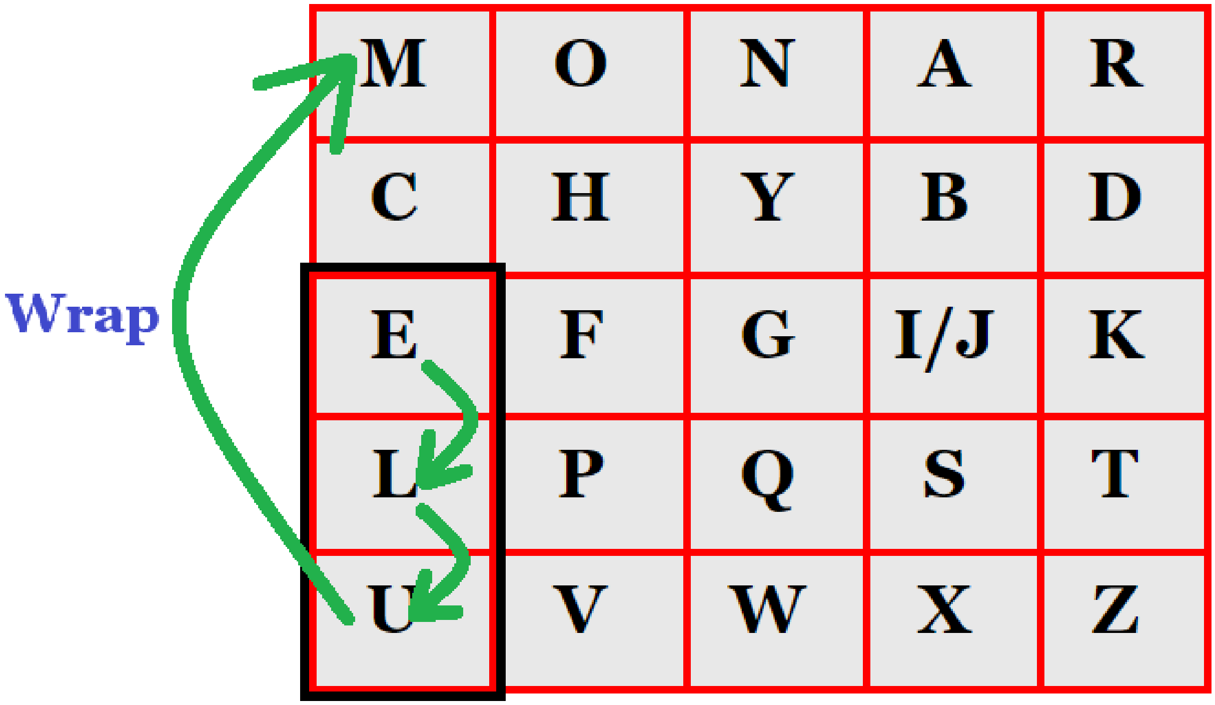


M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Cipher:

Cipher of Q is S

Cipher of S is T



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

Cipher:

Cipher of E is L

Cipher of L is U

Cipher of U is M

Diagrams: mo sq ue

Ciphertext: on ts ml

Vigenère & Autokey: book

The Rail Fence Cipher is a type of transposition cipher in which the plaintext is written in a zigzag pattern (like a rail fence) across multiple "rails" and then read row-wise to create the ciphertext.

Steps for Rail Fence Cipher:

1. **Determine the Number of Rails**:
   - Choose the number of "rails" (rows) to use for encryption.
2. **Write the Plaintext in a Zigzag Pattern**:
   - Write the plaintext diagonally down and up in a zigzag pattern, alternating between the rails.
3. **Create the Ciphertext**:
   - Read the letters row-wise to generate the final ciphertext.

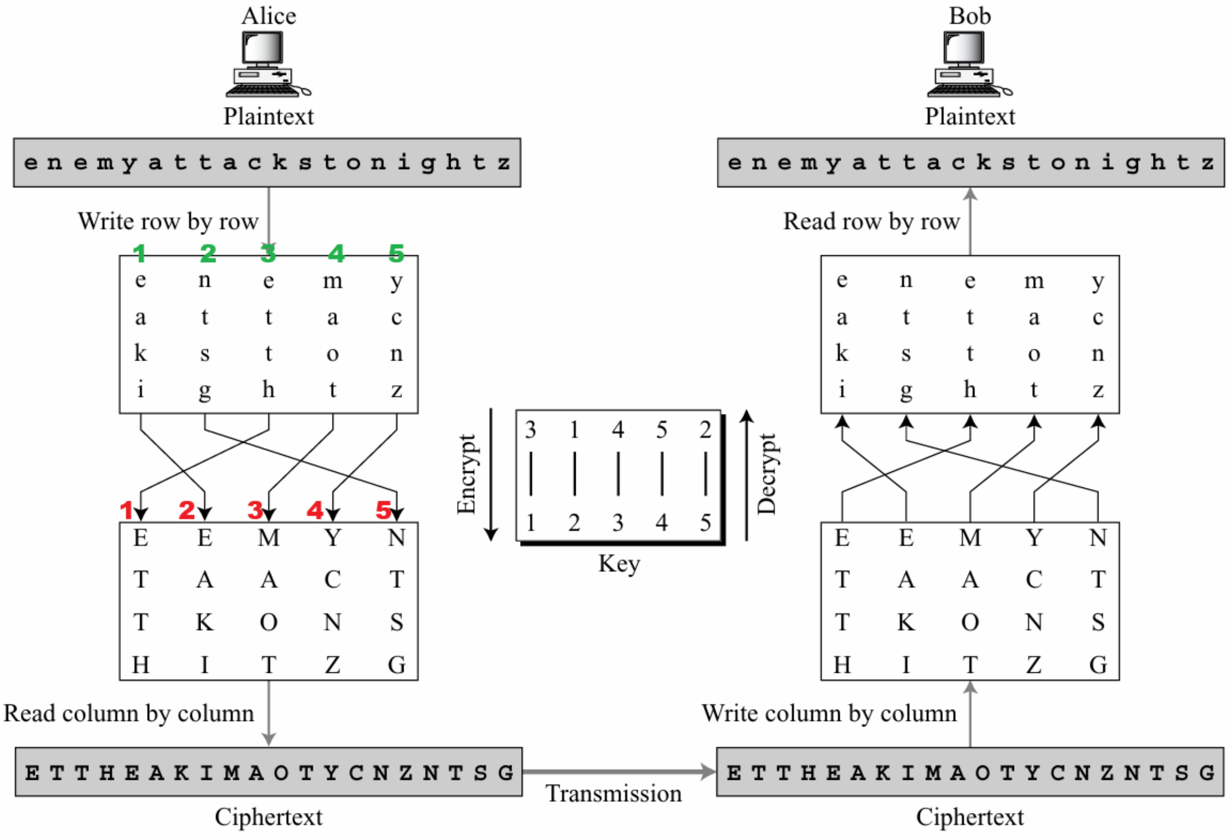
Fascist sheikh hasina

f				i				s				k				a				a
	a		c		s		-		h		i		h		h		s		n	
		s				t				e				-				i		

- **First rail** (top rail): **fiskaa**
- **Second rail** (middle rail): **acs hihhsn**
- **Third rail** (bottom rail): **ste i**

Ciphertext: **fiskaa acs hihhsnste i**

Row-Column Transposition:



enemyattackstonightz

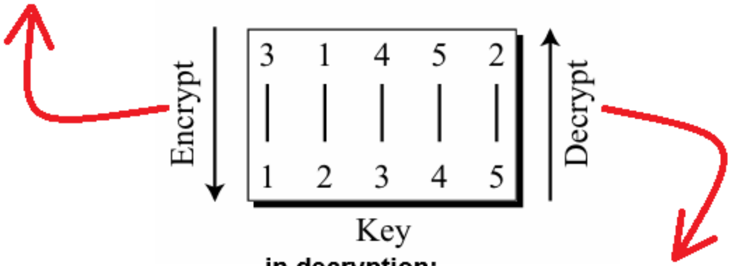
1	2	3	4	5
e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

3	1	4	5	2
1	2	3	4	5

1	2	3	4	5
E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

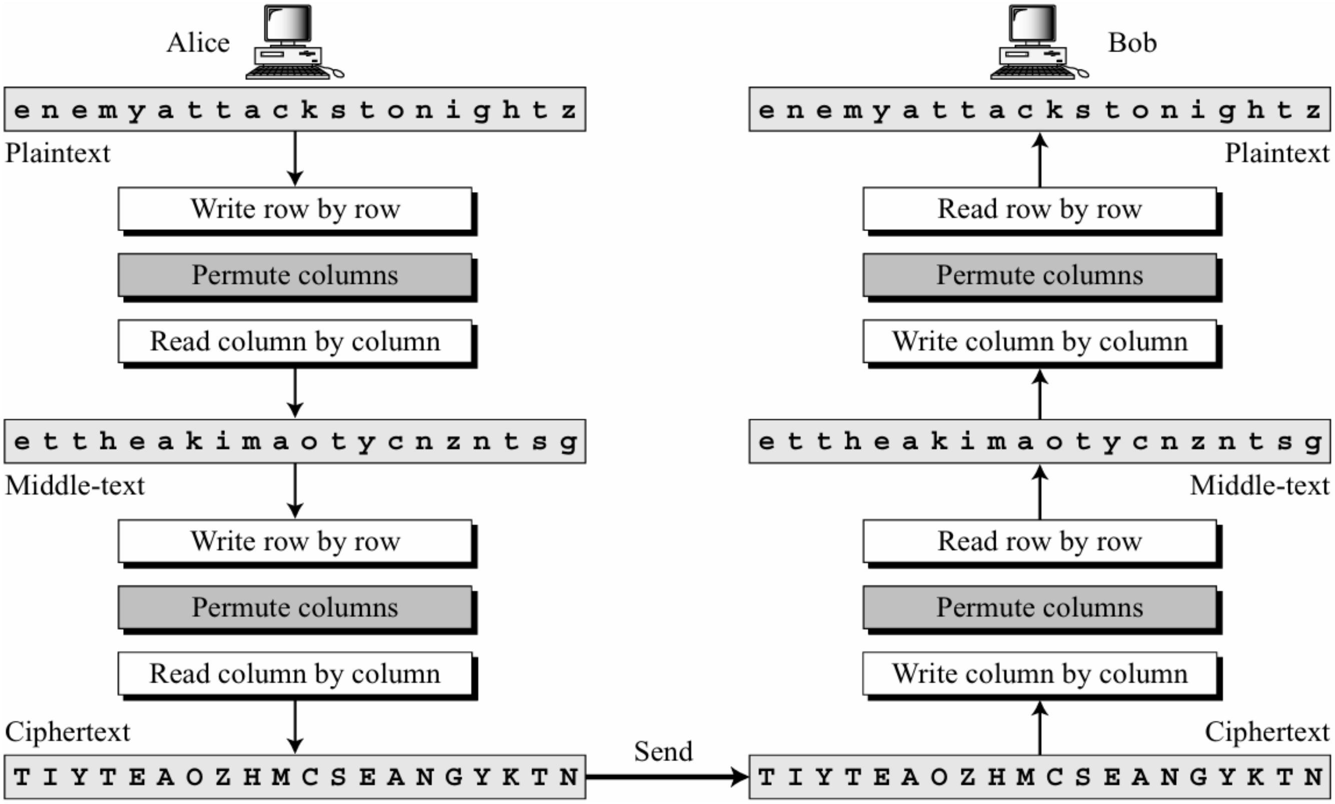
ETTHEAKIMAOTYCNZNTSG

in encryption:
3rd PT column goes to 1st column of CT
1st PT column goes to 2nd column of CT
4th PT column goes to 3rd column of CT
5th PT column goes to 4th column of CT
2nd PT column goes to 5th column of CT



in decryption:
1st CT column goes to 3rd column of PT
2nd CT column goes to 1st column of PT
3rd CT column goes to 4th column of PT
4th CT column goes to 5th column of PT
5th CT column goes to 2nd column of PT

Double transposition:


Alice
Bob
e n e m y a t t a c k s t o n i g h t z
Plaintext
Write row by row
Permute columns
Read column by column
e t t h e a k i m a o t y c n z n t s g
Middle-text
Write row by row
Permute columns
Read column by column
Ciphertext
T I Y T E A O Z H M C S E A N G Y K T N
Send
T I Y T E A O Z H M C S E A N G Y K T N
Ciphertext
Write column by column
Permute columns
Read row by row
Middle-text
e t t h e a k i m a o t y c n z n t s g
Write column by column
Permute columns
Read row by row
Plaintext
e n e m y a t t a c k s t o n i g h t z