2.2.2 Examples of ciphers

Unlike codes, ciphers convert the message by a rule, known only to the sender and recipient, which changes each individual letter (or groups of letters). A message encrypted using a cipher is going to look like a random string of letters or symbols. Ciphers are easier to use than codes, since the users only have to remember a specific algorithm to encrypt the message, and not a whole dictionary of codewords.

Exercise 3 — a Transposition Ciphers.

In mathematics, *transposition* is a permutation or interchange of two letters or symbols.

Ciphers that use a method of jumbling the order that the letters of the plaintext are written are called *Transposition Ciphers*.

1. What does this message say : *"KCATTA"* ? How has it been enciphered?

   What is bad about this method of enciphering?

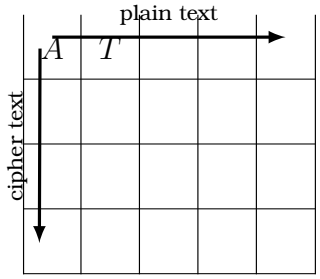
2. Read the boxed text :

   A *Scytale* (rhymes with *Italy*) was an ancient tool used by the Spartans to send secret messages during military campaigns. The sender of the message would wrap a long thin piece of leather around his Scytale, and write the message in rows.

   When the leather was removed from the Scytale, it had a long list of le ers running down it, it no particular order. The receiver would reveal the original message by wrapping the leather around his Scytale (of the same length and diameter).

3. Encypher the message *"attack tomorrow"* with a Scytale wrapped 5 times, with 4 letters per turn :



4. How secure is the Scytale?

Exercise 4 — The Atbash Cipher. See answers

Gsv Zgyzhs Xrksvi is a very old **Substitution Cipher** that was originally developed for use with the Hebrew alphabet. In fact, in the Book of Jeremiah there are several words that have been enciphered using the Atbash Cipher. It is generally considered one of the easiest ciphers to use as it follows a very simple substitution method:

> The first letter of the alphabet is replaced with the last letter, the second letter is replaced with the second from last, and so on...

In Hebrew, the first letter א (aleph) is substituted with the last letter ת (tav), the second letter ב (beth) is replaced with the penultimate letter ש (shin). This is where the cipher gets its name: aleph-tav-beth-shin.

1. Write down what each letter in our alphabet would be substituted with under the Atbash Cipher :

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

2. These words have been enciphered using the Atbash Cipher. Decode them.

a) RHLHXVOVH : ..... | b) ZOTVYIZ: .....

Zgyzhs cipher is not very secure, as there is no "key". If you know that your cipher text is in Atbash, you can very easily decode it.

3. In the tv show "Gravity Falls", there is a cryptogram during the credits of each episode using various ciphers.
Episodes 7 to 13 have Atbash ciphers.
Decode the ciphertext : "V. KOFIRYFH GIVNYOVB"

[ ] is a traditional 13-letter motto of the United States, appearing on the Great Seal. It translates to "One out of many", and is symbolic of the original Thirteen Colonies.