

Cipher Challenge 3

For this challenge you will be given the ciphertext after it has been encoded via the Modified Progressive Shift Cipher (MPSC). Here is how Alice enciphers a message to Bob in MPSC:

Step 1: Alice and Bob agree on a keyword, say “treenut”, and remove duplicate letters leaving them with the reduced keyword “trenu”.

Step 2: The Alphabet Line is created by writing the reduced keyword followed by the remaining English letters in alphabetical order:

t r e n u a b c d f g h i j k l m o p q s v w x y z

Step 3: The plaintext message is written down keeping the word lengths intact. Under the first letter of the first word, write a “1” and continue numbering the letters in the **first word** sequentially. Under the first letter of the second word, write a “2” and continue numbering the letters in the **second word** sequentially. This process continues in the obvious way (first letter of third word is given a “3” ...). For example:

t h i s i s t h e o n l y e x a m p l e
1 2 3 4 2 3 3 4 5 4 5 6 7 5 6 7 8 9 10 11

Step 4: To encipher the first “t”, locate “t” in your alphabet line and shift 1 letter to the right (since there is a 1 under the “t”) to become a “R”. The letter “h” is shifted two letters to the right from its place in the alphabet line to become a “J”. “i” is shifted 3 letters to become “L”. This process continues: each letter is shifted to the right a distance of d where d is the numeral below the letter. If you reach the end of the alphabet line, just wrap around to the beginning. For this example we have:

Plain: t h i s i s t h e o n l y e x a m p l e
 1 2 3 4 2 3 3 4 5 4 5 6 7 5 6 7 8 9 10 11
Cipher: R J L Y K X N L C V D V A C N I Y R Z J

Step 5: The ciphertext is now transmitted, **keeping word lengths intact**. Since Bob knows the keyword, he can easily re-create the alphabet line, write down the appropriate numerals under the ciphertext and start shifting **to the left** to decipher the message.

The following ciphertext was encoded using MPSC. Recover the plaintext.

RW PYXZ TFUAFOE TAHAGFRKW MHXX KWMHO HCMTGQO