**Worksheet 1: The Caesar Cipher**

Julius Caesar used a simple substitution cipher to send messages to his troops. He substituted each letter by the letter that was 3 places further along in the alphabet, so that “a” was replaced with “D”, “b” with “E” and so on.

***Part I*.** complete the table below to show what each letter is enciphered as using this system.

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

***Part II.*** Using the Caesar Cipher, encode the name of your school. Did your partner get the same answer?

Athlone community college

Dwkoqh frppxqlwb froohjh

***Part III.*** Computer scientists would call 3 the “key” for this cipher. How many different keys are possible?

50

***Part IV.*** Decode this message, which was encoded using the Caesar cipher from the table above:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| W | h | a | t |  | d | o |  | y | o | u |  | g | e | t |  | w | h | e | n |  | y | o | u |  |
| Z | K | D | W |  | G | R |  | B | R | X |  | J | H | W |  | Z | K | H | Q |  | B | R | X |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| c | r | o | s | s |  | a |  | s | n | o | w | m | a | n |  | w | i | t | h |  | a |  |
| F | U | R | V | V |  | D |  | V | Q | R | Z | P | D | Q |  | Z | L | W | K |  | D |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| v | a | m | p | i | r | e | ? |  | F | r | o | s | t | b | i | t | e |
| Y | D | P | S | L | U | H | ? |  | I | U | R | V | W | E | L | W | H |

Part 2 Write a program in Python to implement a Caesar cipher.

The program should ask the user for :

* the message, either from a file or direct from the user
* the key number and if the message should be encoded or decoded.
* It should output the answer to a file and to the screen.

Part 3

Extend part 2, so that the user can use any integer value as a key and a mod calculation will be applied to give a valid key value.