Activity - Cipher #1
------------------------
Shift Cipher

Assign each letter to a number $A = 0$, $B = 1$, $C = 2$, $\ldots$, $Z = 25$

We have a secret key that is an integer from 0 to 25. To encrypt a letter, add the key to the numeric version of the letter, if the answer is 26 or greater, take the remainder when divided by 26.

$k = 3.$

Encrypt(CAT) = C = 2, $2 + 3 = 5$ --&gt; F
  A = 0, $0 + 3 = 3$ --&gt; D
  T = 19, $19 + 3 = 22$ --&gt; W

Encrypt(ZOO) = Z = 25, $25 + 3 = 28$ mod 26 = 2 --&gt; C
  O = 14, $14 + 3 = 17$ --&gt; R
  O = 14, $14 + 3 = 17$ --&gt; R

Mathematically, $f(x, k) = (x + k) \% 26$

Do decrypt we do $f^{-1}(y, k) = (y - k + 26)\%26$

Note in programming we need the $+26$ for decrypt, in the book definition, we don't need it.

Note $\%$ is mod in programming…
Also note that the programming mod and math mod are different

The programming mod is a function that returns one answer.
The math mod is stating an equivalence.

How to do this in code…
C
Java

in both C and Java, we access Ascii values in a similar way. So, coding for crypto at least in terms of character values is similar in both languages.

Ascii values for uppercase letters are contiguous.

A = 65, B = 66, ..., Z = 90

same for lowercase

a=97, b=98, ..., z=122

Python

--------
In python you CAN'T ADD or SUBTRACT characters. You have numbers and letters, and they are different types so you have to convert between them.

ord('A') = 65 (in python we convert from letter to number using the ord function)

chr(65) = 'A', we convert from number to letter using the chr function