

CIS 3362 8/24/26

#1 Shift Cipher

$A=0, B=1, \dots, Z=25$

$$f_k(x) = (x+k) \bmod 26$$

In programming $53 \% 26 = 1$ (one answer)
evaluates to $\rightarrow$

$-5 \% 26 = -5$, and this doesn't work well
with ASCII values.

In math $a \equiv b \pmod{n} \Leftrightarrow$

$$n \mid (a-b)$$

$$\left. \begin{array}{l} 53 \equiv 27 \pmod{26} \\ 53 \equiv 1 \pmod{26} \\ 53 \equiv -25 \pmod{26} \end{array} \right\} \text{all true}$$

To decrypt Shift Cipher

$$f_k^{-1}(x) = (x-k) \bmod 26$$

letter to encrypt is $R(17)$ $k=12$

$$(17+12) = 29 \% 26 = 3 \text{ (D)}$$

Decrypt

$$3-12 = -9$$

$$-9 \equiv -9+26 \equiv 17 \pmod{26} \\ = \text{ (R)}$$