HW 2 Selected solutions

Prof. Shahed Sharif

Due 9/20: 2.8/1, 3, 5, 8, 9, 11, Python problems.

2.8.1 Antony cannot tell the difference! If either ARENA is encrypted with $k = 4$ or RIVER is encrypted with $k = 13$, one gets the exact same ciphertext, EVIRE.

2.8.9 The numbers corresponding to C, R, H, A are respectively $2, 17, 7, 0$. We therefore have

$$\begin{aligned} 7\alpha + \beta &\equiv 2 \pmod{26} \\ 0\alpha + \beta &\equiv 17 \pmod{26}. \end{aligned}$$

We immediately obtain $\beta \equiv 17$. Therefore $7\alpha \equiv -15 \equiv 11 \pmod{26}$. The Extended Euclidean algorithm yields $-11 \cdot 7 + 3 \cdot 26 = 1$ (answers may vary), and so $7^{-1} \equiv -11 \equiv 15 \pmod{26}$. Thus $\alpha \equiv 15 \cdot 11 \equiv 9 \pmod{26}$. We have $9^{-1} \equiv 3$, and so decryption is $D(C, k) \equiv 3(C - 17) \pmod{26}$. Plugging in and converting to text yields "HAPPY".