HW 4
Prof. Shahed Sharif

Due 10/11: §4.6/1, 3, 4, 11; §3.14/2, 6, 7

4.6.4 Notice that the 1st and 4th characters of the plaintext are both "a". Since these characters are 3 apart, and the key length is 3, they will be encrypted with the same shift cipher; namely, the shift coming from the first entry in the key. This means that the 1st and 4th characters of the ciphertext should be the same. That is *not* the case for "eblkfg", hence

$$P(M = \text{“attack”} | C = \text{“eblkfg”}) = 0.$$

But $P(M = \text{“attack”}) > 0$, so we do not have perfect secrecy.

4.6.11 With the shift cipher, since the 6th and 7th characters of m_0 ("SS") are the same, those characters in the ciphertext will be the same if m_0 was encrypted. For m_1, the plaintext characters are not the same ("IL"), and so those characters in the ciphertext will also not be the same.

With the Vigenère cipher, the 1st and 4th characters are encrypted with the same shift. But the numerical difference between these is preserved under encryption! Let c_1, c_4 be the 1st and 4th characters of the ciphertext, respectively, and p_1, p_4 same for the plaintext. Let k_1 be the first character of the key. We have

$$\begin{aligned} c_1 - c_4 &\equiv (p_1 + k_1) - (p_4 + k_1) \pmod{26} \\ &\equiv p_1 - p_4 \pmod{26}. \end{aligned}$$

Now consider $Y = 24$, $P = 15$, $F = 5$. The alphabetical distance between the 1st and 4th characters of m_0 is $24 - 15 = 9$, and for m_1 is $24 - 5 = 19$. Thus we measure the alphabetical distance between the 1st and 4th characters of the ciphertext; if it is 9, then the plaintext was m_0, and if it was 19, then the plaintext was m_1.

Lastly, the OTP has perfect secrecy, hence we have advantage 0 in the CI game. Thus we cannot determine anything about the plaintext.

3.14.2 We apply our Extended Euclidean Python code to get

$$-1405 \cdot 65537 + 26226 \cdot 3511 = 1.$$

Multiplying through by 17 yields

$$-23885 \cdot 65537 + 445842 \cdot 3511 = 17.$$