HW4  30 Points   Due  Sep 14

1) With modulus p = 29 and unknown enciphering key e, produces the cipher text

   04 19 19 11 04 24 09 15 15   (5 points)

   It is also known that the cipher text number 24 corresponds to the plaintext letter U.

2) Compute H(X) if there are 256 equally likely messages?   (5 points)

3) Suppose a message X is one of the 6 letters: ABCDEF   (10 points)
   p(A) = p(B) = 1/4
   p(C) = p(D) = p(E) = p(F) = 1/8

   a) What is H(X)?
   b) Construct an optimal encode/decode tree
   c) Encode the string ACBDAEBF
   d) What is the total number of bits in the encoded string?
   e) What is the average number of bits per character in the string?
   f)

4) (10 points)

   Consider a cryptosystem in which \( \mathcal{P} = \{a, b, c\} \), \( \mathcal{K} = \{K_1, K_2, K_3\} \) and \( \mathcal{C} = \{1, 2, 3, 4\} \). Suppose the encryption matrix is as follows:

   \[
   \begin{array}{ccc}
   a & b & c \\
   K_1 & 1 & 2 & 3 \\
   K_2 & 2 & 3 & 4 \\
   K_3 & 3 & 4 & 1 \\
   \end{array}
   \]

   Given that keys are chosen equiprobably, and the plaintext probability distribution is \( \Pr[a] = 1/2 \), \( \Pr[b] = 1/3 \), \( \Pr[c] = 1/6 \), compute \( H(\mathcal{P}), H(\mathcal{C}), H(\mathcal{K}), H(\mathcal{K}|\mathcal{C}), \) and \( H(\mathcal{P}|\mathcal{C}) \).