ELG 5373
Data Encryption

Assignment #2
Due: Thursday, February 15, 2018 (in class, before the lecture begins)
Please answer clearly (show your work).

1. Let \( X \) be an integer variable represented with 32 bits. Suppose the probability is 0.65 that \( X \) is in the range \([0, 2^{24} - 1]\), with all such values being equally likely, and 0.35 that \( X \) is in the range \([2^{24}, 2^{32} - 1]\), with all such values being equally likely. Compute \( H(X) \). [1 mark]

2. Let \( X \) be one of the six messages A, B, C, D, E, F, where \( p(A) = p(B) = p(C) = 1/4 \), \( p(D) = 1/8 \), and \( p(E) = p(F) = 1/16 \). Compute \( H(X) \) and find an optimal binary encoding of the messages. [1.5 marks]

3. Let \( M \) be a secret message revealing the recipient of a scholarship. Suppose that there was one female applicant, Anne, and there were three male applicants, Bob, Doug, and John. The probability of each applicant receiving the scholarship is given by the following: \( p(\text{Anne}) = 1/3 \); \( p(\text{Bob}) = p(\text{Doug}) = p(\text{John}) = 2/9 \). Compute \( H(M) \). Letting \( S \) denote a message revealing the gender of the recipient, compute \( H_S(M) \). [1.5 marks]

4. 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 \( \Pr[a] = 1/10 \), \( \Pr[b] = 1/2 \), and \( \Pr[c] = 2/5 \), compute \( H(P) \), \( H(C) \), \( H(K) \), \( H(K|C) \), and \( H(P|C) \). [2 marks]

5. If you have an encryption algorithm that is not very strong, explain how you can use the concept of unicity distance to improve the security of your ciphertexts without increasing the key length or changing the algorithm in any way. [1 mark]