Math 401 Fall 2018
Cryptology HW 4
Due Thursday, September 27

1. Consider a cipher with three keys, three plaintexts, and four ciphertexts, given by:

	m_1	m_2	m_3
k_1	c_2	c_4	c_1
k_2	c_1	c_3	c_2
k_3	c_3	c_1	c_4

   Suppose all keys are equally likely, and the messages have probability $P(m_1) = 2/5, P(m_2) = 2/5, P(m_3) = 1/5$.

   (a) What is the probability of each ciphertext?

   (b) Compute $P(c_1|m_1), P(c_1|m_2), P(c_1|m_3)$. Can you tell if the ciphertext has perfect secrecy?

   (c) Compute $P(c_2|m_1), P(c_3|m_1), P(c_4|m_1)$.

   (d) Compute $P(k_1|c_3), P(k_2|c_3), P(k_3|c_3)$.

2. Suppose $\#\mathcal{M} = \#\mathcal{C}$. Prove that for a fixed key $k \in \mathcal{K}$ and a fixed ciphertext $c \in \mathcal{C}$, there is a unique plaintext $m \in \mathcal{M}$ such that $e(k, m) = c$. (Hint: this is a counting argument using the fact that e_k is 1-1).

3. Let X be a random variable with possible outcomes $x_1, \ldots, x_n$, and Y a random variable with possible outcomes $y_1, \ldots, y_m$. Let Z be a random variable that corresponds to testing X followed by Y, so the possible outcomes are pairs (x_i, y_j) with $P(x_i, y_j) = P(x_i)P(y_j)$.

   Use the definition of entropy to prove that $H(Z) = H(X) + H(Y)$. This is a special case of property 3 from Shannon's theorem.

   Definition 0.1. The *Key Equivocation* of a cryptosystem is $H(K|C) = H(K) + H(M) - H(C)$. (There's a more complicated formula in terms of rnadom variables, which I'm omitting here). It measures the amount of information about the key revealed by the ciphertext.

   In particular, it tells us how much *more* information we get from the key if we already know the ciphertext. If it is low, knowing the ciphertext tells us a lot about the key. If it's zero, we can determine the key and message purely from the ciphertext.

4. Suppose we have a cryptosystem with two keys $\mathcal{K} = \{k_1, k_2\}$ and three plaintext $\mathcal{M} = \{m_1, m_2, m_3\}$. Suppose the plaintexts have probabilities $P(m_1) = 1/2, P(m_2) = P(m_3) = 1/4$.

   (a) Create an encryption function with three ciphertexts $\mathcal{C} = \{c_1, c_2, c_3\}$, such that $P(c_1) = 1/2$.

   (b) Compute $H(K), H(M), H(C)$.

   (c) Compute the equivocation $H(K|C)$.

   (d) How secure is this cipher?

5. How does key equivocation relate to unicity distance?

6. Compute the unicity distance for

   (a) An autokey cipher

   (b) A Hill cipher with a block size of 2. (Note: only count matrices that are valid keys!)

   (c) A Hill cipher with a block size of 5.