Math 4981 Spring 2021
Cryptography HW 5
Due Thursday, February 18

1. 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. 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 random 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.

2. 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 $P(m_1) = 1/2, P(m_2) = P(m_3) = 1/4$, while the keys are equally likely with $P(k_1) = P(k_2) = 1/2$.

   (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?

3. How does key equivocation relate to unicity distance? (Hint: if your message is much longer than the unicity distance, what should happen to the key equivocation?)

4. Compute the unicity distance for

   (a) An autokey cipher with a N-letter keyword.

   (b) An affine cipher

   (c) A Hill cipher with a block size of 2. (Note: only count matrices that are valid keys! Assume 12/26 of possible matrices are valid keys; this isn't quite right but it's close enough for our purposes.)

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

5. From the definition of big-O notation, prove that $x^2 + \sqrt{x} = O(x^2)$.

6. Prove (using the definition or the limit property) that:

   (a) $k^{300} = O(2^k)$

   (b) $(\log_2(k))^{100} = O(k)$.

7. (a) Prove that $2^{\sqrt{k}} = O(2^{\varepsilon k})$ for any $\varepsilon > 0$.

   (b) Prove that $k^n = O(2^{\sqrt{k}})$ for any n.