CS361 Questions: Week 7

Type your answers and submit on Canvas by midnight on Oct. 25.

1. Why is it impossible to transmit a signal over a channel at an average rate greater than C/h?
2. How can increasing the redundancy of the coding scheme increase the reliability of transmitting a message over a noisy channel?
3. If we want to transmit the numbers 0-9, using a zero-order model, what is the entropy of the language?
4. What are reasons why computing the entropy of a natural language is difficult?
5. Explain the difference between zero, first, second and third-order models.
6. Why are prior probabilities sometimes impossible to compute?
7. Why is the information content of a message relative to the state of knowledge of an observer?
8. What effect does encrypting a message have on the information content of a file?
9. How can redundancy in the source give clues to the decoding process?
10. Rewrite the following in its simplest form: $D(E(D(E(P))))$.
11. Rewrite the following in its simplest form: $D(E(E(P, K_E), K_E), K_D)$.
12. Why might a cryptanalyst want to recognize patterns in encrypted messages?
13. How might properties of language be of use to a cryptanalyst?
14. Explain why an encryption algorithm, while breakable, may not be feasible to break?
15. Why, given a small number of plaintext/ciphertext pairs encrypted under key K, can K be recovered by exhaustive search in an expected time on the order of 2^{n-1} operations?
16. Explain the difference between confusion and diffusion.
17. Is confusion or diffusion better for encryption?