CS361 Questions: Week 7

These questions relate to Modules 8 and 9. Type your answers and submit on Canvas by midnight on Friday, March 10, 2017.

Lecture 34

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?

Lecture 35

1. If we want to transmit the numbers 0-9, using a zero-order model, what is the entropy of the language?

2. What are reasons why computing the entropy of a natural language is difficult?

3. Explain the difference between zero, first, second and third-order models.

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

2. Why is the information content of a message relative to the state of knowledge of an observer?

3. Explain the relationship between entropy and redundancy.

Lecture 37

1. List your observations along with their relevance to cryptography about Captain Kidd’s encrypted message.

2. Explain why a key may be optional for the processes of encryption or decryption.

3. What effect does encrypting a message have on the information content of a file?
4. How can redundancy in the source give clues to the decoding process?

Lecture 38

1. Rewrite the following in its simplest form: \( D(E(D(E(P)))) \).
2. Rewrite the following in its simplest form: \( D(E(E(P, K_E), K_E), K_D) \).
3. Why might a cryptanalyst want to recognize patterns in encrypted messages?
4. How might properties of language be of use to a cryptanalyst?

Lecture 39

1. Explain why an encryption algorithm, while breakable, may not be feasible to break?
2. 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?
3. Explain why substitution and transposition are both important in ciphers.
4. Explain the difference between confusion and diffusion.
5. Is confusion or diffusion better for encryption?