Week 7 Questions

Lecture 34

1. Because you can always get arbitrarily close to the entropy which would get the average rate to be on average C/h.
2. By increasing redundancy, it become more likely that the important bits of the message are not corrupted as they are sent through the noisy channel.

Lecture 35

1. H = -(log 1/10)
2. All natural languages contain specific redundancies. For example, in English, the grammar and cadence of speech varies from person to person.
3. Zero order assumes that all symbols have the same probability. First order assumes that all symbols are independent of each other and some occur more frequently than others. Second and third order is the likelihood of two-letter and three-letter combinations.

Lecture 36

1. For example, the contents of the envelopes at the Academy Awards has the name of the winner in them. Out of 5 nominees, you don't know who is more favored of the other. There are other factors other that there being 5 nominees.
2. If an observer does not know the language, there is no context for which he/she may base their observations on. If it was a binary string, all they would see is a string of 0s and 1s.
3. The more redundant an encoding is the less efficient a message is.

Lecture 37

1. The message is made entirely of numbers and symbols. What is the underlying language of the message that result in such an encoding?
2. *Explain why a key may be optional for the processes of encryption or decryption.*
3. Encryption will hopefully preserve the information content of a file. The goal of is encryption is to hide the message not destroy it.
4. It can give clues to redundancies in the encrypted text. If there were 5 E's in the original message, then in the encryption there could be a certain symbol that shows up only 5 times.

Lecture 38

1. P
2. $D(E(C, K_E), K_E), K_D)$
3. It can give clues to the scenario.
4. Like in English, certain symbols are more likely than others. This would be useful for a cryptanalyst because it gives them a clue as to how the message may have been encoded.

Lecture 39

1. It may take too long to break. If you have a 1 million character encoded message and 100 symbols, it would take 1 million * 100 at most to break the message.
2. There are two possible bits to choose from. With an n-bit string, it would take at most 2^{n-1} operations to find the correct bits.
3. They are the basic building blocks of encryption. Nearly all modern encryption methods use some form of them.

4. Confusion takes the plaintext and changes the text to some other symbols. Diffusion moves the characters around so they are not recognizable.
5. Neither, they are both useful. Sometimes they can be both used.