Week 8 Questions

Lecture 40

1. Monoalphabetic uniformly substitutes whereas polyalphabetic substitutes based on where the plaintext symbol occurs.
2. Itself or another alphabet.
3. Using the English alphabet, you can try all 26 letters to see which one is correct. It would take at most 26! because you would need to try each letter for each symbol in the ciphertext, removing one character each time once the correct one is found.
4. The English alphabet shifted right two times, and wraps around once it reaches the end.
5. 26! size keyspace.
6. No, the Caesar Cipher is not strong.
7. The corresponding decryption algorithm is a reverse lookup on the Vigenère Tableau.

Lecture 41

1. There are 26 letters in the English alphabet and each letter has 26 different ways to be decrypted. Therefore, there are 26^3 = 17,576 possible ways to decrypt.
2. It's a simple substitution of "xyy" which means that there are only 26*25 possible encryptions. Therefore, it is reduced by 26^3 / 26*25.
3. Yes, a perfect cipher is possible. An encryption and decryption algorithm can be written so that they are not inverses of each other.

Lecture 42

1. Ever possible plaintext can be a plausible key for the encryption. Therefore, there is no reduction in the search space.
2. It is important that the key is random so that there is not pattern that can be followed to clue in on the key used to encrypt.
3. With one-time pad is that both the sender and receiver must know the secret key to encrypt and decrypt. The problem is how do they securely share the key.

Lecture 43

1. It preserves the letter frequencies, which can be used as a clue to find the plaintext.
2. The combination of ciphers may give even more clues to the encryption rather than less.

Lecture 44

1. It is an asymmetric algorithm.
2. Key distribution is about we securely distribute keys to everyone who needs it. Key management is about keeping a large number of keys secure.
3. In an asymmetric system, no. Only S has his/her private key therefore only he/she can decrypt the messages.
4. It depends. The two approaches are different and not comparable. A 128-bit symmetric key may be the same strengh as a 3000-bit public key.

Lecture 45

1. One plaintext symbol can be diffused to several different ciphertext symbols. It is harder to break the encryption.
2. It means being able to manipulate ciphertext with predictable effects on plaintext. Being malleable would mean that you can insert symbols to give a clue into how the plaintext is being encrypted.