CS361 Questions: Week 8

Type your answers and submit them on Canvas.

1. What is the difference between monoalphabetic and polyalphabetic substitution?
2. What is the key in a simple substitution cipher?
3. Why are there k! mappings from plaintext to ciphertext alphabets in simple substitution?
4. What is the key in the Caesar Cipher example?
5. What is the size of the keyspace in the Caesar Cipher example?
6. Is the Caesar Cipher algorithm strong?
7. What is the corresponding decryption algorithm to the Vigenere ciphertext example?
8. Why are there 17576 possible decryptions for the "xyy" first encoding on slide 35?
9. Why is the search space reduced by a factor of 27 on the second question?
10. Explain why the one-time pad offers perfect encryption.
11. Why is it important that the key in a one-time pad be random?
12. Why is it important that the key in a one-time pad not be reused?
13. Explain the key distribution problem.
14. What is a downside to using encryption by transposition?
15. How could a combination of ciphers be *weaker* than the individual ciphers alone?
16. Is a one-time pad a symmetric or asymmetric algorithm?
17. Describe the difference between key distribution and key management.
18. If someone obtains K_s, can that person decrypt S's encrypted messages? Explain?
19. Why do you suppose most modern symmetric encryption algorithms are block ciphers?
20. What is the significance of malleability?