CSH6 CH 7 Part 1 – Early Cryptography

1. What do we call well-defined instructions that accomplish a specific task and result in a defined end-state when operating on an initial state?
2. What is a core algorithm for encrypting data called?
3. What is the term used for text in encrypted form?
4. What is the term used for a set of substitutions that allow for transmission of innocent-looking text that can be transformed into meaningful or important text (e.g., "See Manny" could mean "Attack at dawn")?
5. What is the term for extracting plaintext from ciphertext?
6. Which of these pairs are synonyms?
7. What is the term used for a word or system for extracting meaningful information from a ciphertext or an encoded message?
8. What is the term used for the original message that can be encoded or enciphered?
9. What is the term used for converting plaintext to ciphertext?
10. What is the name for the total number of possible keys for a specific key pattern?
11. What is the keyspace of a two-bit key?
12. What is the keyspace of a three-bit key?
13. What is the keyspace of a 1-character key that can use any of the digits from 0 through 9 in any of the positions?
14. What is the keyspace of a 4-character key that can use any of the digits from 0 through 9 in any of the positions?
15. Roughly when did cryptology first make a recorded mark in history?
16. Which of the following aspects of information can be protected or assured using modern cryptograph?
17. What's a MAC in discussions of cryptography?
18. A program computes a MAC for a message being sent to a recipient and the recipient recomputes the MAC and compares it with the one attached to the message. This process is designed to assure ___ of the sent message.
19. A program computes a MAC for a message being sent to a recipient and the recipient recomputes the MAC and compares it with the one attached to the message. If the two MACs do not match, then the recipient should ___ the received message.
20. If someone "signs" a message using their private key in the public key cryptosystem, the sender cannot claim not to have sent the message (unless they also claim that someone else got access to their private key). This feature is known as ___.
21. The stick with a piece of leather or parchment wrapped around it that was used by the Spartans was called a ___.

22. A famous military leader used to shift the letters he used in communicating secretly by three positions (e.g., A became D, B became E and so on). This is now referred to as the ___.
23. Shifting each letter by a fixed number of positions (e.g., writing D for A, E for B and so on) is known as a ___.
24. Shifting each letter by a fixed number of positions (e.g., writing D for A, E for B and so on) is known as a ___.
25. Simple cryptanalysis of a Caesar cipher depends on knowing
26. Brute-force cryptanalysis involves ___.
27. Brute-force cryptanalysis involves knowing ___.
28. Which of the following is the most frequently occurring letter in ordinary English?
29. If a different offset is applied to each value in a plaintext, we can call the resulting cipher a ___.
30. What was the name of the German encryption machine whose mechanism was cracked by the British cryptanalysts in World War II?
31. A method of encrypting text being sent by teletype that was invented by Gilbert Vernam in 1917 used what logical function to encrypt and decrypt?
32. What is, in theory, the only unbreakable cipher (assuming that the shared secret is not compromised)?
33. When a cipher rearranges the data (e.g., using the rail fence technique), it is an example of using ___.
34. The algorithm developed by IBM as "Lucifer" and adopted by the US government as a standard was the ___.
35. What is the meaning of the acronym "DES" in cryptography?
36. Until roughly when was the DES viewed as thoroughly satisfactory?