Review for second test

1. When we did the lab on the Vigenère cipher, we subtracted 96 from both the plain text letter value and the key letter value. We also added 96 to the cipher letter value. Show why these adjustments were necessary.
2. In steganography, a message is inserted into a larger text file.
	1. Explain how to accomplish this insertion without changing the text file’s size.
	2. Explain how to extract the message.
	3. How much larger should the text file be compared to the message? Why?
	4. How was steganography accomplished in ancient times?
3. In cryptography, what is the difference between a cipher and a code?
4. In order to convert plaintext into ciphertext, you need two pieces of information. What are they?
5. What is asymmetric encryption? What advantage does it have over symmetric encryption?
6. Describe the cryptanalysis of the Caesar cipher.
7. The two classic types of cryptography are transposition and substitution. Explain what each one means.
8. In the simple substitution cipher, how many possible keys are there? Why is this not a secure method of encryption, despite the number of keys?
9. When using a homophonic cipher, why is each letter replaced with a two-digit number instead of a one-digit number or letter?
10. Give two examples of a polyalphabetic cipher system.
11. Use this review document as the key for a book cipher to encrypt this phrase: “we did the test for value.” When encoding words, do not encode any numeral such as 96, 1, 2, 3, etc.
12. What was the weakness of the Vigenère cipher that Charles Babbage was able to exploit? How did Alan Turing build on this cryptanalysis later?
13. Why is the one-time pad considered the best form of a Vigenère cipher?
14. When Germans used Enigma, why did they have both a day key and a message key?
15. What did Enigma’s plugboard do?
16. What is a bombe?
17. Use the XOR cipher to convert the plaintext message 10110011 into ciphertext using the key 110.
18. What does the Diffie-Hellman protocol accomplish? What is its advantage?
19. Calculate 2n mod 19 for each value of n from 1 through 12.
20. Explain the principle behind what is called “public key” cryptography. How can a system such as RSA be secure if it uses a public key?
21. If two text messages have the same hash value, this situation is called a \_\_\_\_\_\_\_\_\_\_.
22. A certain cipher system will take 50 years to break using current technology. Assuming Moore’s Law is still valid into the future, how long can we expect the cipher system to still be secure?
23. What does 2-way authentication mean?
24. How does the sender of a message compute a digital signature?
25. Suppose we are using quantum cryptography to send a message in order to generate a random key. Alice wishes to send Bob the bits 00111 and uses the filter orientations X+X+X. Bob guesses the filter orientations as +++++.
	1. What photon orientations does Alice transmit?
	2. How does Bob interpret the message he receives (in terms of bits)
	3. On which bits did Bob use the same filter orientation as Alice?
	4. Is it possible for Bob to use the same filter as Alice, but guess the bit wrong?