Answers to Review for second test

1. If we did not make the adjustments, then our answer would be off by 96. We like to think of the letters a-z represented by the numbers 1-26, but in reality their actual numerical values are 96 larger. For example, ‘a’ is encoded as 97 (a fact you do not need to memorize). In a Vigenère cipher, if we add ‘a’ + ‘a’ we should get ‘b’ since 1+1=2. But 97+97 does not equal 98. The sum is 96 too high.
2. In steganography, a message is inserted into a larger (text) file.
   1. In order to perform steganography so that it does not change the background text file’s size, we need to replace existing letters in it with the letters of our message. In other words, we are not adding more letters to the file.
   2. Scan the file one character at a time. Count the number of characters read so far. The hidden characters are spaced an equal distance apart, and you should already know this distance as the key. For example, if it is 100, then you simply grab every 100th digit in the file.
   3. We discovered in the lab that even spacing the letters in our message 100 characters apart made our insertion too obvious. Spreading them out every 1000 characters, for example, would be better. In this case, the background text file needs to be 1000 times larger than the message.
   4. Some examples of ancient steganography include hiding messages inside food, underneath a layer of wax, on their scalp, or as pinpricks on an innocuous document.
3. With a cipher, we are manipulating (i.e. transposing or changing) the message at the level of individual letters. With a code, the procedure is done on entire words.
4. In order to convert plaintext into ciphertext, we need to know the encryption/decryption function as well as the key.
5. Asymmetric encryption means that we have separate (public) encryption and (private) decryption keys. The advantage is that the two parties do not need to agree in advance on a single secret key.
6. To cryptanalyze the Caesar cipher, we realize that the key must be a number from 1 to 25. We try each of these numbers, subtracting the key from each letter. We stop when we discover a message that makes sense.
7. Transposition means you are swapping the positions of letters in the plaintext in order to generate the ciphertext. Substitution means that you are replacing each letter with some other letter according to some mathematical function.
8. The number of keys in a simple substitution cipher is 26!. This is a very big number. Nevertheless, it is not a secure form of encryption, because a cryptanalyst can perform frequency analysis to deduce which letters, double letters and short words are most common, just like the way people solve cryptogram puzzles in the newspaper.
9. In a homophonic cipher, we need more codes than there are letters, so that we can thwart frequency analysis. A 2-digit number (allowing a leading zero) affords us 100 possible symbols for each letter.
10. Essentially, polyalphabetic means we are performing several Caesar ciphers at once. Examples include the Vigenère and one-time pad ciphers. (In other words, you can think of a Caesar cipher as a degenerate form of Vigenère cipher: the key has just one letter.)
11. Here are the first 25 words in the review document.

1 review 6 we 11 the 16 from 21 letter

2 for 7 did 12 Vigenère 17 both 22 value

3 second 8 the 13 cipher 18 the 23 and

4 test 9 lab 14 we 19 plain 24 the

5 when 10 on 15 subtracted 20 text 25 key

To encrypt the phrase “we did the test for value” using this book cipher we replace each word with its corresponding number in the table. So, the ciphertext becomes 6, 7, 8, 4, 2, 22.

1. Babbage took advantage of short keys. He would look for repetitions of short letter sequences, and take note of how far away they were. This would tell him the length of the key. Knowing the length, Babbage could then treat each nth letter as part of a Caesar cipher. Alan Turing knew that the German Enigma code was based on a Vigenère cipher. Turing took advantage of the fact that messages at certain times of the day were weather forecasts, and he focused on where known words would appear in the plaintext.
2. A one-time pad is really a Vigenère cipher with the best possible key, one that is both very long and random.
3. If the Germans sent all of their traffic in one day using the same key, it would have made it easier for the Allies to break the code. So, only the message key was encrypted using the day key. Each message would have a unique key, and would be sent after the message key.
4. The Enigma plugboard would swap letters before they got encrypted by the scramblers.
5. During World War 2, Polish and British cryptanalysts built machines to automate the procedure of breaking the German Enigma code. These machines were called bombes.
6. In order to perform the XOR cipher on 10110011 into ciphertext using the key 110, we work this problem like the Vigenère cipher: repeat the key as often as necessary. Then XOR means the result is 1 if the corresponding bits differ, 0 if they are the same.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| Key | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| Ciphertext | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |

1. In the Diffie-Hellman protocol, the two parties send messages in order to establish a secret key that they can both use for encrypting. It has the advantage that the two people don’t need to see each other in person or trust a third party messenger to deliver the key information.
2. Calculate 2n mod 19 for each value of n from 1 through 12.

|  |  |
| --- | --- |
| Value of n | Value of 2n mod 19 |
| 1 | 2 |
| 2 | 4 |
| 3 | 8 |
| 4 | 16 |
| 5 | 32 mod 19 = 13 |
| 6 | 13 \* 2 = 26; and then 26 mod 19 = 7 |
| 7 | 7 \* 2 = 14 |
| 8 | 14 \* 2 = 28; and then 28 mod 19 = 9 |
| 9 | 9 \* 2 = 18 |
| 10 | 18 \* 2 = 36; and then 36 mod 19 = 17 |
| 11 | 17 \* 2 = 34; and then 34 mod 19 = 15 |
| 12 | 15 \* 2 = 30; and then 30 mod 19 = 11 |

1. A public key is used to encrypt, but in order to decrypt you must have the private key.
2. If two text messages have the same hash value, this situation is called a collision.
3. Every 1.5 years, the runtime will be reduced by half. So, we can decide to wait a few years before starting to run the long-running program. How long should we wait? Let’s arrange our calculations in a table. The numbers represent years (to the nearest hundredth), and we should take these numbers with a grain of salt. Moore’s Law is an approximation.

|  |  |  |
| --- | --- | --- |
| Wait time | Run time | Total time |
| 0 | 50 | 50 |
| 1.5 | 25 | 26.5 |
| 3 | 12.5 | 15.5 |
| 4.5 | 6.25 | 10.75 |
| 6 | 3.12 | 9.12 |
| 7.5 | 1.56 | 9.06 |
| 9 | 0.78 | 9.78 |

Theoretically, our best answer is a little over 9 years.

1. Two-way authentication means that both parties need to prove who they are. For example, if you enter your account number and password to the bank’s Web site, during this process the bank must provide you with a secret word you set up in advance.
2. An encryption function may be used to compute a digital signature. If the message is very long, preliminary step would be to “hash” (i.e. condense) the message into a smaller string.
3. Using quantum cryptography, Alice wishes to send Bob the bits 00111 and uses the filter orientations X+X+X. Bob guesses the filter orientations as +++++.
   1. Alice transmits \ – / | /
   2. Bob interprets this message as ?0?1?, where ‘?’ means the value could either be 0 or 1.
   3. Bob used the same filter as Alice for the 2nd and 4th bits.
   4. If Bob and Alice use the same filter on the same photon, then Bob’s answer has to be right. He cannot misinterpret it.