CS 105 Review Questions #3

These review questions only include topics since our second test. To study for the final, please look at the first two review documents as well. Almost all of these questions are actual exam questions from the past. Besides the review questions, also study the labs and notes in the course. Good luck!

1. What is a bombe?

2. If we use the XOR function to encrypt a message, then how do we decrypt the ciphertext? What is the key in this case?

3. What does the Diffie-Hellman protocol accomplish? What is its advantage?

4. Calculate 2^n mod 19 for each value of n from 1 through 12.

5. 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?

6. RSA encryption relies on the fact that it is very tedious to factor a large number that is the product of two _____ numbers.

7. Name two ways in which the Germans during World War II weakened the security of their Enigma-based cipher system.

8. When Linear B was being deciphered, what fact about the script told researchers that they were not dealing with an alphabet like that used in English or modern Greek? In other words, if Linear B is phonetic, what is encoded by each symbol?

9. Suppose x and y are binary values used as input to a digital circuit. First, the value of x is fed to a NOT gate to produce x'. Then, x' and y are combined in an XOR gate to produce output z. If z is 1, what can we assume about the original values x and y?
   a. x and y are the same value
   b. x and y are different values
   c. x = 1
   d. y = 1
   e. x = 0
   f. y = 0

10. Suppose an XOR gate has two inputs x and y and an output z. If x = 1 and z = 1, is it possible for us to determine the value of y? If so, what is it?

    a. Practice this question with other logic gates, and other values of x and z.

11. Suppose the values x = 1 and y = 0 are to be fed simultaneously into 4 logic gates: an AND gate, an OR gate, an XOR gate and a NOR gate. What is the output from each gate?

    AND = _____
    OR = _____
    XOR = _____
    NOR = _____

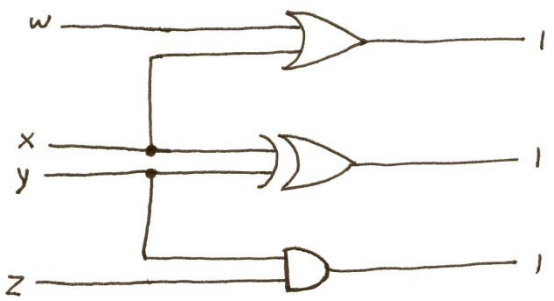
12. In the circuit drawing, assume that the outputs from all the gates are 1. What are the input values w, x, y and z? Fill in the blanks (and indicate if any of these values cannot be determined).

    w = _____

    x = _____

    y = _____

    z = _____



13. Suppose binary values X, Y and Z are the inputs into logic gates as follows. X and Y are inputs to an AND gate, and the result is 1. Y and Z are inputs to an XOR gate and the result is 0. What are the values of X, Y and Z?

14. Suppose the binary values x and y are going to be used as input into both an XOR gate and an AND gate. Can the output of these two gates be the same? Explain.

15. Consider a NAND gate with two inputs x and y and an output z. If x = y, then what can we conclude about z?

16. What are the two outputs of a binary adder circuit?
    a. Sum and difference
    b. Carry in and carry out
    c. Sum and carry
    d. Sign and magnitude
    e. Sum and sign

17. In the von Neumann computer model, what are the three tasks that must be performed on each instruction in a program? List them in the order they occur, and explain why each step is necessary.

18. Let's look at units of memory size.
    a. How many kilobytes are in a gigabyte?

    b. A terabyte equals 2^n bytes of data. What is n?

    c. How many megabytes are there in 2^{25} bytes?

19. The two key parts of a computer's memory system are its RAM and hard disk.
    a. Which typically has a larger capacity, RAM or the hard disk?

    b. Which is faster to access information, RAM or the hard disk?

    c. Give an example of information that would be in RAM, but not on the hard disk.

    d. Give an example of information that would be on the hard disk, but not in RAM

20. Terminology regarding various data transfers:
    a. Suppose you just opened Access, and you want to open a database file for editing. To open this file, what data transfer is taking place in the computer's memory? We say that the file is being copied from _____ to _____.

    b. Suppose you are working in Excel, and after making some significant modifications, you save the spreadsheet file. When you save, data is being copied from _____ to _____.

    c. When files are being "backed up", typically they are being copied from _____ to _____.

    d. When we load a value into a register, the value is being copied from _____ to _____.

21. Which is/are true about RAM, in general?
    a. It has a smaller capacity than the hard drive.
    b. It requires a constant supply of electricity to maintain data.
    c. It contains the registers that the CPU uses to perform operations.
    d. two of the above
    e. all of the above
    f. none of the above

22. Give two reasons why we should not use RAM for all of our computer memory, even if the amount of RAM is more than we will ever need.

23. Which of the following is not an example of secondary memory?
    a. CD
    b. floppy disk
    c. magnetic tape
    d. DVD
    e. super disk
    f. random access memory

24. In a 16-bit instruction, the first 4 bits of an instruction are its opcode. The opcode value 2 means the instruction will put a constant value in a register. Its general format is 2RXX where R is the 4-bit register number, and XX is the 8-bit signed value to put in the register. Write the binary or hexadecimal instruction that will set register number twelve to the number 5.

25. Here is an instruction set for a simple computer. Assume that there are 16 8-bit registers, and the size of RAM is 256 bytes. Instructions are 16 bits long.

Opcode	Hex format	Meaning
1	1RXY	Load register R with the value contained in memory at hex address XY.
2	2RXY	Load the hexadecimal number XY into register R.
3	3RXY	Store the value from register R into memory at address XY.
5	5XYZ	Add the values in registers Y and Z and put the result in register X.

Suppose we wanted to write machine code that adds the contents of bytes 1 and 2 in memory and then puts the result in byte 3. Write the machine code instructions that will accomplish this.

Answers to review #3.

1. A bombe was a special-purpose computer designed by Polish and British cryptanalysts to try numerous key possibilities for deciphering Enigma.

2. With the XOR cipher, we decrypt the message the same way we would encrypt the message: use the XOR function with the same key.

3. The purpose of the Diffie-Hellman protocol is for two people to establish a secret key without transmitting it. The advantage is that it can be used even over an unsecure communication medium.

4. The idea is that we double our previous answer. If our new answer is 19 or more, we subtract 19.

n	2^n mod 19
1	2
2	4
3	8
4	16
5	32 → 13
6	26 → 7
7	14
8	28 → 9
9	18
10	36 → 17
11	34 → 15
12	30 → 11

5. If you want to send someone a message, you encrypt it using their public encryption key. Then you send the ciphertext. The recipient maintains his own secret decryption key to decipher the message. This communication is secure because it uses two keys instead of one. Only the encryption key is public.

6. Prime

7. The Germans duplicated the message key. When using the plugboard, they never linked letters that were next to each other on the keyboard. They did not allow a rotor (scrambler) to reside in the same place two days in a row. Finally, the regimented structure of daily military life made some messages predictable.

8. The total number of phonetic symbols was about 87, which is far more than the number of letters in an alphabet. This suggests that each symbol represents more than one sound, as in a consonant along with a vowel.

9. A

10. Yes; The only possibility that makes sense is that y = 0.

    a. Let's look at several possibilities…

Logic gate	Given output Z	Given input X	Deduce input Y
AND	0	0	Could be either 0 or 1
AND	0	1	Must be 0
AND	1	0	Impossible case
AND	1	1	Must be 1
OR	0	0	Must be 0
OR	0	1	Impossible case
OR	1	0	Must be 1
OR	1	1	Could be either 0 or 1
XOR	0	0	Must be 0
XOR	0	1	Must be 1
XOR	1	0	Must be 1
XOR	1	1	Must be 0

11. AND = 0, OR = 1, XOR =1, NOR = 0

12. First, consider the AND gate. Its output is 1. Thus, its two inputs must also be 1. Thus, y = 1 and z = 1. Next, we consider the XOR gate. The output is 1 and one of its inputs, the y, equals 1. Therefore, the other input, x, equals 0. Finally, we consider the OR gate. Its output is 1, and we know that one of its inputs, x, is 0. Therefore, w = 1. So our 4 answers w-z are 1, 0, 1, 1.

13. All variables equal 1.

14. The outputs are the same only when x = 0 and y = 0. We can verify this with a truth table.

x	y	x AND y	x XOR y
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

15. If x and y are both 0, then the NAND of x and y is 1. If x and y are both 1, then the NAND of x and y is 0. Therefore, z is the negation of x (and also the negation of y). In other words z = NOT x.

16. C

17. Fetch – the instruction resides in RAM and needs to be acted upon in the CPU
    Decode – the instruction is in binary, and we need to pick apart the various pieces of the instruction such as its opcode and operands
    Execute – finally, we are able to perform the instruction

18. Memory sizes
    a. $2^{30} / 2^{10} = 2^{20}$, which is slightly more than a million.
    b. n = 40
    c. A megabyte is 2^{20} bytes. Therefore, $2^{25} / 2^{20} = 2^5$ or 32.

19. Comparing RAM and disk:
    a. The disk is larger.
    b. RAM is faster.
    c. RAM could contain information that you are entering interactively in a program, but you have not yet saved your document.
    d. Among other things, the disk contains files that are not currently in use (i.e. not open).

20. Terminology
    a. disk; RAM
    b. RAM; disk
    c. Disk; tape or other archival storage
    d. RAM; CPU

21. D (only the first two are correct)

22. When you turn off your computer, you will lose everything that's in RAM. Also, that amount of RAM could be prohibitively expensive.

23. F

24. Remember that 4 bits are equivalent to 1 hex digit. In this case, the opcode is 2 (as given to us), and the register operand is 12. Note that this needs to be converted to hexadecimal. The decimal number 12 is represented as C in hex. The XX portion of the instruction should represent 5, and in hex, this would just be 05. Thus, the entire machine language instruction is 2C05.

25. We need to write several instructions. Let's plan them first before writing the machine code.
    First, we need to load the contents of RAM byte 1 into a register, say register 1.
    Second, we similarly need to load the contents of RAM byte 2 into another register, namely #2.
    Next, we perform the addition of registers 1 and 2, and we can put the answer in register 3.
    Finally, we need to store register 3 into RAM byte 3. Please note that our choice of registers throughout our answer has been arbitrary.

    The 4 instructions become:
    1101
    1202
    5312
    3303