NOTE: THIS TEST IS OPEN BOOK. IF YOU DON’T KNOW THE ANSWER, LOOK IT UP. ALSO FEEL FREE TO GO TO THE POWERPOINTS OR OTHER HELPFUL FILES IN CANVAS. I MUST RECEIVE THE COMPLETED TEST AT [HRHINE@COLLIN.EDU](mailto:HRHINE@COLLIN.EDU) BY 11:59 PM, June 24, 2023. DON’T FORGET, I EXPECT A THOUGHTFUL RESPONSE TO THE ESSAY QUESTION. DON’T BLOW IT OFF.

When you submit the test, rename the file COSC 2325 Test 1 your-name. I will take off 2 points from your grade if your name isn’t in the test file name.

Grade \_\_\_\_\_\_\_\_

1. What is a collection of low-level subroutines that communicate directly with hardware devices?
   1. CPU
   2. BIOS
   3. DRAM
   4. CACHE
2. What is the decimal representation of each of the following unsigned binary integers?
   1. 00110101 \_\_\_\_\_\_\_\_\_\_\_\_53\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   2. 10010110 \_\_\_\_\_\_\_\_\_\_\_\_\_150\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   3. 11001100 \_\_\_\_\_\_\_\_\_\_\_\_\_\_204\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. If you XOR the following two binary numbers, what is the result?
   1. 11110101
   2. 00101001
   3. \_\_\_11011100\_\_\_
4. Little endian order is when the least significant byte is stored
   1. At the first memory address allocated for data
   2. At the last memory address allocated for data
5. A variable containing the address of another variable is called a \_\_\_\_Pointer\_\_.
6. What do AH, AL, BH, BL, CH, CL, DH, DL have in common?
   1. They are commonly-used memory locations
   2. They are part of the instruction set
   3. They are 8-bit general-purpose registers
   4. They are 16-bit general-purpose registers
7. In the code snippet below, first fill in the values of ax, and then explain why you can’t use INC to get esi to point to the next value in the array.

.data

ArrayW WORD 1000h,2000Hh,3000h

.code

MOV esi,OFFSET ArrayW

MOV ax,[esi] ; ax = 1000h

ADD esi,21000h

MOV ax,[esi] ; ax = 2000h

ADD esi,2

MOV ax,[esi] ; ax = 3000h

1. What would happen if the RET instruction was omitted in a subroutine?

Without the “Return” instruction, the concept of control flow would no longer function. When you execute the RET instruction you essentially exit the routine and return to a place in the program it was called. This prevents the computer from just executing code is next in the memory but returns to a position that might store a more deterministic plan for code execution.

1. Name at least 4 CPU status flags.

The Parity flag: Error detection

The Overflow flag

The Zero flag

The Carry flag

1. If you are programming a dice game, how many regions do you divide up the results of your random number generator to produce a fair game?

From Probability and Statistics class: The law of equally likely outcomes says you give equal probability to each possibly outcome. A dice has 6 potential outcomes when purposed represent a probability. Therefore you divide the regions 6 times.

1. In order to achieve the intersection of two sets, the bits must be

a. ANDed c. ORed

b. XORed

TRUE/FALSE QUESTIONS:

1. \_\_T\_\_ EPROM can be erased slowly with ultra-violet light and then reprogrammed.
2. \_\_T\_\_ CMOS RAM on the system motherboard stores system setup information. It is refreshed by a battery, so its contents are retained when the computer’s power is off.
3. \_\_\_T\_\_ The **principle of least astonishment** (**POLA**), sometimes also referred to as *Principle of Least Surprise*, applies to user interface and software design, from the ergonomics standpoint.
4. \_\_T\_\_ If you allow critical and non-critical modules to use the same programming resources, there is a very real possibility of some error in the non-critical code which will adversely affect the critical code.
5. \_\_T\_\_ Explicitly stating an array’s size can lead to a programming error, particularly if you should later insert or remove array elements.

17.\_\_T\_\_ Stacks are LIFO structures, ie, (last-in ,first-out).

18. \_\_F\_\_ The LENGTHOF operator counts the number of elements in an array.

19. \_\_T\_\_ The SIZEOF operator multiplies the number of elements by the size of the elements.

20.\_\_F\_\_ JMP is a conditional transfer operation.

21. \_\_T\_\_ Before you use the LOOP instruction, you must be aware of how it uses the counter.

22. \_\_T\_\_ The LOOP instruction first checks to see whether ECX is not equal to zero; then LOOP decrements ECX and jumps to the destination label.

23. \_\_F\_\_ The run-time stack is handled by the BIOS.

24.\_\_T\_\_ The program counter is a pointer to the instruction.

25.\_\_F\_\_ Program labels aren’t necessary to assembled code because the offsets are part of the instruction.

26.\_\_F\_\_ HRNG uses computational algorithms that can produce long sequences of apparently random results, which are completely determined by a shorter initial value, known as a seed value or key.

27. \_\_F\_\_ The INC instruction will increase by the value required, that is, if you are stepping through an array of bytes, INC will add 1 (for 8 bits), add 2 for 16 bits, etc.

28. \_\_F\_\_ correlation is causation.

29.\_\_T\_\_ If using AND or OR, for example, the two operands must be the same size.

30. \_\_F\_\_ Assembly language directives execute at runtime.

**ESSAY QUESTION:**

Dallas Morning News, November 22, 2009

“STOLEN CLIMATE INFO, E-MAILS LAUNCH WARMING DEBATE

London--Computer hackers have broken into a server at a well-respected climate change research center in Britain and posted hundreds of private e-mails and documents online--stoking debate over whether some scientists have overstated the case for man-made climate change.

The University of East Anglia, in eastern England, said in a prepared statement Saturday that the hackers had entered the server and stolen data at its Climatic Research Unit, a leading global research center on climate change. The university said police are investigating the theft of the information but could not confirm if all the materials posted online are genuine.

More than a decade of correspondence between leading British and U.S. scientists is included in about 1,000 e-mails and 3,000 documents posted on Web sites following the security breach last week.

Some climate change skeptics and bloggers claim that the information shows that scientists have overstated the case for global warming, and allege the documents contain proof that some researchers have attempted to manipulate data.

The furor over the leaked data comes weeks before the U.N. climate conference in Copenhagen, when 192 nations will seek to reach an agreement to reduce emissions of carbon dioxide and other heat-trapping greenhouse gases.

In one leaked e-mail, the research center’s director, Phil Jones, writes to colleagues about graphs showing climate statistics over the last millennium. He alludes to a technique--a “trick”--used by a fellow scientist to “hide the decline” in recent global temperatures.

Some evidence appears to show a halt in a rise of global temperatures from about 1960, but it is contradicted by other evidence that appears to show that a rise in temperatures is continuing.

The use of the word “trick” by Jones has been seized on by skeptics, who say his e-mail offers proof of collusion between scientists to distort evidence to support their assertion that human activity is influencing climate change.

However, Jones denied manipulating evidence and insisted his comment had been taken out of context.

The University of East Anglia said that the information published on the Internet had been selected deliberately to undermine “the strong consensus that human activity is affecting the world’s climate in ways that are potentially dangerous.””

The hackers’ actions are clearly illegal. Are they also immoral? Does the morality, or lack thereof, of the hackers depend on whether they have exposed a huge hoax? How can we be protected from scientists who manipulate data and outcomes to suit the scientists’ own opinions and vested interests? Do we need oversight of research if countries are going to formulate laws based on that research?

To address hacking, I think it's important to consider its original emergence and when it first became illegal. The original laws around hacking were established broadly, perhaps with the interest of creating a barrier between what might constitute as ethical versus something that might be blatantly wrong and possibly harmful. In a perfect world, hacking would be considered wrongful in any circumstance. However, too often we hear about small parties taking stances in their countries to try to turn tides for something that is actually morally correct, but they are forced to take a path that the country deems illegal. This easily allows the powerful to paint a bad picture of the less powered. It's disappointing that people have had to resort to the extremes of hacking to attempt to prove something because the company or in this case the research facility wasn't providing enough trustworthy information/arguments.

Sure, you can label hackers as immoral and argue against their wrongdoings, but you fail to realize the sequence of events that may have led them there. Hackers are valuable individuals, often employed by companies to strengthen their defenses. As individuals, they likely allocate much of their resources and time to building infrastructures against other hackers or identifying flaws. To attract the attention of hackers, you must already be on a slippery slope with a good majority of people, invalidating trust, taking distasteful actions, avoiding confrontation, and so on. Essentially, you are giving hackers a reason to target you. Although many would agree that it is wrong for your intellectual property to undergo unsolicited investigation, I think there should be a better legal middle ground that prevents the extreme case of hacking required by the opposing party.

As we enter this new era of information technology, we are still learning through trial and error how society will adopt the use of massive computation and public access to internet lines and tech establishments that store data while providing useful services. We obviously don't want Amazon to disappear because we would lose our convenient shopping platform, but we do want the assurance that our data will not be shared or sold without our consent. This requires a new middle ground where neither party has to lie to meet each other's needs. A constructive dialogue should be allowed, where no one feels suspicious activity is taking place, but the public is comfortable with embracing what the company has to offer. Some people might be okay with a portion of their generated data being used for feature enhancement, bug fixes, or anonymous census data gathering, but this is a topic that both parties should discuss without debate.

Parallel to a scientific institution being convicted of manipulating data to deceive the public due to potential political ties, the consequence of transparency arises. The details may prove their guilt, showing an attempt to sway the masses, or prove their innocence, resulting in no punishment. In the end, the hackers get hurt either way because they engaged in illegal activities, regardless of whether they uncovered something negative. This flaw in society is evident. Hackers should not have had a reason to intervene. If you are genuinely trying to positively impact society, the public should feel your impact, understand and support your progress, and stand united with you. Science has proven successful throughout history because it has been "open-sourced" and peer-reviewed, much like our modern-day programmable technology that we use so often. If the scientific research is beneficial to humanity, it should be conducted publicly, allowing a significant portion of humanity to contribute, rather than being hidden where only hackers have the resources to extract information. It should have been public from the start.

I don't want to see laws created specifically for research. Generally, laws are created when someone has already done something wrong, and we have to apply another rule as a band-aid to redirect and prevent similar actions. There are many laws we haven't created because there may simply be no consensus on certain matters. This issue arises when the public doesn't trust an institution, indicating a lack of agreement between the two parties. Instead of resorting to creating laws, I believe it would be more productive to find a standard, such as transparency, and engage in discussions about whether science should impact politics or vice versa. Addressing public concerns and working towards a mutual understanding and agreement would be more effective than allowing the situation to stagnate.

It is crucial for society to establish a framework where trust is fostered, both in institutions and among the public. This can be achieved through open communication, shared information, and collaborative decision-making processes. By striving for transparency and inclusivity, we can create an environment where hacking becomes unnecessary and the need for extreme measures is minimized.