Aman Patel

INFO-I 101

Nina Onesti

December 8, 2018

I101 Final Reflection

INFO-I 101 is a course offered to undergraduate students at Indiana University that aims to provide students with a broad introduction to a variety of topics in informatics. Some topics that were especially intriguing to me were the Cybersecurity and Bits & Bytes lectures. My semester of I101 is almost over, and the following paragraphs will describe what I’ve learned during this semester.

Although we learned about many interesting topics in lecture, the lecture pertaining to cybersecurity was the most interesting to me. This lecture was given by Matt Hottell, a Senior Lecturer in Informatics at Indiana University. He began by discussing the three main principles of information security: confidentiality, integrity, and availability. Confidentiality deals with accessing information without proper authorization, integrity deals with the unauthorized alteration of data, and availability deals with authorized users being prevented from accessing information when needed due to an external attack. He then discussed the three main components of risk: threat, vulnerability, and cost. Threat deals with the frequency of an adverse event, vulnerability is the probability that an attack is effective, and the cost is the potential impact of a threat (Hottell). The lecture then turned to cryptography or the science of secret messages. Matt outlined two commonly used methods of encryption: transposition and substitution. Transposition involves rearranging the characters of the original phrase and substitution involves swapping each character with another. He then introduced the rail fence cipher, which is a type of transposition cipher. A rail fence cipher uses two or more rows, or rails, to rearrange a message. The message is written out one character at a time from top to bottom, shifting by one column every time the number of rails is reached. This produces rails of a seemingly random sequence of characters, and the rails are combined from top to bottom to create the encrypted message (Rodriguez-Clark). Matt then introduced the Julius Caesar cipher, which is a type of substitution cipher. The Julius Caesar cipher swaps each letter in a message with the letter three steps after it (Tyson). For example, the message “I went to the store” would be encrypted as “L zhqw wr wkh vwruh.” Although this can be decrypted using brute force, the process can be expedited if both parties know the key, or what was used to encrypt the message. This is known as symmetric key encryption because both parties are using the same key. However, using an asymmetric encryption scheme as proposed by Whit Diffie would make it much more difficult for outside sources to access the message as it’s being transferred. In RSA, a type of asymmetric encryption scheme, each device has a public and private key. Messages are encrypted using the recipient’s public key and decrypted using their private key (Gupta). If the private key is kept secret, no one can decrypt the message except the intended recipient.

I found the cybersecurity lecture interesting because it included a section on cryptography, which has always been interesting to me. I love solving puzzles, and cryptography is essentially creating and solving puzzles to convey a message. I was first introduced to cryptography in 8th-grade math when my teacher would give a set of logic puzzles each week for extra credit. One week’s set of problems was about cryptography, particularly keyword ciphers. Other than this, I haven’t explored cryptography, but I would like to learn a few more encryption methods in the future.

Another lecture I thought was interesting was the Bits & Bytes lecture. I liked this lecture because it detailed the history and evolution of computers. This topic is intriguing to me because computers began as mechanical machines that occupied entire buildings and have now become digital machines that can fit in your pocket. I also found it interesting that the term “bug” was coined by Grace Hopper because a moth flew into Mark II, one of the first electromechanical computers (Onesti). I think the topic that was the most challenging for me was distinguishing between UX and UI designers. I now know that UX designers are focused on the functionality of an object while UI designers are focused on the interface, or how the user interacts with the object. Looking back, it’s not a very difficult concept, but it was difficult for me to grasp at the time. Before taking I101, I was aware that computers and technology could be applied to a lot of the things we do and use in our everyday lives. However, after taking I101, I learned that technology is already used in a lot more ways and places than I initially thought. For example, I have learned that there are so many devices connected to the Internet that a new IP address system had to be created to accommodate for every device.

I enjoyed my time in INFO-I 101, as it gave me a basic understanding of a variety of topics in computer science and informatics. Learning about cybersecurity and the history and evolution of computers was very interesting, along with many other topics we discussed during the semester. I would recommend this course to anyone who is interested in computer science and/or informatics and anyone who isn’t sure about what they want to pursue as a career.

Works Cited

1. Gupta, Mohit. “RSA Algorithm in Cryptography.” *GeeksforGeeks*, 6 Sept. 2018, [www.geeksforgeeks.org/rsa-algorithm-cryptography/](http://www.geeksforgeeks.org/rsa-algorithm-cryptography/).
2. Hottell, Matt. “Dimensions of Informatics and Computing: Cyber-security” Canvas, iu.instructure.com/courses/1739118/files/folder/Lecture%20Slides?preview=84917292.
3. Onesti, Nina. “Bits & Bytes” Canvas, iu.instructure.com/courses/1739118/files/folder/Lecture%20Slides?preview=82743624.
4. Rodriguez-Clark, Daniel. “Rail Fence Cipher.” *Crypto Corner*, crypto.interactive-maths.com/rail-fence-cipher.html.
5. Tyson, Jeff. “How Encryption Works.” HowStuffWorks, HowStuffWorks, 6 Apr. 2001, computer.howstuffworks.com/encryption2.htm.