+Will Gillette

Dr. Mongan

CS-471: CS Pedagogy

21 September 2023

Cryptography: Refactored into Understanding by Design

Grant Wiggins created the Understanding by Design (UbD) model to reform the classroom, pushing instructors to introduce new activities that ultimately enhance the learning and understanding of their students. Wiggins emphasizes that, “it’s your job to know where you want to end up,” encouraging teachers to be more methodical when developing their curriculum and syllabi. Essentially, goals and assessments are crucial in determining each student’s level of understanding and additionally each instructor’s competence as a teacher. By backtracking from goals, instructors become increasingly organized, ensuring that each of their lessons targets specific areas. On the contrary, without concise goals, lectures have the potential to become confusing for both instructors and students, leaving students wondering about the major takeaway from each lesson. By promoting critical and creative thinking, teachers transition away from “knowledge” and push towards “understanding,” enabling students to apply their learning to their own fields. Ultimately, this causes students to become self-sufficient, as they feel comfortable enough to connect ideas and use their understanding to craft their own original invention. By integrating UbD, instructors unknowingly develop an “agile methodology” within the minds of their students as opposed to, formerly, a “waterfall methodology,” resulting in many successful students from various knowledge backgrounds.

Dr. Mongan integrates many concepts of UbD into his lectures, particularly granting his students the freedom to brainstorm their own ideas that relate to the respective topic. This promotion of critical thinking has allowed me to flourish as a computer science student at Ursinus, as professors push me to submit my own projects that incorporate the learning goals of the given course. Furthermore, having practiced this independence during my undergraduate years, I feel significantly more confident progressing into either the workforce or graduate's school, as I know that I am adequately prepared for those future endeavors. On the other hand, there have been a few experiences in different courses where I have felt that learning goals were unclear or not established, making it tough for me to understand the central ideas of the course. Ultimately, the Understanding by Design framework has enabled me to accumulate so much knowledge and understanding since I began my career at Ursinus.

As per my lightning talk, I became aware of some flaws in my initial presentation. For instance, I assumed some prior knowledge about cryptography, explaining about public and private keys without fully considering that some students in this course do not have a strong computer science background. In my revision, I hope to define my goals, such that students will understand the advantages and disadvantages of using both the Caesar cipher and random substitution cryptographic methods and become comfortable with applying these methods so that they may encrypt their own messages. When explaining the goals and applications of cryptography, I hope to produce practical examples, such as how this was frequently used during World War 2 for countries to allow only certain parties to understand their communications. By pushing away from computer science applications immediately, I hope to enhance the understanding of my students and avoid intimidating them in any capacity. To assess the understanding of the students, I plan to have them decrypt a message that was encrypted via the

Caesar Cipher method using a shift of seven. Following their success, they will then have to encrypt this message again using random substitution. To do this, students will utilize the Frequency Analysis Widget on code.org, allowing them to decode and encode messages less tediously. I hope this tool will help my lecture run efficiently and keep students engaged. For a post-lesson activity, I plan to have students encode and decode their own messages with their peers, submitting the original and encoded messages and indicating which cryptographic method they used and explaining why, targeting the top levels of Bloom's taxonomy. Ultimately, my perspective for learning has shifted after learning about Wiggin's UbD framework, and I hope to be more inclusive by targeting a broader audience comprising of students from various knowledge backgrounds as opposed to only those with prior knowledge.