Cyber Security Lesson Plan

Lesson Title: Analyzing & Developing Encryption Systems
Grade Level: 11th & 12th grade

Summary: In this lesson, students will analyze the Caesar cipher to determine what makes an effective/ineffective encryption, then design their own based on their analysis.

Learning Objectives/Outcomes:
9-12.CY.3 Explain specific trade-offs when selecting and implementing security recommendations

Learning Type: Project

Materials List: Raspberry Pi (or other computer for coding); blank paper or poster paper (for the planning process)

How will you facilitate learning?
Warm up/discussion; focused activity; reflection

Accommodations: predetermined heterogenous pairs; written & verbal directions, etc.

Description of Activity:

- Warm Up: Students discuss the pros/cons of using the Caesar cipher (from previous 1-2 lessons) and in general, what makes a good encryption method
- Students work in pairs to create their own encryption method. Students write out their example on paper at this stage and convert "passwords" into the encrypted versions.
- Students test their method by giving another pair of students one of their encrypted "passwords" to see if they can crack their code.
- Once students are happy with their method, they write the code of their method in Python - for encryption and decryption.
- Students submit, via Google Classroom, the reasons why their encryption method is effective or ineffective as well as their code.
- Students share their methods with the rest of the class and also discuss the analysis submitted to Google Classroom. (Students will use their personal encryption method in subsequent lessons by creating a login system that utilizes some of the physical components of the Raspberry Pi - buzzer sounds and camera activates if the wrong password is typed in, etc.)