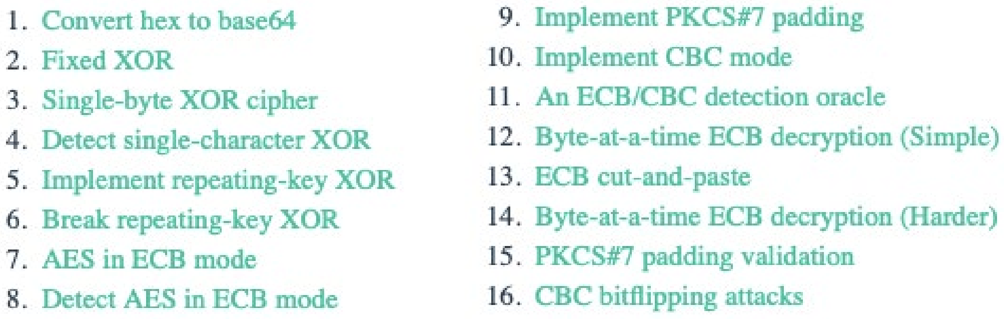
ECEN 5773 Developing the Industrial Internet of Things
Hands on with Security

Description

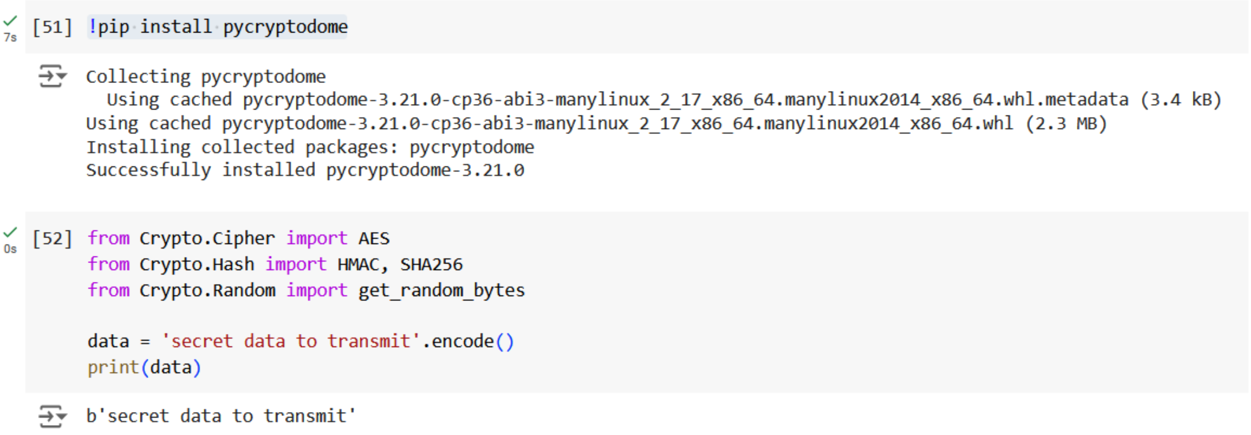
The purpose of this assignment is to give you hands-on experience with security. Think of this as an independent study assignment. You can choose from the following list of 3 topics to explore:

The first choice (Option 1) is CryptoPals, see: http://cryptopals.com/. This site presents a series cryptographic challenges. You will write programs for each of the challenges. You can code your solutions to each challenge in any language you choose. I recommend python. See the python cryptographic library: https://pypi.org/project/pycrypto/ which makes developing the code for these challenges much easier. I believe pycryptodome is more up to date as of 3/7/2022: https://pypi.org/project/pycryptodome/ - you can use any python crypto library in your solutions. You decide how many sets of these challenges you perform. At the time of this writing there are 8 sets of challenges. **To get credit for this choice** you must complete Set 1 (Basics) and Set 2 (Block crypto). If you choose to complete additional sets, that is your option. In terms of hands-on experience with security, this first choice is ideal. The two sets are:



1. Convert hex to base64
2. Fixed XOR
3. Single-byte XOR cipher
4. Detect single-character XOR
5. Implement repeating-key XOR
6. Break repeating-key XOR
7. AES in ECB mode
8. Detect AES in ECB mode
9. Implement PKCS#7 padding
10. Implement CBC mode
11. An ECB/CBC detection oracle
12. Byte-at-a-time ECB decryption (Simple)
13. ECB cut-and-paste
14. Byte-at-a-time ECB decryption (Harder)
15. PKCS#7 padding validation
16. CBC bitflipping attacks

Note: if you wish to do this in google colab, you can create a cell with a line that has the pip install command, and put an exclamation point in front of it. e.g.:



```
[51] !pip install pycryptodome
```

```
Collecting pycryptodome
  Using cached pycryptodome-3.21.0-cp36-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (3.4 kB)
Using cached pycryptodome-3.21.0-cp36-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (2.3 MB)
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.21.0
```

```
[52] from Crypto.Cipher import AES
     from Crypto.Hash import HMAC, SHA256
     from Crypto.Random import get_random_bytes

     data = 'secret data to transmit'.encode()
     print(data)
```

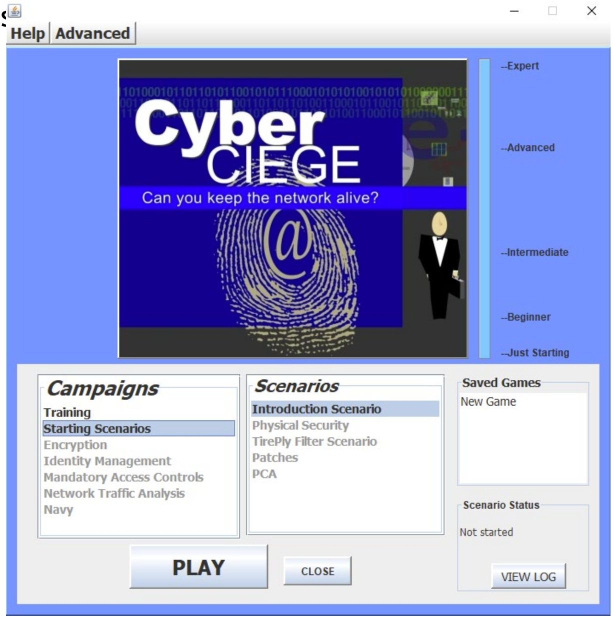
```
b'secret data to transmit'
```

Note: There’s a nice series on youtube that is effectively a walkthrough of the solutions for these. Try to solve things on your own. If you don’t understand the problem being asked, watch the first part of the video. If you still are stumped, watch the whole thing, but implement it yourself (and take note in your writeup what you did for each problem).

https://www.youtube.com/watch?v=Yg1ZWegeZiM&list=PLWvDpnCcem1P6i8pZm2x7KHp5iaxwrK_P

The second choice (Option 2) is a game called CyberCiege. The game was developed by the US Naval Postgraduate School. You can download the latest version here: http://my.nps.edu/web/c3o/latestv. The installer will ask for a password. The password is **grostolis**. There is a notional syllabus here: http://my.nps.edu/web/c3o/syllabus. There is a support page here: http://www.c3o.nps.edu/cyberciege/support.html. After installation to play the game, open the CyberCIEGE icon, which will start the "Campaign Player". Then select "Game Help and Getting Started" from the menu and follow the suggested steps (including a brief movie) to become familiar with the tool. Most scenarios include Lab Manuals to help guide players through the game. You decide how many of these labs you perform. **Note**: I could not get this game to run on my Windows 11 Dell machine.

Your results may vary. One student shared with this trick: Run the application in Administrator mode. However, many students have been successful running the game on a Windows 10 machine. **To get credit for this choice** you must proceed past the Training Campaign (Stop Worms, Life with Macros, Identity Theft, Passwords) **and at a minimum complete the Starting Scenarios Campaign** (Introduction Scenario, Physical Security, TirePly Filter Scenario, Patches



As an alternate to Option 2 CyberCiege, but in a similar spirit, you can explore labs from SEED Labs 2.0
https://seedsecuritylabs.org/Labs_20.04/

To get credit, you need to complete at least 2 total labs, selected from at least 2 different categories. I have not completed any of these, but I have read the instructions for a few and they look solid. I can't speak to the time estimation accuracy. If you find you are completing 2 labs in under 4 hours, add a third lab. For the write up, you are being asked how much time you spent.

The third choice (Option 3) is to strike out on our own self-study. Here is one idea: Review presentations and papers from Black Hat (https://www.blackhat.com) and/or DefCon (https://www.defcon.org/index.html). Others are listed at:
https://www.tripwire.com/state-of-security/top-information-security-conferences
See also: https://www.nist.gov/itl/applied-cybersecurity/nice

To get credit for this choice you must read at least 3 papers on one specific topic, that ideally relates to something we discussed in lecture.

The assignment:

Make a selection from one of the options above. Spend time exploring that option. Explore, tinker, experiment, read, learn. Write a 5 to 6 page paper (5 or 6 pages of text, not including figures etc.), 12 point font, single spaced. The length can be extended beyond 5 to 6 pages to include code, figures, pictures and diagrams. However, the total length of the paper shall remain under 12 pages, including the title page. You can include some code snippets, if that is applicable, but you do not have to submit all of your code. In this paper write about:

- What you did (which option you chose: 1, 2 or 3)
- How many hours you spent
- What you learned
- How what you learned in class reinforced, or not, what you learned in this assignment

Remember to include your **name** and the **number of hours you spent**. Don't assume your reader (me) has familiarity with the protocols, terminology and acronyms used in your sources. This is an opportunity for you to explain these things. The grading rubrics are intentionally not defined. I'm looking to you to impress me; teach me something new or something I don't know. Think of this assignment as an independent study.

Format of your paper: Start with the provided template.

To submit for grading: A single PDF file of your paper that contains all of the content of your paper. If you submit your paper in any other format, you will receive 0 points.

Note: It is super important to do your own writing. You will find that in your professional life you will do a great deal of technical writing as an engineer. Citing up to 10 or less web resources or on-line papers is fine for this assignment, but you must indicate your citations as other people's work. See the paper template provided to you to use as a starting point for your paper. Points may be taken off for any un-cited web references.

Also note: The CryptoPals option, although valuable in giving you excellent hands-on experience with security (validated over and over again by past students), is also the most time demanding. So plan your time management appropriately.