Assignment 2

- This is a programming assignment. Please upload your scripts/code via the course webpage.
- The deadline for submission is October 11th, 8:00 (then -3 points per each started 24h). Remark: This is 24 hours more than normal to amortize for a longer time for the first assignment.
- Please name the submission file as <uco_number>_hw2.zip. Put there both the python code and the openssl commands (e.g., in the readme file). If you have more files pack them together to the zip file.
- The code must contain comments so that it is reasonably easy to understand how to run the script for evaluating each answer.

Assignment 2 - Tasks

1. Use the openssl command tool to encrypt alice.txt with AES128 in OFB mode (with cryptographically secure IV and key). Do the same (with the same key and IV) using the python cryptography library (like in Assignment 1). Give the two outputs in two different files and attach them to your solution. Also, attach the openssl command that you used.
   Remark: make sure that your code would work for large files. **[3 points]**
2. Test that step 1 works fine with openssl (for decryption). Attach the command to your solution. **[1.5 point]**
3. Suppose you are a trusted CA and you receive Bob's CSR. Write a python script to generate Bob's certificate. Write a script that checks that the certificate and the key match. **[3 points]**
4. Suppose Alice wants to verify Bob's certificate issued by you (from step 3). Write a python function that verifies the validity of Bob's certificate. Your function must raise an error in case the certificate is not issued by you. The function should be executed by the main code (no need to include testing the negative path). **[2.5 points]**
5. **Extra (bonus):**
   Generate and send me an email (lukchmiel@gmail.com) encrypted with my public key and signed with your private key.
   For the sake of simplicity, I posted the public key in the study materials for the seminar (Lukasz Chmielewski lukchmiel@gmail.com-(0xF077D43514C58924)-public.asc).
   Make sure that I can learn your public key (e.g., attach it to the email).
   Describe briefly how you performed Step 5 in the email. **[1 point]**
   Note: do not use keys generated by third parties (e.g., websites)

Good luck!!!