CS 528 Data Privacy and Security
Homework 2
Due Tuesday, 04/09/2019 (11:59 PM)

Name: **CWID:**

Part I (50 points). Alice holds a private matrix A (nonnegative integer entries) with size 5×8 while Bob holds a private matrix B (nonnegative integer entries) with size 8×4. Design and implement a two-party protocol to securely compute the product $A \times B$. Hint: Homomorphic Encryption (e.g., Paillier Cryptosystem which is asymmetric) can be used to design the protocol.

- Paillier in Python:

  https://python-paillier.readthedocs.io/en/develop/

  https://github.com/mikeivanov/paillier

- Paillier in Java:

  https://www.csee.umbc.edu/ kunliu1/research/Paillier.html

Tasks include:

1. Alice generates random nonnegative integer entries for A while Bob generates random nonnegative integer entries for B
2. Design the protocol between Alice and Bob to perform secure computation
3. Write the programs for Alice and Bob: communication should be established to exchange encrypted messages, e.g., using Socket programming
4. Report the input matrices, the last ciphertext (right before the decryption) and the decrypted product $A \times B$ using two different key sizes 512-bit and 1024-bit

Submission includes source code files and txt file for the results: all named with the prefix "hw2-I-" (e.g., *hw2-I-alice.java*).

Part II (50 points). Alice holds a private Boolean vector $\vec{A}$ with 10 Boolean entries ({0,1}) while Bob holds another private Boolean vector $\vec{B}$ with another 10 Boolean entries ({0,1}). Design and implement a protocol using the *Fairplay* to securely compute the scalar product $\vec{A} \cdot \vec{B}$ without sharing their inputs. Hint: the scalar product computation should be converted to garbled circuits using SFDL. *Fairplay* secure function evaluation: https://www.cs.huji.ac.il/project/Fairplay/.

Tasks include:

1. Alice generates random Boolean entries for $\vec{A}$ while Bob generates random Boolean entries for $\vec{B}$
2. Write the SFDL program for Alice and Bob, compile it for Alice and Bob, and run the protocol (communication is integrated in *Fairplay*).
3. Report the input Boolean vectors, the SFDL program, SHDL circuit and output result $\vec{A} \cdot \vec{B}$.
4. Readme file for running *Fairplay* SFE:

   https://www.cs.huji.ac.il/project/Fairplay/Fairplay/Readme.txt

Submission includes input vectors, source code files, SDFL program, SHDL circuit and output result: all named with the prefix "hw2-II-" (e.g., *hw2-II-scalarsdfl.txt*).

You can include a PDF report to capture some screenshots for the protocol demonstration for both Part I and II.