Introduction to FinTech
Assignment for Bitcoin/Blockchain

★ Welcome to the Exciting World of Cryptocurrency! In this assignment, you'll embark on a journey to explore the fascinating technical foundation behind Bitcoin and blockchain. Get ready to dive deep into the world of cryptography and understand how these groundbreaking technologies work at their core.

Using the elliptic curve **secp256k1**, the same one employed by Bitcoin and Ethereum, you'll learn to work with fundamental concepts like elliptic curve arithmetic and the base point **G** defined in the standard. This is your chance to connect theory with real-world applications in the cryptocurrency ecosystem.

Don't worry if it feels complex at first; think of this as a puzzle waiting to be solved! Tackle the challenges step by step, experiment, and let your curiosity guide you. By the end, you'll not only deepen your understanding but also gain confidence in handling advanced cryptographic tools. Have fun, and enjoy it!

The assignment package contains the following files:

1. **Assignment4.pdf**: This Assignment specification.
2. **main.py**: The testing framework for your reference only.
3. **mySubmission.py**: The *ONLY* file you need to submit to the gradescope for grading. You are not allowed to import any additional package, or you will receive "0" grade for this assignment.

Assignment Details:

Please read this paragraph carefully. It can save you tremendous time on this Assignment.

1. main.py is the main framework TA used for reference only. You don't need to submit this file to gradescope.
2. You can browse how we grade your submission on each Problem through ***main.py***. Then, you can start to complete each corresponding function in ***mySubmission.py***. This assignment is supposed to be completed by simply completing the predefined function body without designing any additional functions.
3. You are encouraged to utilize TA hour to help you initialize your assignment. The TA, Wen Hsiao, who has office hours at 1pm on Friday is responsible for this assignment.
4. TA has the responsibility to help you clarify the understanding of the assignment, and coach you to learn all necessary concepts on solving this assignment. TA has NO responsibility to assist you on the debugging of your assignment.

The Problem Set (105%):

Problem 0. (2%, realtime grading) Find the correct base point used in Bitcoin's public-key cryptography. Hint: See reference hints in code

Problem 1. (2%, realtime grading) Evaluate $4G$. Hint: Lecture slide p14

Problem 2. (2%, realtime grading) Evaluate $5G$. Hint: Lecture slide p14

Problem 3. (9%, realtime grading) Evaluate $Q = dG$.

Problem 4. (20%, post-grading with hidden data) Write a standard Double-and-Add algorithm mentioned during the class for scalar multiplications, and return the scalar multiplication result, and the number of doubles used and the number of additions used respectively when evaluating Q? Hint: Lecture slide p16

Problem 5. (40%, post-grading with hidden data) Note that it is effortless to find $-P$ from any P on a curve. If the addition of an inverse point is allowed, try your best to evaluate dG as fast as possible. Then, use the optimized Double-and-Add algorithm to compute arbitrary scalar multiplications. Hint: $31P = 2(2(2(2(2P)))) - P$.

Problem 6. (15%, post-grading with hidden data) Sign given Bitcoin transactions with a random number k and your private key. Hint: Lecture slide p31

Problem 7. (15%, post-grading with hidden data) Verify a given digital signature with your public key. Hint: Lecture slide p32

========== END OF ASSIGNMENT ==========