Introduction to FinTech   Assignment for Bitcoin/Blockchain

- Use the elliptic curve "secp256k1" as Bitcoin and Ethereum. Let G be the base point in the standard. Let d be the last 6 digits of your student ID number.

1. Evaluate $4G$.

2. Evaluate $5G$.

3. Evaluate $Q = dG$.

4. With standard Double-and Add algorithm for scalar multiplications, how many doubles and additions respectively are required to evaluate dG?

5. 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. Hint: $31P = 2(2(2(2(2P)))) - P$.

6. Take a Bitcoin transaction as you wish. Sign the transaction with a random number k and your private key d.

7. Verify the digital signature with your public key Q.