MATH/CS 295: CRYPTOGRAPHY
HOMEWORK #12 ADDITIONAL PROBLEM

Problem 5.A*. Alice and Bob use a Diffie-Hellman exchange with the elliptic curve $E : y^2 = x^3 + 383$ over $\mathbb{F}_{2003}$ with $\#E(\mathbb{F}_{2003}) = 2004$ and the point $G = (977, 314)$. Alice sends Bob the point $(930, 937)$ and Bob sends Alice the point $(425, 1182)$. What is their common secret key? *[Hint: Use baby-step giant-step to solve an elliptic curve discrete logarithm problem.]*