CS 198 Codebreaking at Cal
Spring 2023 Makeup Assignment

Week 7

Question 1

Consider the group of invertible 2×2 matrices in $\mathbb{R}^{2\times 2}$, and the binary operation of matrix multiplication.

1. What is the identity element in this group?
2. For a matrix A, what is its inverse element in this group?

Now suppose we instead choose addition as our binary operation.

3. Now what is the identity element in the group?
4. For a matrix A, what is its inverse in this group?

Question 2

Alice and Bob are deriving a shared secret key using elliptic-curve Diffie-Hellman. They agree on a curve and a point P on this curve. Alice knows a secret number a, and Bob knows a secret number b. As a reminder, Alice sends aP, Bob sends bP, and they each derive the point abP.

Suppose Mallory wants to perform a man-in-the-middle attack that allows her to read and modify any message Alice and Bob send each other after the ECDH exchange without being detected. Mallory knows a secret value m.

1. Mallory intercepts Alice's message aP intended for Bob. What should she send Bob instead?
2. Mallory intercepts Bob's message bP intended for Alice. What should she send Alice instead?
3. What shared secret will Mallory and Alice derive?
4. What shared secret will Mallory and Bob derive?
5. Explain how when Alice sends a message M encrypted with the shared secret she derived, Mallory can both read its value and make Bob receive a modified message M'.

Hint: If you're not sure how to approach this, try finding a solution with modular arithmetic Diffie-Hellman, then convert it to ECDH.

Contributors:
- Ryan Cottone, Will Giorza