Cryptography
ECE 5632
Assignment 2
Spring 2025

Name:..... **ID:**.....

Problem 1

(a) Compute the Euler function $\phi(m)$ for $m = 256, 275, 252$

(b) Calculate $(AA)_{16} \times (BB)_{16}$ in $GF(2^8)$ using the AES irreducible polynomial.

Problem 2

Let $x =$ "*Right-most 4 decimal digits of your MSA ID*", Calculate the following:

(a) $\gcd(x, 1234)$ using the basic form of Euclid's algorithm.

(b) $x^{-2} \mod 2341$ using the extended Euclidean algorithm