# Cryptography
## ECE 5632
### Sheet 5

Spring 2024

## Problem 1

Compute the Euler function $\phi(m)$ for $m = 10, 11, 15, 18$, and 30.

## Problem 2

Let $x = 358703$ and $y = 611939$. Answer the following:

(a) Compute $\phi(27)$.

(b) Compute $y^{-2} \mod 17$.

(c) Is it possible to compute $x^{-1} \mod 27$? Why?

(d) If you know that both x and y are primes, what are $\phi(x)$ and $\phi(y)$?

## Problem 3

Using the basic form of Euclid's algorithm, compute the greatest common divisor of:

(a) 7469 and 2464

(b) 2689 and 4001

(c) 654321 and 123456

Show every iteration step in detail of Euclid's algorithm.

## Problem 4

Compute the inverse $a^{-1} \mod n$ with Fermat's Theorem (if applicable) or Euler's Theorem:

(a) $a = 4, n = 7$

(b) $a = 5, n = 12$

(c) $a = 6, n = 13$

## Problem 5

Using Fermat's theorem, find $3^{201} \mod 11$.

## Problem 6

Use Fermat's theorem to find a number $x$ between 0 and 36 with $x^{145}$ equivalent to 7 modulo 37.

## Problem 7

Using the extended Euclidean algorithm, find the multiplicative inverse of:

(a) $24140 \mod 40902$

(b) $550 \mod 1769$

## Problem 8

Using the following properties:
if $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$,
if p is prime, then $\phi(p^i) = p^i - p^{i-1}$ ,
if $p$ is prime, $\phi(p) = p - 1$,
Determine the following:

(a) $\phi(27)$

(b) $\phi(231)$

(c) $\phi(41)$

(d) $\phi(440)$