Homework 4

Required Reading Assignment

W. Stallings, "Cryptography and Network Security," 8/E or 7/E

Chapter 2.1 Divisibility and The Division Algorithm
Chapter 2.2 The Euclidean Algorithm
Chapter 2.3 Modular Arithmetic
Chapter 2.4 Prime Numbers
Chapter 3.2 Substitution Techniques.

A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography" (available for free at http://cacr.uwaterloo.ca/hac/)

Chapter 2.4.1 The integers (2.79-2.94)
Chapter 2.4.2 Algorithms in Z (2.103-2.109)
Chapter 2.4.3 The integers modulo n (2.110-2.119)
Chapter 2.4.4 Algorithms in Z_n (2.142)
Chapter 7.3 Classical ciphers and historical development.

Written Assignment

due by Tuesday, October 13, 11:59pm

(submission using Blackboard)

Problem 1

Find values of x and y fulfilling the equation

$$\gcd(a, n) = x * a + y * n$$

for the following values of a and n:

a) $\{a=546, n=1260\}$
b) $\{a=3289, n=4199\}$

Problem 2

Find the private keys $\{d, P, Q\}$ corresponding to the following public keys in mini-RSA:

a) $\{e=3, N=799\}$
b) $\{e=3, N=1189\}$

Problem 3

Solve by hand the following four (separate) equations:

a) $455 \cdot x \equiv 231 \pmod{1386}$
b) $85 \cdot x \equiv 102 \pmod{1386}$
c) $1001 \cdot x \equiv 455 \pmod{1386}$
d) $585 \cdot x \equiv 126 \pmod{1386}$

For each equation, find **all** values of x in the range from 0 to 1385 for which the given equation holds.
Verify the obtained answers and include calculations used during your verification in your solutions.
Show your solutions graphically on a horizontal axis, with the positions of 0 and 1386 clearly marked.

Problem 3B – bonus

Using a high-level programming language of your choice, write a program for solving equations of the form $a \cdot x \equiv b \bmod n$.

The program should take as inputs a, b, and n, and return all solutions in the range $[0, n)$.

Demonstrate the correct operation of your program for all equations from Problem 3, and four additional examples of your choice.

Problem 4

Break the affine cipher (i.e., find the key K=(k1, k2)) based on the knowledge that

1. the least frequent letter of the ciphertext is 'P'
2. the second least frequent letter of the ciphertext is 'H'
3. the most frequent trigram is 'AJM'.

You cannot use any specialized computer program (other than a spreadsheet and a calculator), and your solution should be obtained by constructing and solving a system of linear equations in modular arithmetic.

Hint: Solve a system of linear equations based on the knowledge of points 1 and 2, and then verify that point 3 holds (i.e., the decryption of 'AJM' gives one of the most frequent trigrams).