

HW # 8

Due Date: Tuesday, November 14th, 2007, 7:20 PM
at the beginning of class

Reading Assignment:

- W. Stallings, *Cryptography and Network Security*, Chapter 9, Sections 8.1, 8.2, 8.3, 8.4
- A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography* Sections: 2.4.1, 2.4.3, 4.1, 4.2 (w/o 4.2.2), 4.4 (w/o 4.4.3, 4.4.4)

Recommended Additional Reading

- Please get familiar with The Prime Pages: prime number research, records, and resources by Chris Caldwell
- Presentation Generating strong prime numbers using probabilistic tests for primality, developed by Dong Wan Han as a part of the project for a previous edition of this course.

Problems:

1. (10 points) Verify that Euler's theorem holds in Z_m , $m = 7, 10$ for all elements a for which $\gcd(a, m) = 1$. Also verify that the theorem does not hold for elements a for which $\gcd(a, m) \neq 1$.
2. (5 points) For the affine cipher the multiplicative inverse of an element modulo 26 can be found as

$$a^{-1} \equiv a^{11} \pmod{26}$$

Derive this relationship by using Euler's theorem.

3. (20 points) Write a C program which realizes the extended form of Euclid's algorithm. The following features must be supported:
 - (a) The program should ask the user to enter r_0 and r_1 and write the return $s, t, \gcd(r_0, r_1)$ on the screen.
 - (b) In the beginning of the program, check whether $r_0 > r_1$. Otherwise, swap the two values.

Provide a print out of the C program as well as a sample run with one input pair r_0, r_1 of your choice.

4. (20 points) Modify the program from above, to compute $\phi(m)$ according to its definition, i.e., without using the prime factorization of m , for

(a) $m = 13257$

(b) $m = 13681$

(c) $m = 1000019$

(d) $m = 1000003$

Which of the numbers m are primes?