Homework Assignment # 5

Due Date: Wednesday, October 11

0. Read the pages 394–399 from Kahn's "The Codebreakers", provided as copies in the class. These pages describe the invention of the automatic stream cipher by Vernam and the extension of it which lead to the one time pad.

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

   (a) 7469 and 2464,

   (b) 2689 and 4001,

   Use for this problem only a pocket calculator. Show every iteration step of Euclid's algorithm, i.e., don't write just the answer, which is only a number. Also, for every gcd, provide the chain $\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots$.

2. Using the extended Euclidean algorithm, compute the greatest common divisor and the parameters s, t, of

   (a) 198 and 243,

   (b) 1819 and 3587,

   For every problem check if $s\,r_0 + t\,r_1 = \gcd(r_0, r_1)$ is actually fulfilled. The rules are the same as above: use a pocket calculator and show what happens in every iteration step.

3. With the Euclidean algorithm we finally have an efficient algorithm for finding the multiplicative inverse in Z_m which is much better than exhaustive search. Find the inverses in Z_m of the following elements a modulo m:

   (a) $a = 7$, $m = 26$ (this inverse was needed in the first homework assignment for the affine cipher)

   (b) $a = 19$, $m = 999$

   Note that the inverses must again be elements in Z_m and that you can easily verify your answers.

4. Write a C program which realizes the extended form of Euclid's algorithm. Since we will need this program for subsequent homework assignments, the following features must be included:

   - Write the program as a single *function* which has r_0, r_1 as input parameters, and returns $s, t, \gcd(r_0, r_1)$.
   - In the beginning of the function, check whether $r_0 > r_1$. Otherwise, swap the two values.
   - The program must be able to perform all arithmetic with `long` type variables, i.e. 31 bit values. Make sure you call the program with `long` type variables if the magnitude of the input values is larger than $2^{15} - 1 = 32767$.
   - Write a user interface (e.g., in the `main` program) which asks the user for r_0, r_1 and returns $s, t, \gcd(r_0, r_1)$ after calling the function.

   (a) Compute s, t, and $\gcd(r_0, r_1)$ for $r_0 = 92204805, r_1 = 139928096$

   (b) Compute s, t, and $\gcd(r_0, r_1)$ for $r_0 = 123456789, r_1 = 987644322$

5. Determine $\phi(m)$, for $m = 12, 15, 26$, according to the definition: Check for each positive integer n smaller m whether $\gcd(n, m) = 1$. (You do *not* have to apply Euclid's algorithm.)

6. Develop formulae for $\phi(m)$ for the special cases when

   (a) m is a prime,

   (b) $m = p \cdot q$, where p and q are primes. This case is of great importance for the RSA cryptosystem. Verify your formula for $m = 15, 26$ with the results from the previous problem.

7. Using the program from problem 4, compute $\phi(m)$ according to its definition, i.e., without using the prime factorization of m, for

   (a) $m = 12111$

   (b) $m = 12553$

   (c) $m = 10000017$

   (d) $m = 10000019$

   Which of the numbers m are primes? (Warning: The last two numbers might take a while on slow PCs.)

8. Verify that Euler's theorem holds in Z_m, $m = 6, 9$, for all elements a for which $\gcd(a, m) = 1$. Also verify that the theorem does not hold for elements a for which $\gcd(a, m) \neq 1$.

9. For the affine cipher you were told that the multiplicative inverse of an element modulo 26 can be found as

$$a^{-1} \equiv a^{11} \bmod 26.$$

Derive this relationship by using Euler's theorem.

10. **(Optional Mathematical Problem, 10 extra points)** The extended Euclidean algorithm has the initial conditions $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$. *Derive* these conditions. It is probably helpful to look how the general iteration formula for the Euclidean algorithm was derived in the lecture.