Cryptology 2016: Assignments

Problem 1. Implement the Miller Rabin primality test. Your program should read a 256 bit number represented in hexadecimal format from a file and output either prime or composite. Your implementation should be able to test primality of a 256 bit number in reasonable time. You should not use any multi precision library for this implementation. The basic arithmetic operations for large integers which would be required should also be implemented.

Problem 2. Given a polynomial $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^{n-1}$, where $a_i \in \mathbb{F}_{2^{128}}$ and the addition and multiplications are also in the finite field $\mathbb{F}_{2^{128}}$, write a program to find $f(h)$ for a given $h \in \mathbb{F}_{2^{128}}$. The program should be written following the rules below.

- The computation would involve multiplications in the finite field $\mathbb{F}_{2^{128}}$. You should use $x^{128} + x^7 + x^2 + x + 1$ as the irreducible polynomial.
- The program should take as input a file with the following structure: The first entry would be the degree of the polynomial (say $n-1$) followed by n coefficients $a_0, a_1, \ldots, a_{n-1}$ which would be followed by the value of h (the point where the polynomial would be evaluated). All values except the degree of the polynomial would be represented in hexadecimal format. The program should output the value of $f(h)$ in hexadecimal format.
- The following reference:
  Shay Gueron and Michael Kounavis, Efficient implementation of the Galois Counter Mode using a carry-less multiplier and a fast reduction, Information Processing Letters 110(2010) 549-553
  may be useful for the implementation. In particular see section 4.2 and the Algorithm 2 for the reduction algorithm.
- Multiplications in the field $h \in \mathbb{F}_{2^{128}}$ can be easily done in modern intel processors with a special instruction called PCLMULQDQ. It is not necessary that you use this instruction for your implementation. But if you use it you will have less work to do. But for using it you need to write code using intel intrinsics, some resources related to this is give in the course webpage.

The deadline for the above two problems is January 5, 2017. You are required to show me your programs in your laptops in my office between 10:00 AM to 6:00 PM. If you do not have a laptop, then you have to show it in my machine, in that case your programs must compile with GCC in a Linux environment (preferably Ubuntu).