Cryptographic Engineering
Spring Term 2018

Homework Assignment 04:

1. Consider the exponent $d = 150 = (10010110)$. Show the steps and all intermediate powers in the computation of m^d for the algorithms:
   (a) the left-to-right binary method
   (b) the square-and-multiply-always algorithm
   (c) the Montgomery powering ladder
   (d) the Atomic square-and-multiply algorithm (Marc Joye Algorithm)

2. Consider the RSA key set

$$\{p, q, n, \phi(n), e, d\} = \{101, 103, 10403, 10200, 2017, 1153\} .$$

   Emulate (numerically) for computing $s = m^d \pmod{n}$ where $m = 100$ using each one of these countermeasure algorithms by selecting suitable random parameters:
   (a) Randomizing m, where e is known
   (b) Randomizing m, where e is unknown
   (c) Randomizing m, using a small r
   (d) Randomizing d, using a small r
   (e) Randomizing d, where $\phi(n)$ is unknown
   (f) Randomizing d, where e is unknown
   (g) Randomizing n, using small r_1 and r_2

3. For the above RSA key pair (in Problem 2), show the computation of $y = m^d \pmod{n}$ for $m = 999$ using the CRT method, and emulate the fault attack by showing that of there is an fault induced on mod p (or q) computations, an incorrect $\hat{y}$ value gives away the prime q (or p) using the GCD attack. When the fault is induced on mod p computation, the other prime factor q can be obtained using

$$\gcd((\hat{y}^e - m) \bmod n, n) = q$$