Cryptographic Engineering
Spring Term 2018

Homework Assignment 03:

1. Let $e = (11110000)$ be the exponent. Illustrate the addition chains produced by each one of the following algorithms and compute the length of each addition chain.
   (a) Factor method
   (b) Power tree method
   (c) Binary method
   (d) m-ary method for $d = 2$ and $d = 4$
   (e) NAF method for $w = 2$ and $w = 3$
2. Let $r = 64$, $n = 55$, $a = 12$, and $b = 15$. First compute $\bar{a}$ and $\bar{b}$, and then compute $\bar{c} = \text{MonPro}(\bar{a}, \bar{b})$ using the classical Montgomery multiplication algorithm. Illustrate the steps and give all temporary results.
3. Consider the field $\text{GF}(2^4)$ and the following two elements $a = (1101)$ and $b = (1011)$ in polynomial basis with the irreducible polynomial $p(\alpha) = \alpha^4 + \alpha + 1$.
   (a) Perform $c = a^2$ in polynomial basis and find c
   (b) Perform $d = a \cdot b$ in polynomial basis and find d
   (c) Find normal basis representations of a and b with the normal element $\beta = \alpha^3$
   (d) Perform $c = a^2$ in normal basis and find c
   (e) Perform $d = a \cdot b$ in normal basis and find d