T-79.5501 Cryptology
Midterm Exam 2
April 11, 2014

1. (6 pts) The sequence

   $S =$ **1 1 0 1 0 1 1 0 0 1 0 0 0 1 1 . . .**

   is generated using an LFSR with polynomial $f(x) = 1 + x^3 + x^4$. Find a polynomial $P(x)$ such that

   $$S(x) = \frac{P(x)}{f^*(x)}.$$

2. (6 pts) The number 332799499 is a nontrivial square root of 1 modulo 332860009. This modulus is a product of two primes. Find the two prime factors of 332860009.

3. (6 pts) The number $p = 257 = 2^{2^3} + 1$ is a Fermat prime. Determine the five least significant bits of x such that

   $$3^x \equiv 226 \pmod{257}$$

   using the Pohlig-Hellman algorithm.

   The task can be done by hand with the help of the following publicly computable information:

$\cdots$	$3^{-1} \bmod 257 = 86$	$\cdots$
$3^2 \bmod 257 = 9$	$3^{-2} \bmod 257 = 200$	$226^2 \bmod 257 = 190$
$3^4 \bmod 257 = 81$	$3^{-4} \bmod 257 = 165$	$226^4 \bmod 257 = 120$
$3^8 \bmod 257 = 136$	$3^{-8} \bmod 257 = 240$	$226^8 \bmod 257 = 2^3$
$3^{16} \bmod 257 = -2^3$	$3^{-16} \bmod 257 = 2^5$	$\cdots$

   In general, $2^{-i} \equiv -2^{8-i} \pmod{257}$, for all $i = 0, 1, 2, \ldots, 7$.

4. (6 pts) Consider the elliptic curve $E : y^2 = x^3 + x + 2014$ over $\mathbb{F}_{5011}$.

   (a) (3 pts) Show [1] that there exists $y \in \mathbb{F}_{5011}$ such that $(4, \pm y) \in E$.

   (b) (3 pts) Show how to use the fast exponentiation algorithm to compute one $y \in \mathbb{F}_{5011}$ such that $(4, \pm y) \in E$.

Exam Calculator Policy. It is allowed to use a function calculator, however no programmable calculator.

[1] Here you may find the following formulas useful:

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8} \\ -1 & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$$

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{if } m \equiv n \equiv 3 \pmod{4} \\ \left(\frac{n}{m}\right) & \text{otherwise.} \end{cases}$$