T-79.5501 Cryptology
Midterm Exam 2
April 8, 2016

1. (6 pts) Let $\alpha = (010)$ be an element in the Galois field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$. Consider function $f : \mathbb{Z}_8 \to \{0,1\}$ defined as

$$f(u) = \begin{cases} \text{msb}(\alpha^u), \text{ for } u \neq 7 \\ 0, \text{ for } u = 7 \end{cases}$$

where msb denotes the most significant bit. By identifying $u = u_3 2^2 + u_2 2 + u_1 \in \mathbb{Z}_8$ with $(u_3, u_2, u_1) \in \{0,1\}^3$, the function f is defined from $\{0,1\}^3$ to $\{0,1\}$.

   (a) (3 pts) Compute the truth table of f.

   (b) (3 pts) Determine the algebraic normal form ANF of f. In case you do not have any result from (a), explain how you would compute the ANF.

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) Element $\alpha = 5$ is of order 24 in the multiplicative group $\mathbb{Z}^*_{2016}$. It is given that element $\beta = 1613$ is in the subgroup generated by α. Using Shanks' algorithm attempt to determine x such that

$$5^x \equiv 1613 \pmod{2016}.$$

4. Consider the elliptic curve $E : y^2 = x^3 + x + 2016$ 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 $y \in \mathbb{F}_{5011}$ 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:

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

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