Quiz-5
Cryptography and Network Security

[Total marks - 20]

[**Instructions**: Please upload your answers in Microsoft Teams by **18/11/2020**. Your **Roll No.** and **Name** must be mentioned. No marks will be awarded without detailed solution.]

1. [2 mark]
   (a) Is the ring $\mathbb{Z}_3[X](\text{mod } X^3 + X^2 + X + 1)$ a field? Explain your answer.
   (b) Compute $(2X^2 + X + 2) + (2X + 1)$ and $(2X^2 + X + 2) \cdot (2X + 1)$ in $\mathbb{Z}_3[X](\text{mod } X^3 + X^2 + X + 1)$.
2. [2 mark] Use the division algorithm to perform the indicated polynomial division: $(X^5 + 4X^2 + 7X) \div (X^2 + 2X)$ in $\mathbb{Z}_{11}[X]$.
3. [2 mark] Use the polynomial Euclidean algorithm to determine whether the following inverse exists. If inverse exists, find it.
   - The element $X + 1$ in $\mathbb{Z}_3[X](\text{mod } X^3 + X + 1)$
4. [4 mark] Using hex notation, perform the following computations in $\mathsf{GF}(256)$ generated by $X^8 + X^4 + X^3 + X + 1$:
   (a) $\mathrm{E1} + 24$
   (b) $(12)^2$
   (c) $4\mathrm{D} \cdot (\mathrm{C7} + 1\mathrm{F})$
   (d) $(\mathrm{F4})^{-1}$
5. [2 mark] Let E be the nonsingular modular elliptic curve defined by $y^2 \equiv x^3 + 84x(\text{mod } 269)$. Compute the scalar multiple $10 \cdot P$ of the point $P = (18, 9) \in E$.

6. [2 mark] Let E be the modular elliptic curve defined by $y^2 \equiv x^3 + 2x + 1 \pmod{11}$. Compute the order $\mathsf{ord}_{\mathsf{E}}((0, 10))$.

7. [6 mark] Let $p = 439$, let E be the (nonsingular) elliptic curve $y^2 \equiv x^3 + 6x + 167 \pmod{p}$, and let $P = (312, 65)$ be the plaintext representative point.

   (a) Noting that $p \equiv 3 \pmod{4}$, generate a point G on E by running through the x coordinates $x_1 = 38, 276, 61$ (use the positive square root sign) until one is first found.

   (b) Suppose that Alice chooses her secret parameter to be $n_A = 24$, and Bob takes his to be $n_B = 71$. Go through the ElGamal encryption process that Alice would need to do to send Bob her message that is represented by the point P. What is the ciphertext?

   (c) Go through the ElGamal decryption procedure that would need to be done at Bob's end to decrypt Alice's message.

——-The End———