06-88-447: Computer Networks and Security, Summer 2017

Assignment one (Due: Friday May 26, 2017)

1.-7. Problems from the textbook (7th Edition): 1.5, 1.6, 2.3, 2.7, 2.12, 2.16, 2.27, and 5.12.

8. A finite field element that has the maximal order is called a primitive element. Find the order of all the elements in GF(19) and indicate those that are primitive elements.

9. Let the finite field GF(2^8) be generated with the irreducible polynomial $f(X) = X^8 + X^4 + X^3 + X + 1$. Let $A = X^5 + X, B = X^7 + X^2 + 1$ and $C = X^7 + X^6 + X^2 + x$ be elements in GF(2^8). Solve A^2 and $A \times B + C$.

10. (optional) An elliptic curve E over GF(7) is defined by

$$E: \quad y^2 = x^3 + 3x + 1.$$

Let $P = (0, 1)$ and $Q = (2, 1)$ be two points on E.

1. Verify that points P and Q are on curve E.
2. Compute point doubling $2P$.
3. Compute point addition $P + Q$.