Tutorial Sheet #02 (Network Security)

T1: Find the particular and general solution to the following Diophantine equation:

$$39x + 15y = 270.$$

T2: Find the solutions for the following linear equations:

i. $256x \equiv 442 \pmod{60}$
ii. $232x + 42 \equiv 248 \pmod{50}$

T3: Find the result of multiplying $P_1 = (X^5 + X^2 + X)$ by $P_2 = (X^7 + X^4 + X^3 + X^2 + X)$ in $GF(2^8)$ with irreducible polynomial $(X^8 + X^4 + X + 1)$.

T4: If the value of X is defines as follows:

$$X \equiv 2 \pmod{3}$$
$$X \equiv 3 \pmod{5}$$
$$X \equiv 2 \pmod{7}.$$

Find the suitable value of X to satisfy the above equation using Chinese Remainder Theorem.

T5: Find the value of the following

i. $44^{-1} \bmod 667$
ii. $17364^{41} \bmod 2134$ (Using square and multiply method)

T6: Find multiplicative inverse of $(x^3 + x + 1)$ in $GF(2^4)$ with the modulus $(x^4 + x + 1)$ using Extended Euclidean algorithm.

T7: Using Miller-Rabin test, prove that the number 2047 is prime or a composite number.

T8: Generate the elements of the field $GF(2^4)$ using the irreducible polynomial $f(x) = x^4 + x + 1$. Also find the value of g^3/g^8.

T9: Find the order of elements and primitive roots of $a^i \equiv x \pmod{19}$ defined for the group $G = \langle Z_{19}^*, x\rangle$.

T10: Using the properties of discrete logarithmic, find the solution of the following congruence:

$$2x^{11} \equiv 22 \bmod 19$$

T11: Using quadratic residue, solve the following congruences:

(i) $X^2 \equiv 3 \bmod 23$
(ii) $X^2 \equiv 7 \bmod 19$

T12: Find the multiplication inverse of the following defined for $GF(2^3)$ with irreducible polynomial $(x^3 + x^2 + 1)$.

i. X^2
ii. $X^2 + 1$
iii. $X^2 + x$

T13: An irreducible polynomial in $GF(2^3)$ is defined as x^3+x+1.Create the Addition and Multiplication table for defined polynomial.

P. T. O

T14: Using Miller-Rabin test, prove that the number 2047 is prime or a composite number.

T15: Find the value of g^{20} for the defined Galois field $GF(2^4)$ using irreducible polynomial $f(x) = x^4 + x + 1$.

T16: Assuming the quadratic congruence modulo a composite is defined as $\mathbf{x^2 \equiv 36 \pmod{77}}$. Find all the possible value of x for the above congruence.