Tutorial Sheet #04 (Network Security)

T1: Given the super-increasing tuple b = [7, 11, 19, 39, 79, 157, 313], r = 37, and modulus n = 900, encrypt and decrypt the letter "H" using the knapsack cryptosystem. Use [4 2 5 3 1 7 6] as the permutation table. Use ASCII value for representing H.

T2: Given the super-increasing tuple b = [7, 11, 23, 43, 87, 173, 357], r = 41, and modulus n = 1001, encrypt and decrypt the letter "d" using the knapsack cryptosystem. Use [7 6 5 1 2 3 4] as the permutation table. Use ASCII value for representing d.

T3: Using the value of p=11 and q=19, for RSA:

i. Find the value of public key.
ii. Find the value of private key.
iii. Encrypt and Decrypt the message "TO" using the key generated in part i and ii.

T4: In RSA cryptosystem find d if you know that e = 17 n= 187

T5: In a public-key system using RSA, Eve intercept the cipher text c = 10 sent to a user whose public key is e = 5 and n = 35. What is the plaintext m?

T6: In Rabin Cryptosystem, user A chooses two prime numbers p= 23 and q= 7. Encrypt and decrypt the plain text P= 24 using this method.

T7: In ElGamal, given the prime p = 31:

a. Choose an appropriate e1 and d, then calculate e2.
b. Encrypt the message "HELLO"; use 00 to 25 for encoding.
c. Decrypt the cipher text to obtain the plaintext.

T8: Assume that Alice uses Bob's ElGamal public key (e1=2) to send two messages P1= 17 and P2= 37 using the same random integer r= 9. Eve intercepts the cipher text and somehow find the value of P1 = 17. Show how Eve can use a known plain text attack to find the value of P2. Assume the value of modulus p= 53 and d= 3.

T9: If two points on the Elliptical curve $E_{23}(1,1)$ is defined as P(3,10) and Q(9,7), then find the value of:

i. P+Q
ii. 4P

T10 : An elliptic curve is defined by $y^2 = x^3 + 2x + 9$ with a modulus of p=37 for the Elliptical curve cryptosystem. Determine any five points on this curve.

T11: An elliptical curve $y^2 + xy = x^3 + g^3x^2 + b$ is defined over $GF(2^3)$ with irreducible polynomial $f(x) = x^3 + x + 1$. Find all the points exist on this curve.

T12: An elliptical curve $y^2 + xy = x^3 + ax^2 + 1$ is defined over $GF(2^3)$ with irreducible polynomial $f(x) = x^3 + x + 1$. Find all points exist on this curve with a= g^3 and b=1.

P.T.O

T13: An elliptical curve $y^2 + xy = x^3 + ax^2 + b$ is defined over $GF(2^4)$ with irreducible polynomial $f(x) = = x^4 + x + 1$. Find any seven points exist on this curve with $a = g^4$ and $b = g^0$.