Practice Question for Integers, Cryptography and Bin packing

Q.N.1 Prove that by using mathematical induction

a. $4+9+14+19+\ldots.+(5n-1)=n(5n+3)/2$

b. $1+4+7+\ldots.+(3n-2)= n(3n-1)/2$

c. $1.3+2.3^2+3.3^3+\ldots.+n.3^n= \{(2n-1)3^{n+1}+3\}/4$

Q.N.2

Give a recursive formula for the following sequence:

a. 3, 9, 81, 6561,….

b. 2, 7, 22, 67, 202, 607,…

c. 1, 3/2, 9/4, 27/8, 81/16……

Q.N.3

If A =$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$, B= $\begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix}$

a. Find AB and BA if Possible.
b. Show that: A^2-2A-5 I = 0 ,where I is an identity matrix of 2 x 2 order
c. Find
   i. $|A|$
   ii. A^{-1}

Q. N.4

a.

i.Find the GCD of (3345, 35) by using Euclidean Algorithm

ii.Construct the addition and multiplication table for Z_6 and Z_7

iii. Calculate: 75^{45} in Z103

iv.Solve: 3x = 2 (mod11)

b. The Hill Cipher uses matrices and congruence arithmetic. First the alphabetic massage is converted to a string of numbers, uses 0 for a,1 for b and son on until we reach 25 for Z. The massage then broken up into segments of equal length , and each of these segments treated as a column matrix and multiplied by an enciphering matrix , C and the result modulo 26 is used to give the cipher text with K= $\begin{pmatrix} 7 & 9 \\ 3 & 4 \end{pmatrix}$

i. Encipher the massage 'HE'

ii. Show that the deciphering matrix recovers the original massage.

iii. Calculate the matrix K.D

c. Messages are to be encoded using the RSA method, and the primes chosen are 13 and 17.Encode and decode the numbers 9, 35.

d. What are the advantages of public key cryptography over private key? What about disadvantages?

e. Describe the *RSA* (Rivest, Shamir and Adelman) public key cryptosystem. Your answer should include

i. The generation of public and private keys
ii. The encryption algorithm
iii. The decryption algorithm

Q.N. 6

i.

29 52 73 87 74 47 38 61 41

The number in the list represents the length in minutes of nine radio programs. They are to be recorded onto tapes which each store up to 100 minutes of program.

a. Obtain a lower bound for the number of tapes needed to store the nine programs.

b. Use the first fit bin packing algorithm to fit the program onto the tapes

ii.

Ten examinations are to be scheduled in the smallest possible number of days. The maximum allowable number of hours per day for examinations is 6, and the examinations have the following durations (in hours).

Activity A B C D E F G H I J

Duration 1 2 3 3 1.5 4 1.5 3 1 4

(a) Find the lower bound, for the number of days required for the examinations.

(b) Use the first fit decreasing algorithm to estimate the minimum number of days required for the examinations. Does the first fit decreasing algorithm give an optimal solution?

(c) Find a solution needing only L days.