Heaven's Light is Our Guide
Computer Science & Engineering
Rajshahi University of Engineering & Technology

Lab Manual

Module- 03

Course Title: Sessional based on CSE 2101
Course No. : CSE 2102

Experiment No. 3

Name of the Experiment: Algorithms, Number Theory and Cryptography

Duration: 2 Cycles

Experiments/Problems:

[1] Given a list of n integers, find the largest integer in the list and its complexity.
[2] Given a list of n integers, find the first and last occurrences of the largest integer in the list.
[3] Given a list of n distinct integers, determine the position of an integer in the list using a linear search.
[4] Given an ordered list of n distinct integers, determine the position of an integer in the list using a binary search.
[5] Given a list of n integers, sort them using a bubble sort.
[6] Given a list of n integers, sort them using an insertion sort.
[7] Given an integer n, use the greedy algorithm to find the change for n cents using quarters, dimes, nickels, and pennies.
[8] *Given the starting and ending times of n talks, use the appropriate greedy algorithm to schedule the most talks possible in a single lecture hall.
[9] Given an ordered list of n distinct integers and an integer x, find the number of comparisons used to determine the position of an integer in the list using a binary search and using a linear search.
[10] Given a list of n integers, determine the number of comparisons used by the bubble sort and by the insertion sort to sort this list.
[11] Given a set of identification numbers, use a hash function to assign them to memory locations where there are k memory locations.
[12] Given a positive integer N, a modulus m, multiplier a, increment c, and seed x_0, where $0 \leq a<m$, $0 \leq c<m$, and $0 \leq x_0 <m$, generate the sequence of N pseudo-random numbers using the linear congruential generator $x_{n+1} = (ax_n + c) \bmod m$.
[13] Given a message, encrypt this message using Caesar cipher; and decrypt this message again.
[14] Given a positive integer, determine whether it is prime.
[15] Given a positive integer, determine whether it is Mersenne prime.
[16] The polynomial $f(n) = n^2-n+41$ has the interesting property that f(n) is prime for all positive integers n not exceeding 40. Given a positive integer n, find the value of f(n) whether f(n) is prime or not.
[17] [Goldbach's Conjecture] Given an even integer n, find two prime number whether the sum of them is equal to n.
[18] Given an integer n, whether $f(n) = n^2+1$ is prime or not.
[19] [The Twin Prime Conjecture] Given a positive number n, whether it is prime or not. If n is prime, check whether n and n+2 are Twin primes or not.
[20] Given two positive integers, find their greatest common divisor using the Euclidean algorithm.
[21] Given two positive integers, find their least common multiple.
[22] Given a positive integer, find the prime factorization of this integer.
[23] Given integers n and b, each greater than 1, find the base b expansion of this integer.
[24] [Modular Exponentiation] Given the positive integers a, b, and m with m> 1, find $a^b \bmod m$.
[25] *Given a positive integer, find the Cantor expansion of this integer.

[26] Given two positive number a and b, find s and t such that gcd(a,b) = sa+tb.
[27] [The Chinese remainder theorem] Given n linear congruence's modulo pair wise relatively prime moduli, find the simultaneous solution of these congruence's modulo the product of these moduli.
[28] [pseudo primes] Given a positive integer b, find all pseudo primes to the base b that do not exceed 10,000.
[29] Given a composite integer n, determine whether it is Carmichael number or not.
[30] **Construct a valid RSA encryption key by finding two primes p and q with 200 digits each and an integer e> 1 relatively prime to $(p - 1)(q - 1)$.
[31] Given a message and an integer n = pq where p and q are odd primes and an integer e> 1 relatively prime to $(p - 1)(q - 1)$, encrypt the message using the RSA cryptosystem with key (n,e).
[32] Given a valid RSA key (n,e), and the primes p and q with n = pq, find the associated decryption key d.
[33] Given a message encrypted using the RSA cryptosystem with key (n,e) and the associated decryption key d, decrypt this message.
[34] Given an $m \times k$ matrix **A** and a $k \times n$ matrix **B**, find **AB**.
[35] Given a square matrix A and a positive integer n, find A^n.
[36] Given a square matrix, determine whether it is symmetric.
[37] Given two $m \times n$ Boolean matrices,find their meet and join.
[38] Given an $m \times k$ Boolean matrix **A** anda $k \times n$ Boolean matrix **B**,find the Boolean product of **A** and **B**.
[39] Given a square Boolean matrix **A** and a positive integer n, find $\mathbf{A}^{[n]}$.

Explain:

[25] A cantor expansion is a sum of the form

$$x = a_n n! + a_{n-1}(n - 1)! + \cdots + a_1 1!$$

procedure Cantor(x:positiveinteger)
n := 1; f := 1
while (n + 1) · f ≤ x
begin
  n := n + 1
  f := f · n
end
y := x
while n> 0
begin
a_n :=⌊y/f⌋
y := y − a_n · f
f := f/n
n := n − 1
end{$x = a_n n! + a_{n-1}(n - 1)! + \cdots + a_1 1!$}

[28] Let b be a positive integer. If n is a composite positive integer, and $b^{n-1} \equiv 1 \pmod n$, then n is called a pseudo prime to the base b.

[29] A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \pmod n$ for all positive integers b with gcd(b,n) = 1 is called a Carmichael number. (These numbers are named after Robert Carmichael, who studied them in the early twentieth century.)

[30-32] **The RSA Cryptosystem**

KEY GENERATION:

[1] Choose two distinct prime numbers p and q, say, with 200 digits each.
Simple Example: $p = 61$ and $q = 53$

[2] Compute $n = pq$.
Simple Example: $n = 3233$

[3] Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$.
Simple Example: $\varphi(n) = 3120$

[4] Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
Simple Example: e= 17

[5] Determine d as $d \equiv e-1 \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$) [This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$]
Simple Example:

d = 2753
Worked example for the modular multiplicative inverse
$d \times e \bmod \varphi(n) = 1$
$2753 \times 17 \bmod 3120 = 1$

[6] The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret.
Simple Example: The public key is (e = 17) and the private key is (n = 3233, d = 2753).

RSA ENCRYPTION:

For a padded plaintext message M, the encryption function is

$$C(M) = M^e \textbf{ mod } n$$

Simple Example: For instance, in order to encrypt m = 65, we calculate

$$C(M) = 65^{\mathbf{17}} \textbf{ mod 3233} = 2790$$

RSA DECRYPTION:

For an encrypted ciphertext c, the decryption function is

$$M(C) = C^d \textbf{ mod } n$$

Simple Example: To decrypt c = 2790, we calculate

$$M(c) = 2790^{\mathbf{2753}} \textbf{ mod 3233} = 65$$

Report:

Your completed work must be submitted through a LAB REPORT.

Read:

[1] Kenneth H. Rosen, "Discrete Mathematics and its Application", 7th Edition: Chapter 3 (Algorithms) Chapter 4(Number Theory and Cryptography).