CS 58000\_01/02I Design, Analysis and Implementation Algorithms (3 cr.)

Assignment As\_02 (Exam 01)

Student Name: Truc L. Huynh

This assignment As\_02 is due at 10:30 am, Thursday, October 18, 2022. Please submit your assignment to Brightspace (purdue.brightspace.com). No late turn-in is accepted. Please write your name on the first page of your assignment. Your file name should be your last name such as Ng.docx. Please number your problem-answer clearly such as Problem 1a, 1b, 1c, Problem 2a, 2b, …. The problems’ answers must be arranged in order. Please answer your questions using only a Word file (.docx file only). No pdf file will be accepted. Without using a Word file (.docx file) the submitted problems’ answers would not be graded.

The total number of points for this Assignment\_02 (Exam 01) is 140 points.

Problem 1[30 points]:

In Ch 00\_03, we addressed Figure 1.4 Modular Exponentiation: Given a function modexp(x, y, N) for computing xy mod N, where x, y, and N are integers. We also addressed when k is a power of 2, and a is any integer. We also addressed Fermat’s Little Theorem.

1a. What is (mod 17)?

Answer:

=

1b. What is (𝑚𝑜𝑑 31)? (Hard Problem)

1c. Construct (Design) a polynomial-time algorithm for computing (mod p), where

x, y, z, and a prime p.

Problem 2 [60 points]:

This problem is an exercise using the formalization of the RSA public-key cryptosystem. For solving the problems, you are required to use the following formalization of the RSA public-key cryptosystem.

Given the following formalization of the RSA public-key cryptosystem, each participant creates their public key (n, g) where a is a small prime number, and n is the product of two large primes, p and q. However, the two large primes p and q are secret keys.

1. Select two very large prime numbers p and q. The number of bits needed to represent p and q might be 1024.
2. Compute

n = pq

(n) = (p – 1) (q – 1).

The formula for (n) is owing to the Theorem: The number of elements in is given by Euler’s totient function, which is

where the product is over all primes that divide n, including n if n is prime.

1. Choose a small prime number as an encryption component g, that is relatively prime to (n). That means,

gcd(g, (n) ) = 1, i.e.,

gcd(g, (p-1)(q-1)) = 1.

1. Compute the multiplicative inverse That is,

The inverse exists and is unique.

That is, the decryption component h = g-1 mod (n).

1. Let pkey = (n, g) be the public key, and skey = (p, q, h) be the secret key.

* For any message M mod n, the encryption of M is C = Mg mod n.
* The decryption of C is M = Ch mod n.

End of the formalization of the RSA public-key cryptosystem.

Use the RSA Cryptosystem formalism for solving problem 2.

Given g = 59, p = 991 and q = 997.

2a. Show that the given values of g, p, and q are prime.

2b. Compute n = pq and (n) = (p – 1) (q – 1).

2c. Given a plaintext **M = 5065747269**, what is the encryption of M, using C = Mg mod n. Show in detail how you derive C, which is the ciphertext of the plaintext M.

2d. Compute the multiplicative inverse That is, the decryption component h = g-1 mod (n).

[Hints: Compute a GCD as a Linear Combination. Then, find an Inverse Modulo n. In other words, you can apply the extended Euclid algorithm to find the linear combination of g and Then find a positive inverse of g mod ]

2e. From problem 2d, what is your secret key (p, q, h)?

2f. What is the decryption of C using M = Ch mod n? Show in detail how you derive M, which is the plaintext M of the ciphertext C.

2g (Bonus)[5 points]:

What is the message (in terms of the alphabet)?

Problem 3[30 points]:

Assume that we define

h1(k) = k mod 13, and

h2(k) = 1 + (k mod 11).

For the open addressing, consider the following methods

**Linear Probing**

Given an ordinary hash function h: U {0, 1, 2, …, m-1}, the method of *linear probing* uses the hash function

h(k, i) = (h1(k) + i) mod m for i = 0, 1, 2, …, m-1.

**Quadratic Probing**

Uses a hashing function of the form

h(k, i) = (h1(k) + c1i + c2i2 ) mod m,

where h1 is an auxiliary hash function, c1 and c2 0 are auxiliary constants c1 3 c2 = 5,

and i = 0, 1, 2, …, m-1.

**Double hashing**

Uses a hashing function of the form

h(k, i) = (h1(k) + i h2(k) ) mod m,

where h1 and h2 are auxiliary hash functions.

The value of h2(k) must never be zero and should be relatively prime to m for the sequence to include all possible addresses.

Given K = {79, 69, 98, 72, 14, 50, 88, 99, 78, 65} and the size of a table is 13, with indices counting from 0, 1, 2, …, 12. Store the given K in a table with the size 13 counting the indices from 0, 1, 2, …, 12. Show the resultant table with 10 given keys for each method applied:

**3a. if linear probing is employed.**

The Resultant Table with 10 given keys is: Complete the table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

**3b. if quadratic probing is employed.**

The Resultant Table with 10 given keys is: Complete the table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

**3c. if double hashing is employed.**

The Resultant Table with 10 given keys is: Complete the table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

Problem 4 [20 points]:

For the division method for creating hash functions, map a key k into one of the m slots by taking the remainder of k divided by m. The hash function is:

h(k) = k mod m,

where m should not be a power of 2.

For the multiplication method for creating hash functions, the hash function is

h(k) = └ m(kA –└ k A ┘) ┘ = └ m(k A mod 1) ┘

where “k A mod 1” means the fractional part of k A and a constant A in the range

0 < A < 1.

An advantage of the multiplication method is that the value of m is not critical.

Choose m = 2p for some integer p.

Give your explanations for the following questions:

4a. Why m should not be a power of 2 in the division method for creating a hash

function?

4b. Why m = 2p, for some integer p, could be (and in fact, favorably) used in the

multiplication method?

**Note: If you provide your answer in your handwriting, good handwriting is required.**

**Proper numbering of your answer to each problem is strictly required. The problem’s solution must be orderly given. (10 points off if not)**