Exercises: Applications of Modular Arithmetic

Exercise 1

Please see "Brooks - The RSA-Algorithm" for an overview of the RSA algorithm.

Using A = 00, B = 01,... J = 09... Z = 25, such that 'GO' is 0614 = 614 and 'SE' is 1804, encrypt and decrypt 'OK' using RSA. The two primes must be 47 and 61. You must choose either 5 or 7 as e.

a. What are the values of the public and private keys?

b. What is the value of the cipher text and what is the cipher text?

c. Decrypt the cipher text and make sure you obtain the original plain text.

Exercise 2

Given input {4371, 1323, 6173, 4199, 4344, 9679, 1989} and hash functions given below, show the tables for a hash table size 10:

a. Hash table using linear probing with the hash function $h(x) = x \bmod 10$.

b. Hash table using quadratic probing with $h'(x) = x \bmod 10$ and $h(x) = (h'(x) + i^2) \bmod 10$

c. Hash table with double hashing using $h_1(x) = x \bmod 10$ and $h_2(x) = 7 - (x \bmod 7)$.

Exercise 3

0	1	2	3	4	5	6	7	8	9	10
11			16		12				15	4

In the hash table above, linear probing with the hash function $h(k) = 5k \mod 11$ has been used.

Find the positions that the five elements 2, 3, 5, 6, and 10 will be inserted in (for each insertion, assume that the hash table only contains the elements shown above, i.e. 4, 11, 12, 15, and 16).

	0	1	2	3	4	5	6	7	8	9	10
INSERT(2)	A	B	C	D	E	F	G	H	I	J	K
INSERT(3)	A	B	C	D	E	F	G	H	I	J	K
INSERT(5)	A	B	C	D	E	F	G	H	I	J	K
INSERT(6)	A	B	C	D	E	F	G	H	I	J	K
INSERT(10)	A	B	C	D	E	F	G	H	I	J	K

Exercise 4

In the hash table below of size 11, quadratic probing with the hash functions $h'(k) = 2k \bmod 11$ and $h = \left(h'(k) + i + 3i^2\right) \bmod 11$ has been used.

0	1	2	3	4	5	6	7	8	9	10
0		1			8	3			19	

Find the positions that the five elements 2, 4, 7, 10, and 11 will be inserted in (for each insertion, assume that the hash table only contains the elements shown above, i.e. 0, 1, 3, 8, and 19).

	0	1	2	3	4	5	6	7	8	9	10
INSERT(2)	A	B	C	D	E	F	G	H	I	J	K
INSERT(4)	A	B	C	D	E	F	G	H	I	J	K
INSERT(7)	A	B	C	D	E	F	G	H	I	J	K
INSERT(10)	A	B	C	D	E	F	G	H	I	J	K
INSERT(11)	A	B	C	D	E	F	G	H	I	J	K

Exercise 5

In the hash table below of size 11, double hashing with the hash functions $h_1(k) = 4k \bmod 11$ and $h_2 = 1 + (2k \bmod 10)$ has been used.

0	1	2	3	4	5	6	7	8	9	10
22					15	7	10			21

Find the positions that the five elements 1, 3, 4, 6, and 11 will be inserted in (for each insertion, assume that the hash table only contains the elements shown above, i.e. 7, 10, 15, 21, and 22).

	0	1	2	3	4	5	6	7	8	9	10
INSERT(1)	A	B	C	D	E	F	G	H	I	J	K
INSERT(3)	A	B	C	D	E	F	G	H	I	J	K
INSERT(4)	A	B	C	D	E	F	G	H	I	J	K
INSERT(6)	A	B	C	D	E	F	G	H	I	J	K
INSERT(11)	A	B	C	D	E	F	G	H	I	J	K

Exercise 6

In this exercise we want to use the RSA Key pair from exercise 1 to sign a message, M = 'I love DMA1'. In order to convert this string to a number we will refer to the ASCII table and then concatenate the values. Using the ASCII table, the string 'Python rules' becomes

$$080\ 121\ 116\ 104\ 111\ 110\ 032\ 114\ 117\ 108\ 101\ 115$$

If we now apply the hash function from Exercise 3 to this value, we get:

$$h(80121116104111110032114117108101115) = 5 \times 80121116104111110032114117108101115 \bmod 11 \equiv 3$$

This position is occupied, so we move to $i = 4$.

We recommend using this String to ASCII converter and Wolfram to do the computation.

a. What is the ASCII value of 'I love DMA1'?

b. What is the hash value of the ASCII value of 'I love DMA1'? Use the hash function and hash table from Exercise 3.

c. What is the signature of the hash value found in (b)?

d. Use the public key to retrieve the hash value from the signature found in (c). Confirm that this hash value is the same as the one found in (b).