Problem 1

Short answer: Consider a text made up of symbols from a symbol set containing 71 elements, each corresponding to a unique integer from 0 to 70, encrypted with the affine cipher, with keys a and b encrypting each plaintext character p according to the formula p · a + b (mod 71). Suppose we know that '52' is enciphered as '6', '20' is enciphered as '51', and '4' is enciphered as '38'. Find the keys a and b mod 71. Include your solution, including all relevant work and explanation, in your a3.pdf.

- With the formula p*a + b (mod 71), we can get the following functions:
    - 52 * a + b (mod 71) = 6
    - 20 * a + b (mod 71) = 51
    - 4 * a + b (mod 71) = 38
- Then we can use the functions above to find "a" first
    - ((52a - 20a) + (b-b)) (mod 71) = 6 - 51
    - 32a mod 71 = -45 = 26
    - 71 = 2 * 32 + 7
    - 32 = 4 * 7 + 4
    - 7 = 1 * 4 + 3
    - 4 = 1 * 3 + 1
    - 1 = 4 - 1 * 3
    - 1 = 4 - 1 * (7 - 1 * 4) = 2 * 4 - 1 * 7
    - 1 = 2 * (32 - 4 * 7) - 1 * 7 = 2 * 32 - 9 * 7
    - 1 = 2 * 32 - 9 * (71 - 2 * 32) = 20 * 32 - 9 * 71
    - a = 26 * 20 mod 71 = 23
- Then we plug it back into the function to get b
    - 4 * 23 + b mod 71 = 38
    - 54 mod 71 = 17 (71-4*23 - 38)
- Thus we have the key for this affine cipher (a,b) = (23, 17)

Problem 3

Short answer: According to the given algorithm in problem 2, Alice started to generate some random numbers with m = 467, generates the numbers R_2 = 28, R_3 = 137, R_4 = 41, R_5 = 118, and R_6 = 105. Help Eve to predict next random numbers by determining the values of a, b, c, R_0, R_1 and R_7. Include the values of these six variables, with all relevant work and explanation for how you found them, in your a3.pdf or a3.txt.

Based on the information given above:

- When Alice uses m = 467
- We got the following equation
  - (137a + 28b + c) mod 467 = 41
  - (41a + 137b + c) mod 467 = 118
  - (118a + 41b + c) mod 467 = 105
- Then we combine 3-2 and 1-3 to eliminate c
  - 77a - 96b mod 467 = -13 = 454
  - 19a - 13b mod 467 = -64 = 403
- Using the above equation we can also delete b
  - 1824a - 1248b mod 467 = 394
  - 1001a - 1248b mod 467 = 298
  - 823a mod 467 = 96
  - 356a mod 467 = 96
  - 467 = 1 * 356 + 111
  - 356 = 3 * 111 + 23
  - 111 = 4 * 23 + 19
  - 23 = 1 * 19 + 4
  - 19 = 4 * 4 + 3
  - 4 = 1 * 3 + 1
  - 1 = 4 - 1 * 3
  - 1 = 5 * 4 - 1 * 19
  - 1 = 5 * 23 - 6 * 19
  - 1 = 29 * 23 - 6 * 111
  - 1 = 29 * 356 - 93 * 111
  - 1 = 122 * 356 - 93 * 467
  - a = 122 * 96 mod 467 = 37
- Then we can plug a back to the equation to find b
  - 19 * 37 - 13b mod 467 = 403
  - 13b mod 467 = 300
  - 467 = 35 * 13 + 12
  - 13 = 1 * 12 + 1
  - 1 = 13 - 1 * 12
  - 1 = 13 - 467 + 35 * 13
  - 1 = 36 * 13 - 1 * 467

    - b = 36 * 300 mod 467 = 59
- Then we can plug a and b back into the original equation for c
    - (118a + 41b + c) mod 467 = 105
    - 6785 + c mod 467 = 105
    - C mod 467 = -6680
    - C mod 467 = -142
    - C = 325

After finding the value of a, b, and c, we can now find the values for R0 and R7:

- R1 = 28a + R1b + c mod 467 = 137
    - 28 * 37 + 59R1 + 325 mod 467 = 137
    - 59R1 mod 467 = -1256
    - 59R1 mod 467 = 177
    - 467 = 7 * 59 + 54
    - 59 = 1 * 54 + 5
    - 54 = 10 * 5 + 4
    - 5 = 1 * 4 + 1
    - 1 = 5 - 1 * 4
    - 1 = 5 - 1* (54 - 10 * 5)
    - 1 = 11 * 5 - 54
    - 1 = 11 * (59 - 54) - 54
    - 1 = 11 * 59 - 12 * 54
    - 1 = 11 * 59 - 12 * (467 - 7 * 59)
    - 1 = 95 * 59 - 12 * 467
    - R1 = 95 * 177 mod 467 = 3
- R0 = 37 * 3 + 59 * b + 325 mod 467 = 28 => 1
- R7 = 105a + 118b + c mod 467 = 105 * 37 + 118 * 59 + 325 mod 467 = 11172 mod 467 = 431

To conclude, a = 37, b = 59, c = 325, R0 = 1, R1 = 3, R7 = 431