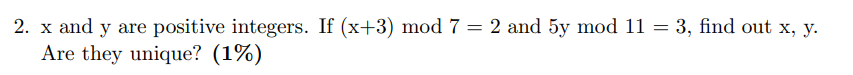
  
No R must satisfy 1<R<n and GDC (R, n) = 1, so that a multiplicative inverse exists(R^-1)



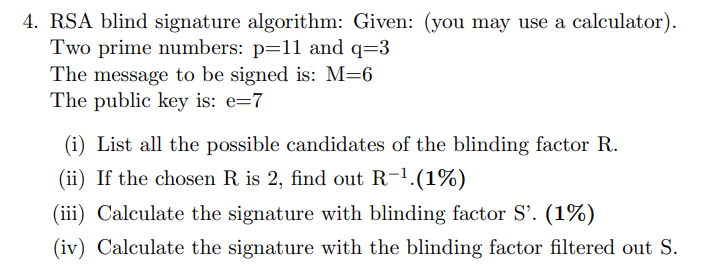
X+3 mod 7 = 2  
x = 6  
x = 6 + 7i; i E Positive Integers [including zero]  
x E { 6, 13, 20 …}  
X is not unique

5y mod 11 = 3  
(5 mod 11 x y mod 11) = 3  
y mod 11 = (3 x 5^-1 mod 11) mod 11  
5^-1 mod 11 = 9  
y = 27  
y = 5 + 11x where x E Positive Integers [including zero]  
y E {5,16,27…}  
Y is not unique  
  


we define a primitive root of a prime number p as one whose powers generate all the integers from 1 to p-1, that is the numbers:  
g^1 mod p, *g^2* mod p, … *g^p-1* mod p are distinct and consist of the integers from 1 to p-1 in some permutation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 31 | 32 | 33 | 34 | 35 | 36 |
| 3 | 2 | 6 | 4 | 5 | 1 |

Yes since 3^x mod 7 where x Element {1,2,3,4,5,6} produce the same elements in some permutation[all values are unique]



(i)   
  
n = 11\*3  
 = 33  
  
phi(n) = 10\*2 = 20  
  
R = { 2,4,5,7,8,10,13,14,16,17,19,20,23,25,26,28,29,31,32 }

(ii)   
  
R = 2  
  
33 = 2(16) + 1  
33 – 2(16) = 1  
33 – 16 = 17  
  
R^-1 = 17

(iii)

Calculate d:

E\*d mod phi(n) = 1  
  
20 = 7(2) + 6  
7 = 6(1) + 1  
----------------------

20 – 7(2) = 6  
7 - 6 = 1  
7 – (20 – 7(2)) = 1  
(3) 7 – 20 = 1   
  
d = 3  
  
M’ = M \* R^e mod 33  
 = 6 \* 2^7 mod 33  
 = 9  
  
S’ = M’^d   
 = M^d R (mod n)

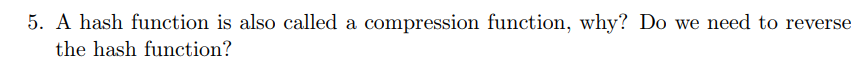
=6^3 \* 2 mod 33

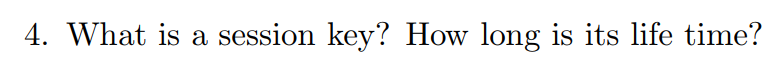
S’ = 3

(iv)

S = S’R^-1 = M^d mod n

S = 6^3 mod 33  
S = 18

  
It is called a compression function because the output of the hash value is smaller than the input. No we do not need reverse the hash function, it is not reversible.

  
  
  
  
A key that is used for communication for a small amount of time [for one session], its lifetime is for the session for the one communication.