Cryptography Assignment 1

1.

2.
Elements in Z_5 are {1, 2, 3, 4}
The multiplicative inverse of the following are: {1, 2, 3 , 4}
Elements in Z_{11} are { 1, 2, 3, 4 ,5, 6, 7 ,8, 9, 10}
The multiplicative inverse of the following are:{10, -5, 4 ,3, 2 ,2 ,3, -4 , 5, 1}

3.
GCD of 56425, 43159 = 1
q= 1
old_r, r 43159 13266
old_s, s 0 1
old_t, t 1 -1
q= 3
old_r, r 13266 3361
old_s, s 1 -3
old_t, t -1 4
q= 3
old_r, r 3361 3183
old_s, s -3 10
old_t, t 4 -13
q= 1
old_r, r 3183 178
old_s, s 10 -13
old_t, t -13 17
q= 17
old_r, r 178 157
old_s, s -13 231

old_t, t 17 -302
q= 1
old_r, r 157 21
old_s, s 231 -244
old_t, t -302 319
q= 7
old_r, r 21 10
old_s, s -244 1939
old_t, t 319 -2535
q= 2
old_r, r 10 1
old_s, s 1939 -4122
old_t, t -2535 5389
q= 10
old_r, r 1 0
old_s, s -4122 43159
old_t, t 5389 -56425

4.
$\phi(3^4) = 3^4 - 3^{3 = 54}$
$\phi(2^{10}) = 2^{10} - 2^9 = 512$
5.
$100 = 2^6 + 2^5 + 2^2$
3^{2^0} mod 31319 = 3 mod 31319
3^{2^1} mod 31319 = 9 mod 31319
3^{2^2} mod 31319 = 81 mod 31319
3^{2^3} mod 31319 = 6561 mod 31319
3^{2^4} mod 31319 = 14415 mod 31319
3^{2^5} mod 31319 = 21979 mod 31319
3^{2^6} mod 31319 = 12185 mod 31319

Therefore, 3^{100} mod 31319 = 12185 x 21979 x 81 mod 31319
= 25879 mod 31319