18CA314-Cryptography and Network Security

ASSIGNMENT-1

2. Find the multiplicative inverse of all the elements in Z5 and Z11

Ans: Multiplicative Inverse of:

Z_5->

a	1	2	3	4
a^{-1}	1	3	2	4

Z_{11}->

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1	6	4	3	9	2	8	7	5	10

3. Determine the gcd of 56245 and 43159

Ans: 56245=43159*1+13086

43159=13086*3+3901

13086=3901*3+1383

3901=1383*2+1135

1383=1135*1+248

1135=248*4+143

248=143*1+105

143=105*1+38

105=38*2+29

38=29*1+9

29=9*3+2

9=2*4+1

2=**1***2+0

Therefore, gcd(56245,43159)=1.

4. Compute phi(n) for 3^4 and 2^{10}

Ans: According to Euler's product formula

Phi(3^4)=3^4*(1-(1/3))

=81*2/3

=54.

Phi(2^{10})=2^{10}*(1-(1/2))

=1024*1/2

=512.

5. Compute 3^{100} mod(31319)

Ans: Here e=100 =>2^6+2^5+2^2

3^0 mod 31319=3

3^2 mod 31319=9

3^4 mod 31319=81

3^8 mod 31319=6561

3^{16} mod 31319=14418

3^{32} mod 31319=21979

3^{64} mod 31319=12185

3^{100} mod(31319)=12185*21979*81 mod 31319

=5346*81 mod 31319

=25879.