Amrita Vishwa Vidyapeetham
MCA
Fourth Semester
18CA314-Cryptography and Network Security
Assignment 1
Part A

3. Determine the gcd of 56245 and 43159

gcd(56245,43159)

56245=1*43159+13086

43159=3*13086+3901

13086=3*3901+1383

3901=2*1383+1135

1383=1*1135+248

1135=4*248+143

248=1*143+105

143=1*105+38

105=2*38+29

38=1*29+9

29=3*9+2

9=4*2+1

2=2***1**+0

gcd(56245,43159) = 1

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

Z5=

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

Z11=

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

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

$100=2^6+2^4+2^2$

3^0 mod 31319 = 3

3^2 mod 31319 = 9

3^4 mod 31319 = 81

3^8 mod 31319= 6561

3^{16} mod 31319 = 14415

3^{32} mod 31319 = 21979

3^{64} mod 31319 = 12185

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

=25879

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

$(3^4) = 3^4-3^{4-1}$

$=3^{4-1}(3-1)$

$=3^4 * (1-1/3) = 54$

$(2^{10}) = 2^{10}-2^{10-1}$

$= 2^{10-1} (2-1)$

$= 2^{10} x (1-1/2) = 512$

1. Prove that $(a + p)^n(\text{mod } p) = a^n(\text{mod } p)$

$(a + p)^n(\text{mod } p)=a^n+p^n \text{ mod } p$

$=a^n \text{ mod } p + p^n \text{ mod } p$

$=a^n \text{ mod } p + 0$

$=a^n \text{ mod } p$