

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

3. Determine the gcd of 56245 and 43159

$\text{gcd}(56245, 43159)$

$$56245 = 1 * 43159 + 13086$$

$$43159 = 3 * 13086 + 3901$$

$$13086 = 3 * 3901 + 1383$$

$$3901 = 2 * 1383 + 1135$$

$$1383 = 1 * 1135 + 248$$

$$1135 = 4 * 248 + 143$$

$$248 = 1 * 143 + 105$$

$$143 = 1 * 105 + 38$$

$$105 = 2 * 38 + 29$$

$$38 = 1 * 29 + 9$$

$$29 = 3 * 9 + 2$$

$$9 = 4 * 2 + 1$$

$$2 = 2 * 1 + 0$$

$$\text{gcd}(56245, 43159) = 1$$

2. Find the multiplicative inverse of all the elements in \mathbb{Z}_5 and \mathbb{Z}_{11}

$\mathbb{Z}_5 =$

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

$\mathbb{Z}_{11} =$

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

5. Compute $3^{100} \bmod(31319)$

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

$$3^0 \bmod 31319 = 3$$

$$3^2 \bmod 31319 = 9$$

$$3^4 \bmod 31319 = 81$$

$$3^8 \bmod 31319 = 6561$$

$$3^{16} \bmod 31319 = 14415$$

$$3^{32} \bmod 31319 = 21979$$

$$3^{64} \bmod 31319 = 12185$$

$$\begin{aligned} 3^{100} \bmod(31319) &= 12185 * 21979 * 81 \bmod 31319 \\ &= 25879 \end{aligned}$$

4. Compute $\varphi(n)$ for 3^4 and 2^{10}

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

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

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

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

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

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