and ......

# ASSIGNMENT - 1

1A. Given

$a \in Z_p$

$(a+p)^n \pmod p = a^n \pmod p$

$({}^nC_0 a^0 p^n + {}^nC_1 a^1 p^{n-1} + {}^nC_2 a^2 p^{n-2} \cdots + {}^nC_n a^n p^0) \bmod p$

$= (0 + 0 + \cdots\ 0 + a^n) \bmod p$

$= a^n \bmod p$

2A. $Z_5$ :-

$a = \{1,2,3,4\}$

$a^{-1} = \{1,3,2,4\}$

$Z_{11}$ :-

$a = \{1,2,3,4,5,6,7,8,9,10\}$

$a^{-1} = \{1,6,4,3,9,2,8,7,5,10\}$

3A. euclidean algorithm to find gcd :-

$\gcd(56245, 43159) = ?$

$56245 = 1 \times 43159 + 13086$

$43159 = 3 \times 13086 + 3901$

$13086 = 3 \times 3901 + 1383$

$3901 = 2 \times 1383 + 1135$

$1383 = 1 \times 1135 + 248$

$1135 = 4 \times 248 + 143$

$248 = 1 \times 143 + 105$

$143 = 1 \times 105 + 38$

$105 = 2 \times 38 + 29$

$38 = 1 \times 29 + 9$

$29 = 3 \times 9 + 2$

$9 = 4 \times 2 + 1$

$2 = 2 \times 1 + 0$

$\therefore \gcd(56245, 43159) = 1$

4A. $\phi(3^4)$

$\because$ 3 is a prime. w.k.t $\phi(p^e) = p^e - p^{e-1}$

$$\Rightarrow \phi(3^4) = 3^4 - 3^{4-1}$$
$$= 3^4 - 3^3$$
$$= 3^3(3-1)$$
$$= 27 \times 2$$
$$= 54$$

$$\phi(2^{10}) = 2^{10} - 2^9$$
$$= 1024 - 512$$
$$= 512$$

1/2/19

Q1) $3^{100} \bmod (31319)$

1) $100 = 1100100$

$= 2^6 + 2^5 + 2^2$

$(3)^{100} = (3)^{2^6+2^5+2^2}$

$= (3)^{2^6} \times (3)^{2^5} \times (3)^{2^2}$

$3^{100} (\bmod (31319)) = \left((3)^{2^6} \times (3)^{2^5} \times (3)^{2^2}\right) (\bmod 31319)$

$(3)^{2^0} (\bmod 31319) = 3$

2) $(3)^{2^1} \equiv ((3)^{2^0})^2$

$= 9$

$\equiv 9 (\bmod 31319)$

$(3)^{2^2} = (3^{2^1})^2$

$= 9^2 (\bmod 31319)$

$= 81 (\bmod 31319)$

3) $(3)^{2^3} = (3^{2^2})^2$

$= (81)^2 (\bmod 31319)$

$= 6561 (\bmod 31319)$

$(3)^{2^4} = (3^{2^3})^2$

$= (6561)^2 (\bmod 31319)$

$= 14415$

$$(3)^{2^5} = (3^{2^4})^2 = (14415)^2 \pmod{31319}$$

$$= 207792225 \pmod{31319}$$

$$= 21979$$

$$(3)^{2^6} = (3^{2^5})^2 = (21979)^2 \pmod{31319}$$

$$= 12185$$

$$\Rightarrow 3^{100} \pmod{31319} = (12185 \times 21979 \times 81) \bmod (31319)$$

$$= 25879 \pmod{31319}$$