15CSE341 – Cryptography

Assignment - 1

PART - A

1. Given,

$a \in \mathbb{Z}_p$.

LHS:- $(a+p)^n \pmod p$

w.k.t binomial expansion of $(x+y)^n$ is $^nC_0 x^0 y^n + {^nC_1} x^1 y^{n-1} + \cdots + {^nC_n} x^n y^0$

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

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

$= \left(0 + 0 + 0 + \cdots + 0 + (1 \times a^n \times 1)\right) \pmod p$

$\left[\because p^n \pmod p = 0 \text{ for all } n > 0\right]$

$= a^n \pmod p$

$=$ RHS.

Hence proved.

2. $\mathbb{Z}_5$, $\mathbb{Z}_{11}$.

we know that, $aa^{-1} \equiv 1 \pmod m$ & $a \neq 0$

$a \in \mathbb{Z}_m$ & $a^{-1} \in \mathbb{Z}_m$

$\mathbb{Z}_5$, $a = \{1, 2, 3, 4\}$

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

multiplicative inverse of all elements in $\mathbb{Z}_5$ are $\{1, 3, 2 4\}$

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

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

multiplicative inverse of $(\mathbb{Z}_{11}) = a^{-1}$

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

3\.

$\gcd(56245, 43159) = ?$

Euclidean Algorithm:- $[\gcd(a,b) = r_n \,;\, a > b]$

$56245 = 1 \times 43159 + 13086$

$43159 = 3 \times 13086 + 3901$

$13086 = 2 \times 3901 + 1383$

$3901 = 2 \times 1383 + 1135$

$1383 = 1 \times 1135 + 248$

$1135 = 4 \times 248 + 143$

$248 = 1 \times 143 + 105$

$143 = 1 \times 105 + 38$

$105 = 2 \times 38 + 29$

$38 = 1 \times 29 + 9$

$29 = 3 \times 9 + 2$

$9 = 4 \times 2 + 1 \rightarrow r_n$

$2 = 2 \times 1 + 0$

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

both are relatively prime.

4\.

$\phi(3^4) = ?$ $\phi(2^{10}) = ?$

w.k.t $\phi(p) = p - 1$ $[\because$ 'p' is prime$]$

$\phi(p^e) = p^e - p^{e-1}$ [from euler phi func^n property]

$\phi(3^4) = 3^4 - 3^{4-1}$ [3 is prime]

$= 81 - 27$

$\boxed{\phi(3^4) = 54}$

$\phi(2^{10}) = 2^{10} - 2^{10-1}$ [2 is prime]

$= 2^{10} - 2^9$

$= 2^9(2-1)$

$\boxed{\phi(2^{10}) = 512}$

5. Given,

$3^{100} \pmod{31319}$

consider exponent, 100 in binary

$100 = 1100100$

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

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

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

$3^{2^0} = 3$

$3^{2^1} = \left(3^{2^0}\right)^2$

$\equiv 9 \pmod{31319}$

$3^{2^2} = \left(3^{2^1}\right)^2$

$\equiv 81 \pmod{31319}$

$3^{2^3} = \left(3^{2^2}\right)^2$

$\equiv (81)^2 \pmod{31319}$

$\equiv 6561 \pmod{31319}$

$$(3)^{2^4} = \left(3^{2^3}\right)^2$$

$$\equiv (6561)^2 \pmod{31319}$$

$$\equiv 14415 \pmod{31319}$$

$$(3)^{2^5} = \left(3^{2^4}\right)^2$$

$$\equiv (14415)^2 \pmod{31319}$$

$$\equiv (207792225) \pmod{31319}$$

$$\equiv 21979 \pmod{31319}$$

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

$$\equiv (21979)^2 \pmod{31319}$$

$$\equiv 12185 \pmod{31319}$$

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

$$= (12185 \times 21979 \times 81) \bmod (31319)$$

$$= (267814115 \times 81) \bmod (31319)$$

$$\equiv (5346 \times 81) \pmod{31319}$$

$$= (433026) \pmod{31319}$$

$$= 25879 \pmod{31319}$$

$$\boxed{\therefore 3^{100} \pmod{31319} \equiv 25879}$$

PART-B

1.(a) $53947^{-1} \bmod 56211 = 7225.$

(b) $19385^{-1} \bmod 43159 = 28812$

Scanned by TapScanner