Tutorial - 4

Name = Surya Kant

Rollno = 19BCS060

Date

DELTA Pg No.

Q1 Given the super-increasing tuple b = [7, 11, 19, 39, 79, 157, 313] r = 37 and modulus n = 900, encrypt and decrypt the letter "H" using the knapsack cryptosystem. Use [4, 2 5 3 1 7 6] as the permutation table. Use ASCII value for representing H.

Sol^n

Super increasing tuple b = [7, 11, 19, 39, 79, 157, 313] r = 37

modulus n = 900 and permutation table = [4 2 5 3 1 7 6]

⇒ tuple t = [ $t_1$, $t_2$, ....., $t_7$ ]

$t_i = r \times b_i \bmod n$

$t_1 = 37 \times 7 \bmod 900 = 259$

$t_2 = 37 \times 11 \bmod 900 = 407$

$t_3 = 37 \times 19 \bmod 900 = 703$

$t_4 = 37 \times 39 \bmod 900 = 543$

$t_5 = 37 \times 79 \bmod 900 = 223$

$t_6 = 37 \times 157 \bmod 900 = 409$

$t_7 = 37 \times 313 \bmod 900 = 781$

⇒ t = [259, 407, 703, 543, 223, 409, 781]

tuple {a} = permute (t) = (using

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 4 | 2 | 5 | 3 | 1 | 7 | 6 |

tuple a = [543, 407, 223, 703, 259, 781, 409]

now, a is publicly announced (n, r and b are secret)

in ascii H = 72 ~~(8 bit) [1000110~~

in 7 bit = [1001000] = x

⇒ knapsackSum (a, x) = a [543, 407, 223, 703, 259, 781, 409]
× 1 0 0 1 0 0 0

(cipher text) S = 1246 ⇐ 543 + 0 + 0 + 703 + 0 + 0 + 0

$37^{-1} \bmod 900 = 73$

now, decrypting S = 1246

$s' = s \times r^{-1} \bmod n = 1246 \times 37^{-1} \bmod 900$

$= (1246 \times 73) \bmod 900 = 58 = s'$

$x' = $ Inv_KnapsackSum $(s', b)$

~~but it is 39+19~~ ~~58~~ 58

588

Date

DELTA Pg No.

inv-knapsacksum $(s', b)$ → { for ( i = k to 1)

if $s' \geq b_i$

{ $x_i \leftarrow 1$

$s' \leftarrow s' - b_i$

}

else $x_i \leftarrow 0$

return $x[1 \ldots k]$

}

| i | $s'$ | $b_i$ | $x_i$ |
|---|---|---|---|
| 7 | 58 | 313 | 0 |
| 6 | 58 | 157 | 0 |
| 5 | 58 | 79 | 0 |
| 4 | 58 | 39 | 1 |
| 3 | 19 | 19 | 1 |
| 2 | 0 | 11 | 0 |
| 1 | 0 | 7 | 0 |

$$x' = \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array}$$
$$x' = [0\ 0\ 1\ 1\ 0\ 0\ 0]$$
$$\begin{array}{ccccccc} 4 & 2 & 5 & 3 & 1 & 7 & 6 \end{array}$$

$x = \text{permute}(x') = [1\ 0\ 0\ 1\ 0\ 0\ 0]$

$= 64 + 8 = 72 =$ "H"

Q2 $b = [7, 11, 23, 43, 87, 173, 357]$

$r = 41$, modulus $n = 1001$, encrypt/decrypt "d" (ASII) using knapsack Cryptosystem, permutation table $= [7\ 6\ 5\ 1\ 2\ 3\ 4]$

tuple $t = [t_1, t_2, \ldots, t_7]$

$t_1 = (41 \times 7) \bmod 1001 = 287$

$t_2 = (41 \times 11) \bmod 1001 = 451$

$t_3 = (41 \times 23) \bmod 1001 = 943$

$t_4 = 41 \times 43 \bmod 1001 = 762$

$t_5 = 41 \times 87 \bmod 1001 = 564$

$t_6 = 41 \times 173 \bmod 1001 = 86$

$t_7 = 41 \times 357 \bmod 1001 = 623$

$$\begin{array}{lccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \text{tuple } t = & 287, & 451, & 943, & 762, & 564, & 86, & 623 \\ & 7 & 6 & 5 & 1 & 2 & 3 & 4 \end{array}$$

tuple $a = \text{permute}(t) = 623, 86, 564, 287, 451, 943, 762$

tuple a is publicly announced →

encryption

in ascii "d" = 100 = [1100100]

$x = [1\ 1\ 0\ 0\ 1\ 0\ 0]$

$a = [623\ 86\ 564\ 287\ 451\ 943,\ 762$

$\text{KnapsackSum}(a,x) = 1160 \Leftarrow 623 + 86 + 0 + 0 + 451 + 0 + 0$

cipher text $s = 1160$

decryption :- ~~inv knapsack~~

$s' = (1160 \times 41^{-1}) \bmod 1001$

$= (1160 \times 293) \bmod 1001$

$= 541$

$41^{-1} \bmod 900$
$= 293$

$x' = \text{Inv\_Knapsack}(s', b)$

| i | s' | bi | xi |
|---|---|---|---|
| 7 | 541 | 357 | 1 |
| 6 | 184 | 173 | 1 |
| 5 | 11 | 87 | 0 |
| 4 | . | 43 | 0 |
| 3 | . | 23 | 0 |
| 2 | 11 | 11 | 1 |
| 1 | 0 | 7 | 0 |

$$\Rightarrow x' = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \left[\begin{matrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{matrix}\right] \\ \begin{matrix} 7 & 6 & 5 & 1 & 2 & 3 & 4 \end{matrix} \end{array}$$

$x = \text{permute}(x') = [1\ 1\ 0\ 0\ 1\ 0\ 0]$

$= 64 + 32 + 4$

$= 100 =$ "d"

Q3 Using value of $p = 11$ and $q = 19$, for RSA

(i) Find the value of public key (ii) Find the value of private key

(iii) Encrypt and Decrypt the message "TO" using the key generated in (i) and (ii)

Sol (i) $p = 11,\ q = 19 \Rightarrow n = p \times q = 209$

$\phi(n) = (11-1)(19-1) = 180$

Now choose 2 exponents e and d from $Z_{180}^*$ such that

$1 < e < \phi(n)$ and e is coprime to $\phi(n)$ and $d = e^{-1} \bmod \phi(n)$

Let $e = 13 \Rightarrow d = 13^{-1} \bmod 180 = 97$

$(e, n) \rightarrow$ public key $e = 13$, $\boxed{d = 97} \leftarrow$ private key

$n = 209$ publicly announced    secret

Date
DELTA Pg No.

(iii) Encryption :- Cipher text = $(\text{plaintext}^e) \bmod n$

plaintext = "TO" = 84 79 (in ASCII)

$\Rightarrow$ Cipher text = $84^{13} \bmod 209$ , $79^{13} \bmod 209$

= 46 52

Decryption: cipher text = 46 52

plaintext = $\text{ciphertext}^d \bmod n$

= $46^{37} \bmod 209$ $52^{37} \bmod 209$

= 84 79

= "T O"

Q4 In RSA cryptography find d if you know e = 17 and n = 187

$d = e^{-1} \bmod n$

$d = 17^{-1} \bmod 187$ gcd (17, 187) = 17 ≠ 1

$x \times 17 \bmod 187 = 1$ $\Rightarrow$ no inverse possible

Q5 c = 10 , e = 5 , n = 35 , In RSA eve intercept ciphertext c find plaintext public key

$p = c^d \bmod 35$

$d = 5^{-1} \bmod 35$ again gcd (5, 35) = 5 ≠ 1

$\Rightarrow$ no plaintext found. $\Rightarrow$ no inverse possible.

Q6 In Rabin cryptosystem, user A chooses two prime nos. p = 23, q = 7 encrypt and decrypt plaintext P = 24 using this method

Q3(iii) other method

$n$ bada chahiye 1914 se.

(iii) encryption

ciphertext $C = P^e \bmod n$

plaintext = "TO" = 1914

$C = 1914^{13} \bmod 209 = 158$

now $1914 > 209$
(Text) $> n$
and $C < n$
$P < n$

decryption

plaintext $P = C^d \bmod n$

$P = 158^{97} \bmod 209$

$= 133$ ?  ans nahi nikal raha 133 hi aa raha

$19^{13} \bmod 209 = 171$
$14^{13} \bmod 209 = 192$

decryption

$171^{97} \bmod 209 = 19 = T$
$192^{97} \bmod 209 = 14 = O$

Ans 6

i) Key generation :- $p$ and $q$ in the form $4k+3$ ~~and $p \neq q$~~
$p = 23$, $q = 7$

$n = 23 \times 7$

(public key) $n = 161$  private key $= (23, 7) \leftarrow (p, q)$

publicly announce

ii) Encryption $C = P^2 \bmod n$

$C = 24^2 \bmod 161$

ciphertext $C = 93$ → sent

iv) Decryption B receives 93 as ciphertext

$a_1 = +93^{\left(\frac{23+1}{4}\right)} \bmod 23 = 1 \bmod 23 = 1$

$a_2 = -93^{\left(\frac{23+1}{4}\right)} \bmod 23 = 22 \bmod 23 = 22$

$b_1 = +93^{\left(\frac{7+1}{4}\right)} \bmod 7 = 4 \bmod 7 = 4$

$b_2 = (-93)^{\left(\frac{7+1}{4}\right)} \bmod 7 = 3 \bmod 7 = 3$

⇒ $P1 = (a_1, b_1) = 116$  $P3 = (a_2, b_1) = 137$

$P2 = (a_1, b_2) = 24$  $P4 = (a_2, b_2) = 45$

(according to chinese remainder theorem)
Search it

Q7 In ElGamal, given the prime $p = 31$:

a) Chose an appropriate $e1$ and $d$; then calculate $e2$.

b) Encrypt the message "HELLO", use 00 to 25 for encoding.

c) Decrypt the cipher text to obtain plaintext.

Date
DELTA Pg No.

Q7

1) Key generation    select large prime $p = 31$ (given)

$e1 =$ given primitive root of 31   such that $e1^i \bmod 31 = \{1 \text{ to } 30\}$

We have 8 primitive roots of 31

$e1$ 3, 11, 12, 13, 17, 21, 22 and 24

$\Rightarrow e1 = 3$

$d = 10, 0 < d < p-2$

$\Rightarrow$

$e2 = 3^{10} \bmod 31 = 25$

public key $(e_1, e_2, p) = 3, 25, 31$

private key $(d) = 10$

2) encryption :- select random $r$ in group $G = \langle Z_{31}^*, X \rangle$

let $r = 7$

$\Rightarrow C_1 = e_1^r \bmod p = 3^7 \bmod 31 = 17$

$C_2 = (P \times e_2^r) \bmod p$    for $C_2$  $e^7 \bmod 21 = 25^7 \bmod 31 = 25$

| | Plaintext | $C(C_1, C_2)$ | | |
|---|---|---|---|---|
| H | 7 | 17,20 | for P = H | $C_2 = (7 \times 25^7) \bmod 31 = 7 \times 25 \bmod 31 = 20$ |
| E | 4 | 17,7 | ← P = E | $C_2 = (4 \times 25^7) \bmod 31 = 7 = 4 \times 25 \bmod 31 = 7$ |
| L | 11 | 17,27 | ← P = L | $C_2 = (11 \times 25^7) \bmod 31 = (11 \times 25 \bmod 31) = 27$ |
| L | 11 | 17,27 | ← P = L | $C_2 = (11 \times 25^7) \bmod 31 = (11 \times 25 \bmod 31) = 27$ |
| O | 14 | 17,9 | ← P = O | $C_2 = (14 \times 25^7) \bmod 31 = (14 \times 25 \bmod 31) = 9$ |

~~$(17^{10})^{-1} \bmod 31 = 25$~~

decryption :-

$P = [C_2 (C_1^d)^{-1}] \bmod p$

| C | P | text |
|---|---|---|
| 17,20 | $20 \times (17^{10})^{-1} \bmod 31 = 7$ | H |
| 17,7 | $7 \times (17^{10})^{-1} \bmod 31 = 4$ | E |
| 17,27 | $27 \times (17^{10})^{-1} \bmod 31 = 11$ | L |
| 17,27 | $27 \times (17^{10})^{-1} \bmod 31 = 11$ | L |
| 17,9 | $9 \times (17^{10})^{-1} \bmod 31 = 14$ | O |

CamScanner

Date
DELTA Pg No.

Q8 Assume that Alice uses Bob's ElGamal public key ($e1 = 2$) to send two messages $P1 = 17$ and $P2 = 37$ using same random integer $r = 9$. Eve intercepts the cipher text and somehow finds the value of $P1 = 17$. Show how Eve can use a known plaintext attack to find the value of P2. Assume the value of modulus $p = 53$ and $d = 3$

Sol^n

Known-Plaintext Attack :- if Alice uses same random exponent $r$, to encrypt 2 plaintexts $P$ and $P'$, Eve discovers $P'$ if she knows P.

Assume, that $C_2 = P \times e_2^r \bmod p$ and $C_2' = p' \times e_2^r \bmod p$.

Eve finds $P'$ using following steps:

1. $(e_2^r) = C_2 \times P^{-1} \bmod p$
2. $p' = C_2' \times (e_2^r)^{-1} \bmod p$

Alice should use new $r$ value to thwart the known-plaintext attack

$\Rightarrow$ $P_1 = 17$, $P_2 = 37$, $r = 9$, $e1 = 2$, $p = 53$

even knows $P_1 = 17$

$\Rightarrow$ $C_2 = P_1 \times 2^9 \bmod 53$ and $C_2' = P_2 \times 2^9 \bmod 53$

$C_2 = 17 \times 2^9 \bmod 53 = 12$ $= 37 \times 2^9 \bmod 53 = 23$

eve intercepts

$\Rightarrow C_2 = 23$

$C_2' = 23$

Step 1 :- $e_2^9 = C_2 \times P_1^{-1} \bmod p$

$= 12 \times 17^{-1} \bmod 53$

$= 12 \times 25 \bmod 53$

$= 35$

Step 2 $P_2 = C_2' \times (35)^{-1} \bmod 53$

$= 23 \times (35)^{-1} \bmod 53$

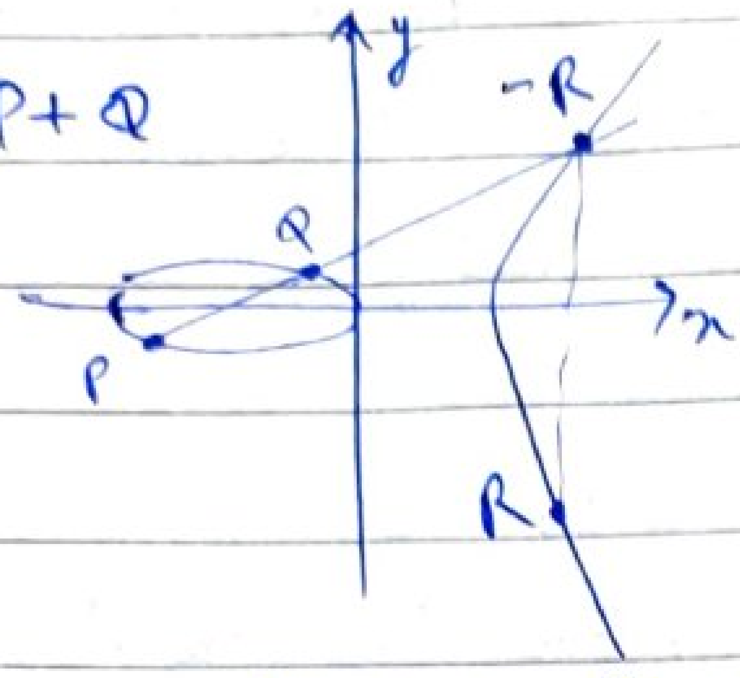
$P_2 = 23 \times 50 \bmod 53$

$\boxed{P_2 = 37}$ ← Now eve knows what $P_2$ was.

$E_p(a,b) \Rightarrow a=1, b=1$

Q9 If 2 points on the Elliptical curve $E_{23}(1,1)$ is defined as $P(3,10)$ and $Q(9,7)$, then find the value of :- (i) $P+Q$ (ii) $4P$

(i) $R = P+Q$




$P(x_1,y_1)$, $Q(x_2,y_2)$, $R(x_3,y_3)$

↑ not known

$\lambda = (y_2-y_1)/(x_2-x_1)$

$x_3 = \lambda^2 - x_1 - x_2$ $\quad y_3 = \lambda(x_1-x_3)-y_1$

$\lambda = (7-10)\times(9-3)^{-1} \bmod 23$

$= -3\times 6^{-1} \bmod 23$

$= -3\times 4 \bmod 23$

$= -12 \bmod 23$

$= 11 \bmod 23$

$\lambda = 11$

$(6\times 4) \bmod 23 = 24 \bmod 23 = 1$

$23-12 = 11$

$x_3 = (11^2-3-9) \bmod 23 = (121-12) \bmod 23$

$= 109 \bmod 23$

$= 17 \bmod 23$

$= 17$

$23\times 4$, $92$, $109-92$

$y_3 = (11\times(3-17)-10) \bmod 23 = -164 \bmod 23$

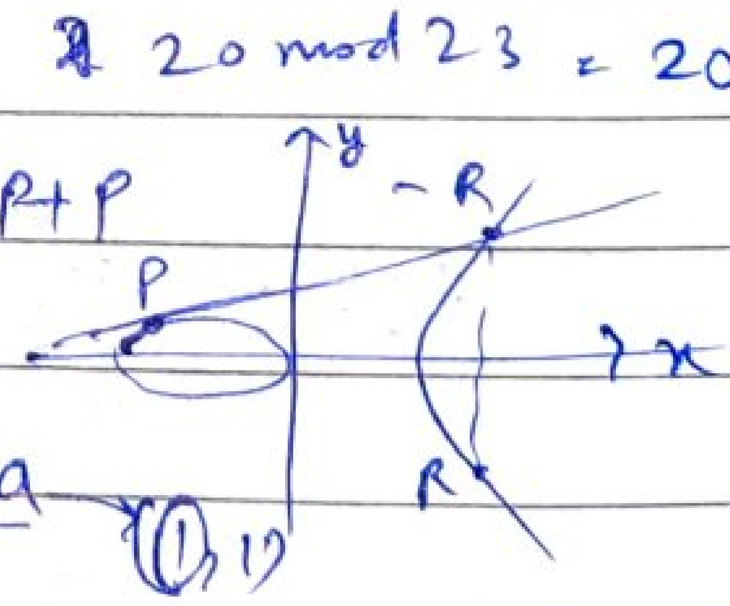
$= (184-164) \bmod 23$

$= 20 \bmod 23 = 20$

$184$, $23$, $23\times 8$

$\Rightarrow R = P+Q = (x_3,y_3) = (17,20)$

(ii) $R = 4P = 2P+2P = 2R' \Rightarrow R' = 2P = P+P$




$R = P+P$

for $R' = 2P$ $\quad P=(3,10)$ $\quad \lambda = \frac{3x_1^2+a}{2y_1}$ $(1,1)$

$\lambda' = (3\times 3^2+1)\times(2\times 10)^{-1} \bmod 23$ $\quad \Big|\; x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1-x_3)-y_1$

$= 28\times 20^{-1} \bmod 23$

$= 28\times 15 \bmod 23$

$\boxed{\lambda' = 6} \Rightarrow x_3' = (6^2-3-3) \bmod 23$, $\quad y_3' = (6(3-7)-10) \bmod 23$

$= (36-6) \bmod 23$ $\quad = -34 \bmod 23$

$x_3 = 30 \bmod 23$ $\quad = (46-34) \bmod 23$

$x_3 = 7$ $\quad = 12$

$R' = (7,12)$

In RSA cryptography find $d$ if you know $e=17$ and $n=187$

DELTA Pg No.

Q4 $d = e^{-1} \bmod \phi(n)$

$n = 187 = \underset{p}{11} \times \underset{q}{17}$

$gcd(17, 160) = 1$

$\phi(n) = (11-1) \times (17-1)$

$= 10 \times 16 = 160$

$(d \times e) \bmod \phi(n) = 1$

$d = 17^{-1} \bmod 160 = 113$

$e, \phi(n)$ coprime

$\Rightarrow$

Q5 In RSA eve intercepts ciphertext $c = 10$, $\underbrace{e=5, n=35}_{\text{publickey}}$ find plain text

$P = C^d \bmod n$

$n = 35 = 5 \times 7 = p \times q$

$\phi(n) = (p-1)(q-1) = (5-1)(7-1) = 4 \times 6 = 24$

$d = e^{-1} \bmod \phi(n)$

$= 5^{-1} \bmod 24$

$5 \times 5 = 25 \bmod 24 = 1$

$d = 5$

$\Rightarrow p = 10^5 \bmod 35$

$= 5$

$\frac{100000}{35} = 2857 \frac{5}{35}$

contd.

Q9 (i) now $R' = 2P = (x_3, y_3) = (7, 12)$

$R = 2R' = 4P = 2R' = ?$

$\lambda = (3 \times 7^2 + 1) \times (2 \times 12)^{-1} \bmod 23$

$24 \times 1 \bmod 23 = 1$

$= 148 \times 24^{-1} \bmod 23$

$= 148 \times 1 \bmod 23 = 10$

$x_3 = (10^2 - 7 - 7) \bmod 23$

$= (100 - 14) \bmod 23$

$= 17$

$y_3 = (10(7-17) - 12) \bmod 23$

$= -112 \bmod 23$

$= 115 - 112 \bmod 23$

$23 \times 5$
$115$

$= 3 \bmod 23$

$= 3$

$\Rightarrow R = 4P = (17, 3)$

Q10. An elliptic curve is defined by $y^2 = x^3 + 2x + 9$ with a modulus of $p = 37$ for the elliptical curve cryptosystem. Determine any five points on this curve.

Date / DELTA Pg No.

| $x$ | RHS = $(x^3+2x+9) \bmod 37$ | perfect square ? | $y = \sqrt{RHS}$ | $(x, y)$ |
|---|---|---|---|---|
| 0 | $9 \bmod 37 = 9$ | ✓ | $\pm 3$ | $(0,3), (0,34)$ |
| 1 | $(1+2+9) \bmod 37 = 12$ | $12$ ✗ $(12+37) = 49$ ✓ | $\pm 7$ | $(1,7), (1,30)$ |
| 2 | $(8+4+9) \bmod 37 = 21$ | $21$ ✗, $21+37 = 58$ ✗ <br> $58+37 = 95$ ✗ <br> $95+37 = 132$ ✗ <br> $132+37 = 169$ ✓ | $\pm 13$ | $(2,13), (2,24)$ |

$\Rightarrow$ any 5 points on the curve are $(0,3), (0,34), (1,7), (1,30), (2,13)$

Q11. An elliptical curve is defined by $y^2 + xy = x^3 + g^3x^2 + b$ is defined over $GF(2^3)$ with irreducible polynomial $f(x) = x^3 + x + 1$. Find all points existing $(b = 1)$

Q12 (same as Q11) An elliptical curve $y^2 + xy = x^3 + ax^2 + 1$ is defined over $GF(2^3)$ with irreducible polynomial $f(x) = x^3 + x + 1$. Find all points existing on this curve with $a = g^3$ and $b = 1$ $\Rightarrow$ elliptical equation $\Rightarrow$ $y^2 + xy = x^3 + g^3x^2 + 1$

Q11 An elliptical curve $y^2 + xy = x^3 + g^3x^2 + 1$ is defined over $GF(2^3)$ with irreducible polynomial $f(x) = x^3 + x + 1$. Find all possible existing points on this curve.

**and Q12**

$$y^2 + xy = x^3 + \underset{a}{g^3}x^2 + \underset{b}{1}$$

$IP = f(x) = x^3 + x + 1 = 0 \Rightarrow g^3 + g + 1 = 0$

$g^3 = -g - 1$

$g^3 = g + 1$

$\boxed{F_{2^3} = F_{p^m}}$ $\quad GF(2^3)$

$x, y \in \{0, 1, g, g^2, g^3, g^4, g^5, g^6\}$

$(x,y) = \{ (0,0)\ (0,1),\ (0,g),\ (0,g^2),\ (0,g^3),\ (0,g^4),\ (0,g^5),\ (0,g^6)$

$(1,0)\ (1,1)\ (1,g)\ (1,g^2)\ (1,g^3)\ (1,g^4),\ (1,g^5),\ (1,g^6)$

$(g,0)\ (g,1)\ (g,g)\ (g,g^2)\ (g,g^3)\ (g,g^4),\ (g,g^5),\ (g,g^6)$

$(g^2,0)\ (g^2,1)\ (g^2,g)\ (g^2,g^2)\ (g^2,g^3)\ (g^2,g^4)\ (g^2,g^5),\ (g^2,g^6)$

$(g^3,0)\ (g^3,1)\ (g^3,g)\ (g^3,g^2)\ (g^3,g^3)\ (g^3,g^4)\ (g^3,g^5),\ (g^3,g^6)$

$(g^4,0)\ (g^4,1)\ (g^4,g)\ (g^4,g^2)\ (g^4,g^3)\ (g^4,g^4)\ (g^4,g^5),\ (g^4,g^6)$

$(g^5,0)\ (g^5,1)\ (g^5,g)\ (g^5,g^2)\ (g^5,g^3)\ (g^5,g^4)\ (g^5,g^5),\ (g^5,g^6)$

$(g^6,0)\ (g^6,1)\ (g^6,g)\ (g^6,g^2)\ (g^6,g^3)\ (g^6,g^4)\ (g^6,g^5),\ (g^6,g^6) \}$

| $(x,y)$ | LHS = $(y^2 + xy)$ mod IP | RHS = $(x^3 + g^3x^2 + 1)$ mod IP | LHS=RHS |
|---|---|---|---|
| $(0,1)$ | $(1^2 + 0) \bmod (g^3+g+1) = 1$ | $(0 + 0 \times g^3 + 1) \bmod g^3+g+1 = 1$ | Yes |
| $(g^2,1)$ | $(1^2 + g^2) \bmod (g^3+g+1) = 1+g^2$ | $g^6 + g^7 + 1 = (g^3)^2[1+g]+1$<br>$= (g+1)^2(1+g)+1$<br>$= (g^2+1)(1+g)+1$<br>$= g^2 + \cancel{1} + g^3 + g + \cancel{1}$<br>$= g^2 + g + 1 + g$<br>$= g^2+1$ | Yes |
| $g^3, g^2$ | $g^4 + g^5 = g(g+1)[1+g] = g(g^2+1)$<br>$= g^3 + g$<br>$= \cancel{g}+1+\cancel{g} = 1$ | $\cancel{g^9} + \cancel{g^9} + 1 = 1$ | Yes |
| $g^5, 1$ | $1 + g^5 = 1 + g^2(g+1) = 1+g^3+g^2$<br>$= \cancel{1}+\cancel{1}+g+g^2$<br>$= g^2+g$ | $g^{15} + g^{13} + 1 = g^{13}(1+g^2)+1$<br>$g(g^3)^4(1+g^2)+1 = g(g+1)^4(1+g^2)+1$<br>$= g(g^4+g+1)(1+g^2)+1$<br>$= (g^4+g^2+1)(1+g^2)+1 = (g^4+g)(g+1)$<br>$= g^5 + g + g^2 + g^3 = g^2 + g^3 + g^2 + g + 1$<br>$= g^2 + g + \cancel{1} + \cancel{1}$<br>$= g^2+g$ | Yes |
| $g^6, g$ | $g^2 + g^7 = g^2 + g(g^3)^2 = g^2 + g(g+1)^2$<br>$= g^2 + g(g^2+1)$<br>$= g^2 + g^3 + g = g^2 + g + 1 + g$<br>$= g^2+1$ | $g^{18} + g^{15} + 1 = g^{15}(g^3+1)+1$<br>$= (g+1)^5(g)+1 = (g+1)(g^4+1)g+1$<br>$= (g^5+g+g^4+1)g+1 = (g^2+g^3+g+g^2+g+1)g+1$<br>$(g+1+1)g+1$<br>$= g^2+1$ | Yes |

Q13 An elliptical curve $y^2+xy=x^3+ax^2+b$ is defined over $GF(2^4)$ with irreducible polynomial $f(x)=x^4+x+1$. Find any 7(seven) points exist on this curve with $a=g^4$ and $b=g^0$.

$GF(2^4) \Rightarrow$ 0 to $g^{2^4-2}$ = 0 to $g^{14}$ ← $(x,y)$

Can assume these values:- $(x,y) = \{(0,0), (0,1), (0,g), (0,g^2) \ldots (0,g^{13}), (0,g^{14}),$
$(1,0), (1,1)$
⋮
$(g^{14},0), (g^{14},1) \ldots (g^{14},g^{13}), (g^{14},g^{14})\}$

| $(x,y)$ | LHS $=(y^2+xy)$ mod IP | RHS $=(x^3+g^4x^2+1)$ mod $(g^4+g+1)$ | LHS = RHS |
|---|---|---|---|
| $(0,1)$ ① | $(1+0)$ mod $g^4+g+1=1$ | $(0+0+1)$ mod $g^4+g+1=1$ | Yes |
| $(1,g^6)$ ② | $(g^{12}+g^6)$ mod $g^4+g+1$ <br> $=g^{4+2}(g^{4+2}+1)$ <br> $=g^2(g+1)(g^2(g+1)+1)$ <br> $=(g^3+g^2)(g^3+g^2+1)$ <br> $=g^6+\cancel{g^5}+g^3+\cancel{g^5}+g^4+g^2$ <br> $=\cancel{g^3}+g^2+\cancel{g^3}+g^4+g^2$ <br> $=g+1$ | $(\cancel{1}+g^4+\cancel{1})$ mod $g^4+g+1$ <br> $=g+1$ | Yes |

Date
Pg No.

LHS | RHS

$(1, g^{13})$ ③

$(g^{26} + g^{13}) \bmod g^4+g+1$
$= (g+1)^6 \cdot g^2 + (g^4+1)^3 g$
$= (g^6 + g^4 + g^2 + 1) g^2 + (g^3+g^2+g+1) g$
$= (g^3+\cancel{g^2}+g+\cancel{1} + \cancel{g^2}+\cancel{1}) g^2 + (g^4+g^3+g^2+g)$
$= g^5 + \cancel{g^4} + \cancel{g}+1 + g^3+g^2+\cancel{g}$
$= g^2+g + \cancel{g^2}+1.$
$= g+1$

$(\cancel{1}+g^4+\cancel{1}) \bmod g^4+g+1$
$= g+1$
(Same as prev point)

Yes

$(g^3, g^8)$ ④

$(g^{16}+g^{11}) (\bmod g^4+g+1)$
$= (g^4)^4 + (g^4)^2 \cdot g^3$
$= (g+1)^4 + (g+1)^2 g^3$
$= g^4+1 + (g^2+1) g^3$
$= g+\cancel{1}+\cancel{1} + g^5+g^3$
$= \cancel{g} + g^2+\cancel{g} + g^3$
$= g^3+g^2$

$(g^9+g^{10}+1) (\bmod g^4+g+1)$
$= g(g^4+1)^2 + g^2(g+1)^2+1$
$= g(g^2+1) + g^2(g^2+1)+1$
$= g^3+g + g^4+g^2+1$
$= g^3+\cancel{g}+\cancel{g}+\cancel{1}+g^2+\cancel{1}$
$= g^3+g^2$

Yes

$(g^3, g^{13})$ ⑤

$(g^{26} + g^{16}) (\bmod g^4+g+1)$
$= g^5+g^3 + g$
$= g^2+\cancel{g}+g^3+\cancel{g}$
$= g^3+g^2$

$(g^9+g^{10}+1) \bmod g^4+g+1$
$= g^3+g^2$
same

Yes

$(g^5, g^3)$ ⑥

$(g^6+g^8) (\bmod g^4+g+1)$
$= g^2(g+1) + (g+1)^2$
$= g^3+\cancel{g^2}+ g^2+1$
$= g^3+1$

$(g^{15}+g^{14}+1) (\bmod g^4+g+1)$
$= g^3(g+1)^3 + g^2(g+1)^3+1$
$= g^3(g^3+g^2+g^2+1) + g^2(g^3+g^2+g+1)+1$
$= g^6+g^5+g^4+g^3 + g^5+g^4+g^3+g^2+1$
$= g^3+g^2 + g^2+1 = g^3+1$

Yes

$(g^5, g^4)$ ⑦

$(g^{22}+g^{16}) (\bmod g^4+g+1)$
$= g^2(g+1)^5 + g$
$= g^2(g+1)(g^4+1) + g$
$= g^2(g+1)g + g = g^3(g+1)+g$
$= g^4+g^3+g = \cancel{g}+1+g^3+\cancel{g}$
$= g^3+1$

$(g^{15}+g^{14}+1)(\bmod g^4+g+1)$
$= g^3+1$
same

Yes