Network Security Assignment

Rayyan Haque
19BCS029.
VIIIth Sem
BTech. CSE.

Ans = 1

$39x + 15y = 270$

$d = \gcd(39, 15) = 3$

$d \mid c \rightarrow \infty$ solⁿ

$d \nmid c \rightarrow$ no solⁿ

Divide both sides by 3

$13x + 5y = 90$

Using the extended algorithm we will find s and t such that

$13s + 5t = 1$

$s = 2 \quad t = -5$

Particular solⁿ $x_0 = \left(\frac{c}{d}\right)s \qquad y_0 = \left(\frac{c}{d}\right)t$

General solⁿ $x = x_0 + k\left(\frac{b}{d}\right) \qquad y = y_0 - k\left(\frac{a}{d}\right)$

Particular solⁿ $x_0 = \left(\frac{270}{3}\right) \times 2 = 180 \qquad y_0 = \left(\frac{270}{3}\right) - 5 = -450$

General solⁿ $x = 180 + k\left(\frac{15}{3}\right) \qquad y = -450 - k\left(\frac{39}{3}\right)$

$= 180 + 5k \qquad = -450 - 13k$

(To find non neg.) values

$k = -35 \quad x = 5 \quad y = 5 \qquad k = -36 \quad x = 0 \quad y = 18$

Teacher's Signature..............

Ans = 2 i) $256x \equiv 442 \pmod{60}$

$ax \equiv b \pmod{n}$

$d = \gcd(a, n)$

$$\begin{cases} d \nmid b & \text{no sol}^n \\ d \mid b & d \text{ sol}^n \end{cases}$$

Divide eq^n by d

Multiply both eq^n by multiplicative inverse of a

$x = x_0 + k\left(\frac{n}{d}\right)$ $k = 0, 1 \ldots (d-1)$

$256x \equiv 442 \pmod{60}$

$d = \gcd(256, 60)$

$d = 4$

~~442/4~~ $d \nmid b$ no sol^n

ii) $232x + 42 \equiv 248 \pmod{50}$

First change this in the form

We add -42 (additive inverse of 42) to both sides

$232x \equiv 206 \pmod{50}$

$d = \gcd(232, 50) = 2$

$d \mid b$ d sol^n

2 sol^n

Divide by d

$$116x \equiv 103 \pmod{25}$$

$$x = 103\,(116^{-1}) \pmod{25}$$

$$x_0 = 103 \times 11 \pmod{25} = 8$$

$$x_1 = 8 + 1 \times \left(\frac{50}{2}\right) = 33$$

Ans=3 $P_1 = (x^5 + x^2 + x)$ ⊗ Q^7

$P_2 = (x^7 + x^4 + x^3 + x^2 + x)$

$GF(2^8)$

irreducible polynomial $(x^8 + x^4 + x + 1)$

$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x$
$+ x(x^7 + x^4 + x^3 + x^2 + x)$

$= x^{12} + \cancel{x^9} + x^8 + x^7 + \cancel{x^6} + \cancel{x^9} + \cancel{x^6} + \cancel{x^5} + \cancel{x^4} + \cancel{x^3}$
$+ \cancel{x^8} + \cancel{x^5} + \cancel{x^4} + \cancel{x^3} + x^2$

$= (x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x + 1)$

$$
\begin{array}{r|l}
 & x^4 + 1 \\
x^8 + x^4 + x + 1 & \cancel{x^{12}} + x^7 + x^2 \\
 & \cancel{x^{12}} + x^8 + x^5 + x^4 \\
\hline
 & x^8 + x^7 + x^5 + x^4 + x^2 \\
 & x^8 + x^4 + x + 1 \\
\end{array}
$$

Remainder $\Rightarrow \boxed{x^7 + x^5 + x^2 + x + 1}$

Teacher's Signature..............

Ans-4

$$x \equiv 2 \pmod 3 \qquad x \equiv a_1 \pmod{m_1}$$
$$x \equiv 3 \pmod 5 \qquad x \equiv a_2 \pmod{m_2}$$
$$x \equiv 2 \pmod 7 \qquad x \equiv a_k \pmod{m_k}$$

i) Find M $\quad M = m_1 \times m_2 \times m_3 \text{ --- } m_k$

$$= 3 \times 5 \times 7 = 105$$

ii) $M_1 = \frac{M}{m_1} \rightarrow \frac{105}{3} = 35 \qquad M_2 = \frac{105}{5} = 21 \qquad M_3 = \frac{105}{7} = 15$

iii) $M_1^{-1} = 2 \qquad M_2^{-1} = 1 \qquad M_3^{-1} = 1$

iv) $x = (a_1 \times M_1 \times M_1^{-1} + a_2 * M_2 \times M_2^{-1} \text{ --- }) \bmod M$

$$x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$$
$$= 23 \bmod 105$$

Ans:5 (i) $44^{-1} \bmod 667$

$44^{\phi(667)-1} \bmod 667$

$44^{\phi(23)\,\phi(29)-1} \bmod 667$

$\phi(23) \times \phi(29) = 22 \times 28 = 616$

$44^{615} \bmod 667$

	Multiplication $(y=1)$	Squaring $(a=44)$
1	$y = 1 \times 44 \bmod 667 = 44$	$44^2 \bmod 667 = 602$
1	$y = 44 \times 602 \bmod 667 = 475$	$602^2 \bmod 667 = 223$
1	~~$y = 475 \times 223$~~ $y = 475 \times 223 \bmod 667 = 539$	$223^2 \bmod 667 = 371$
0		$371^2 \bmod 667 = 239$
0		$239^2 \bmod 667 = 426$
1	$y = 539 \times 426 \bmod 667 = 166$	$426^2 \bmod 667 = 52$
1	$y = 166 \times 52 \bmod 667 = 628$	$52^2 \bmod 667 = 36$
0		$36^2 \bmod 667 = 629$
0		$629^2 \bmod 667 = 110$
1	$y = 628 \times 110 \bmod 667 = 379$	$110^2 \bmod 667 = 94$

379

(ii) $(17364)^{41} \bmod 2134$

$y = 1$ $\qquad$ $a = 17364$

1 $\qquad y = 1 \times 17364 \bmod 2134$ (292) $\qquad a = 17364^2 \bmod 2134 = 2038$

0 $\qquad a = 2038^2 \bmod 2134 = 680$

0 $\qquad a = 680^2 \bmod 2134 = 1456$

1 $\qquad y = 292 \times 1456 \bmod 2134$ $\qquad a = (1456)^2 \bmod 2134 = 874$

0 $\qquad \cancel{425152} = 486$ $\qquad a = (874)^2 \bmod 2134 = 2038$

1 $\qquad \cancel{y = 425152 \times 2038 \bmod 2134}$

$y = 486 \times 2038 \bmod 2134$

$= \underline{\underline{292}}$

Ans = 6 (x^3+x+1) modulus (x^4+x+1) $(t_1 - q \times t_2)$

q	r_1	r_2	r	t_1	t_2	t
(x)	(x^4+x+1)	(x^3+x+1)	(x^2+1)	(0)	(1)	(x)
(x)	(x^3+x+1)	(x^2+1)	(1)	(1)	(x)	x^2+1
x^2+1	x^2+1	1	0	x	x^2+1	x^4+x+1
	1	0		x^2+1	x^4+x+1	$(x^2+1)(x^2+1)$
						$x^4+x^2+x^2+1$

This mean $(x^3+x+1)^{-1}$ modulo (x^4+x+1) is (x^2+1)

Ans = 7

Using base 2

$$n-1 = m \times 2^k$$

$$2047 - 1 = 1023 \times 2^1 \qquad m = 1023$$

$$k = 1$$

$$T = 2^{1023} \bmod 2047 \qquad a = 2$$

1	$y = 1 \times 2 \bmod 2047 = 2$	$a = 2^2 \bmod 2047 = 4$
1	$y = 2 \times 4 \bmod 2047 = 8$	$a = 4^2 \bmod 2047 = 16$
1	$y = 8 \times 16 \bmod 2047 = 128$	$a = 16^2$ ——— $= 256$
1	$y = 128 \times 256 \bmod 2047 = 16$	$a = 256^2 \bmod 2047 = 32$
1	$y = 16 \times 32 \bmod 2047 = 512$	$a = 32^2 \bmod 2047 = 1024$
1	$y = 512 \times 1024 \bmod 2047 = 256$	$a = 1024^2 \bmod 2047 = \cancel{256}\ 512$
1	$y = 256 \times 512 \bmod 2047 = 64$	$a = 512^2 \bmod 2047 = 128$
1	$y = 64 \times \cancel{128} \bmod 2047 = 4$	$a = 128^2 \bmod 2047 = 8$
1	$y = 4 \times 8 \bmod 2047 = 32$	$a = 8^2 \bmod 2047 = 64$
1	$y = 32 \times 64 \bmod 2047 = 1$	$a = 64^2 \bmod 2047 = 2$

~~composite~~

$$2^{1023} \bmod 2047 = (2 \times 4 \times 16 \times 256 \times 32 \times 1024 \times 512 \times 128 \times 8 \times 64 \times 2) \bmod 2047$$

$$= 1.$$

hence it is prime//

Ans = 8

Elements of the field $GF(2^4)$

$F(x) = x^4 + x + 1$ $\qquad$ $N = 2^4 - 2 = 14$

$0 \longrightarrow 0000$

$g^0 \longrightarrow 0001$

$g^1 \longrightarrow 0010$

$g^2 \longrightarrow 0100$

$g^3 \longrightarrow 1000$

$g^4 \rightarrow (g+1) \quad 0011$

$g^5 \longrightarrow g(g+1) = g^2+g = 0110$

$g^6 \longrightarrow g(g^5) = g(g^2+g) = g^3+g^2 = 1100$

$g^7 \rightarrow g(g^6) = g(g^3+g^2) = g^4+g^3 = 1011 \quad (g^3+g+1)$

$g^8 \longrightarrow \cancel{g(g^7) = g(g^4+g^3) = g^5+g^4 = g^2+g+g^4}$

$g(g^7) = g(g^3+g+1) = g^4+g^2+g = g^2+1 = 0101$

$g^9 \longrightarrow g(g^8) = g(g^2+1) = g^3+g = 1010$

$g^{10} \longrightarrow g(g^9) = g(g^3+g) = g^2+g+1 = 0111$

$g^{11} \longrightarrow g(g^{10}) = g^3+g^2+g = 1110$

$g^{12} = g(g^{11}) = g^4+g^3+g^2 = g^3+g^2+g+1 = 1111$

$g^{13} = g(g^{12}) = g^4+g^3+g^2+g = g^3+g^2+1 = 1101$

$g^{14} = g(g^{13}) = g(g^3+g^2+1) = g^4+g^3+g = g^3+1 = 1001$

$g^{-3} = g^{12}$

$(-3 \bmod 15 = 12)$

Q9 Order of elements

Ord(1) = 1	Ord(4) = 9	Ord(6) = 9	Ord(9) = 9	Ord(12) = 6
Ord(2) = 18	Ord(4) = 9	Ord(7) = 3	Ord(10) = 18	Ord(13) = 18
Ord(3) = 18	Ord(5) = 9	Ord(8) = 6	Ord(11) = 3	Ord(14) = 18
Ord(15) = 18	Ord(16) = 9	Ord(17) = 9	Ord(18) = 2	

No. of primitive roots is 6

Q19 $2x^{11} \equiv 22 \pmod{19}$

Logarithmic root

x	1	2	3	4	5	6	7	8	9	10	11	12
$L_2 x$	18	1	13	2	16	14	6	3	8	17	12	15

$L_2(2x^{11}) = L_2(3) \pmod{18}$

$L_2(2) + 11 \times L_2(x) = L_2(3) \pmod{18}$

$11 \times L_2(x) = 12 \pmod{18}$

$11 \times y = 12 \pmod{18}$

$y = 11^{-1} \times 12 \pmod{18}$

$= 6 \pmod{18}$

$\boxed{x = 7}$

Teacher's Signature : ____________

Ans = 11

$x^2 \equiv a \bmod p$

$p \rightarrow$ prime $\quad p \nmid a \quad$ no solⁿ

two incongruent solⁿ

a is Quadratic residue $\quad$ 2 solⁿ

QNR $\quad$ no solⁿ

How to Check?

$a^{(p-1)/2} \equiv 1 \quad$ QR

$a^{(p-1)/2} \equiv -1 \quad$ QNR

a) $x^2 \equiv 3 \pmod{23}$

$$\left[\begin{array}{l} p = 4k+3 \text{ form} \qquad a \rightarrow QR \\ x \equiv a^{(p+1)/4} \bmod p \\ x \equiv -a^{(p+1)/4} \bmod p \end{array}\right.$$

$x \equiv 3^6 \bmod 23$

$= \pm 16 \bmod 23$

$\sqrt{3} \equiv \pm 16 \pmod{23}$

b) $x^2 \equiv 7 \pmod{19}$ $\qquad x \equiv 7^5 \pmod{19}$

$x \equiv \pm 11 \pmod{19}$

$\sqrt{7} \equiv \pm 11 \pmod{19}$

Teacher's Signature.........

Ans = 12

(1) $t = t_1 - q \times t_2$

q	r_1	r_2	r	t_1	t_2	t
x	x^3+x^2+1	x^2	x^2+1	0	1	x
1	x^2	x^2+1	1	1	x	$x+1$
x^2+1	x^2+1	1	0	x	$x+1$	x^3+x^2+1
	1	0		$x+1$	x^3+x^2+1	

$\boxed{x+1}$

(2) x^2+1

q	r_1	r_2	r	t_1	t_2	t
x	x^3+x^2+1	x^2+1	x^2+x+1	0	1	x
1	x^2+1	x^2+x+1	x	1	x	$x+1$
x	x^2+x+1	x	$x+1$	x	$x+1$	x^2
1	x	$x+1$	1	$x+1$	x^2	x^2+x+1
$x+1$	$x+1$	1	0	x^2	x^2+x+1	x^3+x^2+1
	1	0		x^2+x+1	x^3+x^2+1	

$\boxed{x^2+x+1}$

(3) x^2+x

q	r_1	r_2	r	t_1	t_2	t
x	x^3+x^2+1	x^2+x+1	$x+1$	0	1	x
x	x^2+x+1	$x+1$	1	1	x	x^2+1
$x+1$	$x+1$	1	0	x	x^2+1	x^3+x^2+1
	1	0		x^2+1	x^3+x^2+1	

$\boxed{x^2+1}$

Ans = ~~8~~ 14 Elements of the field $GF(2^4)$

$F(x) = x^4 + x + 1$ $\quad\quad$ $N = 2^4 - 2 = 14$

$0 \longrightarrow 0000$

$g^0 \longrightarrow 0001$

$g^1 \longrightarrow 0010$

$g^2 \longrightarrow 0100$

$g^3 \longrightarrow 1000$

$g^4 \rightarrow (g+1) \quad 0011$

$g^5 \longrightarrow g(g+1) = g^2+g = 0110$

$g^6 \longrightarrow g(g^5) = g(g^2+g) = g^3+g^2 = 1100$

$g^7 \rightarrow g(g^6) = g(g^3+g^2) = g^4+g^3 = 1011 \quad (g^3+g+1)$

$g^8 \longrightarrow \cancel{g(g^7) = g(g^4+g^3) = g^5+g^4 = g^2+g+g^4}$

$g(g^7) = g(g^3+g+1) = g^4+g^2+g = g^2+1 = 0101$

$g^9 \longrightarrow g(g^8) = g(g^2+1) = g^3+g = 1010$

$g^{10} \longrightarrow g(g^9) = g(g^3+g) = g^2+g+1 = 0111$

$g^{11} \longrightarrow g(g^{10}) = g^3+g^2+g = 1110$

$g^{12} = g(g^{11}) = g^4+g^3+g^2 = g^3+g^2+g+1 = 1111$

$g^{13} = g(g^{12}) = g^4+g^3+g^2+g = g^3+g^2+1 = 1101$

$g^{14} = g(g^{13}) = g(g^3+g^2+1) = g^4+g^3+g = g^3+1 = 1001$

$g^{-3} = g^{12}$

$(-3 \bmod 15 = 12)$

$$\frac{g^3}{g^8} = g^3 \times g^7 = g^{10} = g^2 + g + 1 = 0111$$

$$g^{20} = g^{20 \bmod 15} = g^5 = g^2 + g = 0110$$

Q15

$x^2 \equiv a \pmod p$

$x^2 \equiv 36 \pmod{77}$

If we have factorization of n

$77 = 7 \times 11$

We can write

$x^2 \equiv 36 \pmod 7 \equiv 1 \pmod 7$ and

$x^2 \equiv 36 \pmod{11} \equiv 3 \pmod{11}$

We have choose 7 and 11 so that it is of form $4k+3$

$x \equiv \pm a^{(p+1)/4} \bmod p$

$\equiv \pm 1^2 \bmod 7 \equiv \pm 1 \bmod 7$

$x \equiv \pm 3^3 \bmod 11$

$\equiv \pm 5 \bmod 11$

Four sets of equations

Set 1: $x \equiv +1 \pmod 7$ $\quad x \equiv +5 \pmod{11}$

Set 2: $x \equiv +1 \pmod 7$ $\quad x \equiv -5 \pmod{11}$

Set 3: $x \equiv -1 \pmod 7$ $\quad x \equiv +5 \pmod{11}$

Set 4: $x \equiv -1 \pmod 7$ $\quad x \equiv -5 \pmod{11}$