

Date _____

BASIL ALI KHAN

20K-0477

Assignment # 03

QUESTION # 01

$$\begin{aligned}x &= 6 \pmod{11} \\x &= 13 \pmod{16} \\x &= 9 \pmod{21} \\x &= 19 \pmod{25}\end{aligned}$$

$$m_1 = 11$$

$$m_2 = 16$$

$$m_3 = 21$$

$$m_4 = 25$$

$$m = m_1 \times m_2 \times m_3 \times m_4$$

$$m = 11 \times 16 \times 21 \times 25$$

$$m = 92400$$

$$M_1 = \frac{92400}{11}$$

$$M_2 = \frac{92400}{16}$$

$$M_3 = \frac{92400}{21}$$

$$M_4 = \frac{92400}{25}$$

$$M_1 = 8400$$

$$M_2 = 5775$$

$$M_3 = 4400$$

$$M_4 = 3696$$

$$\begin{aligned}M_1 y_1 &= 1 \pmod{m_1} \\8400 y_1 &= 1 \pmod{11} \quad \text{--- (1)}\end{aligned}$$

$$8400 = 11 \cdot 763 + 7 \Rightarrow 7 = 8400 - 763(11)$$

$$11 = 7 \cdot 1 + 4 \Rightarrow 4 = 11 - 1(7)$$

$$7 = 4 \cdot 1 + 3 \Rightarrow 3 = 7 - 1(4)$$

$$4 = 3 \cdot 1 + 1 \Rightarrow 1 = 4 - 1(3)$$

$$3 = 1 \cdot 3 + 0$$

Signature _____

RC

No. _____

$$1 = 1(4) - 1(3)$$

$$1 = 1(4) - 1(7 - 1(4))$$

$$1 = 1(4) - 1(7) + 1(4)$$

$$1 = 2(4) - 1(7)$$

$$1 = -1(7) + 2(11 - 1(7))$$

$$1 = -1(7) + 2(11) - 2(7)$$

$$1 = -3(7) + 2(11)$$

$$1 = 2(11) - 3(18460) - 763(11)$$

$$1 = 2(11) - 3(8400) + 2289(11)$$

$$1 = 2291(11) - 3(8400)$$

$-3 \Rightarrow \text{inverse}$

$$M_2 y_2 = 1 \pmod{16}$$

$$5775 y_2 = 1 \pmod{16} \quad \text{--- (2)}$$

$$5775 = 16 \cdot 360 + 15 \Rightarrow 15 = 1(5775) - 360(16)$$

$$16 = 15 \cdot 1 + 1 \Rightarrow 1 = 1(16) - 1(15)$$

$$15 = 1 \cdot 15 + 0$$

$$1 = 1(16) - 1(15)$$

$$1 = 1(16) - 1(1(5775) - 360(16))$$

$$1 = 1(16) - 1(5775) + 360(16)$$

$$1 = 361(16) - 1(5775)$$

$-1 \Rightarrow \text{inverse}$

$$M_3 y_3 = 1 \pmod{21}$$

$$4400 y_3 = 1 \pmod{21} \quad \text{--- (3)}$$

$$4400 = 21 \cdot 209 + 11 \Rightarrow 11 = 4400 - 209(21)$$

$$21 = 11 \cdot 1 + 10 \Rightarrow 10 = 21 - 1(11)$$

$$11 = 10 \cdot 1 + 1 \Rightarrow 1 = 11 - 1(10)$$

$$10 = 1 \cdot 10 + 0$$

Date _____

$$1 = 1(11) - 1(10)$$

$$1 = 1(11) - 1(121) + 1(11)$$

$$1 = 1(11) - 1(21) + 1(11)$$

$$1 = 2(11) - 1(21)$$

$$1 = -1(21) + 2(1(4400) - 209(21))$$

$$1 = -1(21) + 2(4400) - 418(21)$$

$$1 = -419(21) + 2(4400)$$

2 \Rightarrow inverse.

$$114 y_4 = 1 \pmod{25}$$

$$3696 y_4 = 1 \pmod{25} \quad \text{--- } (4)$$

$$3696 = 25 \cdot 147 + 21 \Rightarrow 21 = 3696 - 147(25)$$

$$25 = 21 \cdot 1 + 4$$

$$4 = 25 - 1(21)$$

$$21 = 4 \cdot 5 + 1$$

$$1 = 21 - 5(4)$$

$$4 = 1 \cdot 4 + 0$$

$$1 = 1(21) - 5(4)$$

$$1 = 1(21) - 5(25 - 1(21))$$

$$1 = 1(21) - 5(25) + 5(21)$$

$$1 = 6(21) - 5(25)$$

$$1 = -5(25) + 6(3696 - 147(25))$$

$$1 = -5(25) + 6(3696) - 882(25)$$

$$1 = -887(25) + 6(3696)$$

6 \Rightarrow inverse.

Date _____

$$\begin{aligned} \textcircled{1} \Rightarrow 8400 y_1 &= 1 \pmod{11} \\ 8400(-3) &= 1(-3) \pmod{11} \\ y_1 &= 8 \end{aligned}$$

$$\begin{aligned} \textcircled{2} \Rightarrow 5775 y_2 &= 1 \pmod{16} \\ 5775(-1) &= 1(-1) \pmod{16} \\ y_2 &= -1 \pmod{16} \\ y_2 &= 15 \end{aligned}$$

$$\begin{aligned} \textcircled{3} \Rightarrow 4400 y_3 &= 1 \pmod{21} \\ 4400(2) &= 1(2) \pmod{21} \\ y_3 &= 2 \pmod{21} \\ y_3 &= 2 \end{aligned}$$

$$\begin{aligned} \textcircled{4} \Rightarrow 3696 y_4 &= 1 \pmod{25} \\ 3696(6) &= 1(6) \pmod{25} \\ y_4 &= 6 \pmod{25} \\ y_4 &= 6 \end{aligned}$$

$x \equiv 6 \pmod{11}$	$y_1 = 8$	$M_1 = 8400$
$x \equiv 13 \pmod{16}$	$y_2 = 15$	$M_2 = 5775$
$x \equiv 9 \pmod{21}$	$y_3 = 2$	$M_3 = 4400$
$x \equiv 19 \pmod{25}$	$y_4 = 6$	$M_4 = 3696$

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4 \\ x &= (6)(8)(8400) + (13)(15)(5775) + (9)(2)(4400) \\ &\quad + (19)(6)(3696) \end{aligned}$$

$$\begin{aligned} x &= 403200 + 1126125 + 79200 + 421344 \\ x &= 2029869 \end{aligned}$$

$$\begin{aligned} x &= 2029869 \pmod{72400} \\ x &= 89469 \pmod{72400} \end{aligned}$$

Signature _____

RC

No. _____

Date _____

QUESTION # 02:

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

$$x \equiv 10 \pmod{11}$$

$$m_1 = 5$$

$$m_2 = 7$$

$$m_3 = 11$$

$$m = m_1 \times m_2 \times m_3$$

$$m = 5 \times 7 \times 11$$

$$m = 385$$

$$M_1 = \frac{385}{5}$$

$$M_2 = \frac{385}{7}$$

$$M_3 = \frac{385}{11}$$

$$M_1 = 77$$

$$M_2 = 55$$

$$M_3 = 35$$

$$M_1 y_1 \equiv 1 \pmod{m_1}$$

$$77 y_1 \equiv 1 \pmod{5} \rightarrow \textcircled{1}$$

$$77 = 5 \cdot 15 + 2 \Rightarrow 2 = 77 - 15(5)$$

$$5 = 2 \cdot 2 + 1$$

$$1 = 5 - 2(2)$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 5 - 2(2)$$

$$1 = 1(5) - 2(1(77) - 15(5))$$

$$1 = 1(5) - 2(77) + 30(5)$$

$$1 = 31(5) - 2(77)$$

$$-2 \Rightarrow \text{inverse}$$

Signature _____

RC

No. _____

Date _____

$$\begin{aligned} M_2 y_2 &= 1 \pmod{7} \\ 55 y_2 &= 1 \pmod{7} \rightarrow \textcircled{2} \end{aligned}$$

$$\begin{aligned} 55 &= 7 \cdot 7 + 6 \Rightarrow 6 = 55 - 7(7) \\ 7 &= 6 \cdot 1 + 1 \quad 1 = 7 - 1(6) \\ 6 &= 1 \cdot 6 + 0 \end{aligned}$$

$$1 = 1(7) - 1(6)$$

$$1 = 1(7) - 1(55 - 7(7))$$

$$1 = 1(7) - 1(55) + 7(7)$$

$$1 = 8(7) - 1(55)$$

$-1 \Rightarrow$ inverse

$$\begin{aligned} M_3 y_3 &= 1 \pmod{11} \\ 35 y_3 &= 1 \pmod{11} \rightarrow \textcircled{3} \end{aligned}$$

$$\begin{aligned} 35 &= 11 \cdot 3 + 2 \Rightarrow 2 = 35 - 3(11) \\ 11 &= 2 \cdot 5 + 1 \quad 1 = 11 - 5(2) \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

$$1 = 1(11) - 5(2)$$

$$1 = 1(11) - 5(35 - 3(11))$$

$$1 = 1(11) - 5(35) + 15(11)$$

$$1 = 16(11) - 5(35)$$

$-5 \Rightarrow$ inverse

Signature _____

RC

No. _____

$$\textcircled{1} \Rightarrow 77 y_1 = 1 \pmod{5}$$

$$77(-2) = 1(-2) \pmod{5}$$

$$y_1 = -2 \pmod{5}$$

$$y_1 = 3$$

$$\textcircled{2} \Rightarrow 55 y_2 = 1 \pmod{7}$$

$$55(-1) = 1(-1) \pmod{7}$$

$$y_2 = -1 \pmod{7}$$

$$y_2 = 6$$

$$\textcircled{3} \Rightarrow 35 y_3 = 1 \pmod{11}$$

$$35(-5) = 1(-5) \pmod{11}$$

$$y_3 = -5 \pmod{11}$$

$$y_3 = 6$$

$x \equiv 2 \pmod{5}$	$y_1 = 3$	$M_1 = 77$
$x \equiv 3 \pmod{7}$	$y_2 = 6$	$M_2 = 55$
$x \equiv 10 \pmod{11}$	$y_3 = 6$	$M_3 = 35$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$

$$x = (2)(77)(3) + 3(55)(6) + (10)(35)(6)$$

$$x = 462 + 990 + 2100$$

$$x = 3552$$

$$x = 3552 \pmod{385}$$

$$x = \cancel{3552} \pmod{385}$$

$$87$$

QUESTION #03 :

i) $a = 4, m = 9$

$x = a \pmod{m}$

$x = 4 \pmod{9}$

$9 = 4 \cdot 2 + 1 \Rightarrow 1 = 1(9) - 2(4)$

$4 = 1 \cdot 4 + 0$

-2 & 1 are bezout coefficients of 4 & 9.

$-2(4) \pmod{9} = -8 \pmod{9} = 1$

ii) $a = 19, m = 141$

$x = 19 \pmod{141}$

$141 = 19 \cdot 7 + 8 \Rightarrow 8 = 1(141) - 7(19)$

$19 = 8 \cdot 2 + 3 \Rightarrow 3 = 1(19) - 2(8)$

$8 = 3 \cdot 2 + 2 \Rightarrow 2 = 1(8) - 2(3)$

$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 1(3) - 1(2)$

$2 = 1 \cdot 2 + 0$

$1 = 1(3) - 1(2)$

$1 = 1(3) - 1(1(8) - 2(3))$

$1 = 1(3) - 1(8) + 2(3)$

$1 = -1(8) + 3(1(19) - 2(8))$

$1 = -1(8) + 3(19) - 6(8)$

$1 = 3(19) - 7(8)$

$1 = 3(19) - 7(1(141) - 7(19))$

$1 = 3(19) - 7(141) + 49(19)$

$1 = 52(19) - 7(141)$

52 and -7 are bezout coefficients

$$52(19) \pmod{141} = 988 \pmod{141} \\ = 1$$

iii) $a = 55, m = 89$
 $x = 55 \pmod{89}$

$$89 = 55 \cdot 1 + 34 \Rightarrow 34 = 89 - 1(55)$$

$$55 = 34 \cdot 1 + 21 \Rightarrow 21 = 55 - 1(34)$$

$$34 = 21 \cdot 1 + 13 \Rightarrow 13 = 34 - 1(21)$$

$$21 = 13 \cdot 1 + 8 \Rightarrow 8 = 21 - 1(13)$$

$$13 = 8 \cdot 1 + 5 \Rightarrow 5 = 13 - 1(8)$$

$$8 = 5 \cdot 1 + 3 \Rightarrow 3 = 8 - 1(5)$$

$$5 = 3 \cdot 1 + 2 \Rightarrow 2 = 5 - 1(3)$$

$$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 3 - 1(2)$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 1(3) - 1(2)$$

$$1 = 1(3) - 1(1(5) - 1(3))$$

$$1 = 2(3) - 1(5)$$

$$1 = -1(5) + 2(1(8) - 1(5))$$

$$1 = -1(5) + 2(8) - 2(5)$$

$$1 = 2(8) - 3(5)$$

$$1 = 2(8) - 3(1(13) - 1(8))$$

$$1 = 2(8) - 3(13) + 3(8)$$

$$1 = -3(13) + 5(8)$$

$$1 = -3(13) + 5(1(21) - 1(13))$$

$$1 = -3(13) + 5(21) - 5(13)$$

$$1 = 5(21) - 8(13)$$

$$1 = 5(21) - 8(1(34) - 1(21))$$

$$1 = 5(21) - 8(34) + 8(21)$$

$$1 = -8(34) + 13(21)$$

$$1 = -8(34) + 13(1(55) - 1(34))$$

$$1 = -8(34) + 13(55) - 13(34)$$

$$1 = -21(34) + 13(55)$$

$$1 = 13(55) - 21(1(89) - 1(55))$$

$$1 = 13(55) - 21(89) + 21(55)$$

$$1 = 34(55) - 21(89)$$

34 and -21 are bezout coefficients of 55 and 89.

$$34(55) \pmod{89} = 1870 \pmod{89} = 1$$

$$iv) a = 89 \quad m = 232$$

$$x = 89 \pmod{232}$$

$$232 = 89 \cdot 2 + 54 \Rightarrow 54 = 232 - 2(89)$$

$$89 = 54 \cdot 1 + 35 \Rightarrow 35 = 89 - 1(54)$$

$$54 = 35 \cdot 1 + 19 \Rightarrow 19 = 54 - 1(35)$$

$$35 = 19 \cdot 1 + 16 \Rightarrow 16 = 35 - 1(19)$$

$$19 = 16 \cdot 1 + 3 \Rightarrow 3 = 19 - 1(16)$$

$$16 = 3 \cdot 5 + 1 \Rightarrow 1 = 16 - 5(3)$$

$$3 = 1 \cdot 3 + 0$$

$$1 = 16 - 5(3)$$

$$1 = 16 - 5(1(19) - 1(16))$$

$$1 = 16 - 5(19) + 5(16)$$

$$1 = 6(16) - 5(19)$$

$$1 = -5(19) + 6(35 - 1(19))$$

$$1 = -5(19) + 6(35) - 6(19)$$

$$1 = 6(35) - 11(19)$$

Date _____

$$1 = 6(35) - 11(54 - 1(35))$$

$$1 = 6(35) - 11(54) + 11(35)$$

$$1 = 17(35) - 11(54)$$

$$1 = -11(54) + 17(89 - 1(54))$$

$$1 = -11(54) + 17(89) - 17(54)$$

$$1 = 17(89) - 28(54)$$

$$1 = 17(89) - 28(232 - 2(89))$$

$$1 = 17(89) - 28(232) + 56(89)$$

$$1 = 73(89) - 28(232)$$

73 and 232 are bezout coefficient of 89
mod 232

$$73(89) \pmod{232} = 6497 \pmod{232} \\ = 1$$

QUESTION # 04:

$$i) 19x = 4 \pmod{141}$$

$$141 = 19 \cdot 7 + 8 \Rightarrow 8 = 1(141) - 7(19)$$

$$19 = 8 \cdot 2 + 3 \Rightarrow 3 = 1(19) - 2(8)$$

$$8 = 3 \cdot 2 + 2 \quad 2 = 1(8) - 2(3)$$

$$3 = 2 \cdot 1 + 1 \quad 1 = 1(3) - 1(2)$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 1(3) - 1(2)$$

$$1 = 1(3) - 1(1(8) - 2(3))$$

$$1 = 1(3) - 1(8) + 2(3)$$

$$1 = -1(8) + 3(3)$$

$$1 = -1(8) + 3(1(19) - 2(8))$$

$$1 = -1(8) + 3(19) - 6(8)$$

$$1 = 3(19) - 7(8)$$

Signature _____

RC

No. _____

$$1 = 3(19) - 7(1(141) - 7(19))$$

$$1 = 3(19) - 7(141) + 49(19)$$

$$1 = 52(19) - 7(141)$$

52 and -7 are bezant coefficient of 19
mod 141.

$$19(52)x = 4(52)(\text{mod } 141)$$

$$\text{let } x = (19)(52)x$$

$$x = 208 (\text{mod } 141)$$

$$x = 67$$

$$\text{ii) } 55x \equiv 34 (\text{mod } 89)$$

$$89 = 55 \cdot 1 + 34 \Rightarrow$$

$$55 = 34 \cdot 1 + 21$$

$$34 = 21 \cdot 1 + 13$$

$$21 = 13 \cdot 1 + 8$$

$$13 = 8 \cdot 1 + 5$$

$$8 = 5 \cdot 1 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

Already solved this in question # 03
part (iii)

$$1 = 34(55) - 21(89)$$

34 and -21 are bezant coefficient

$$55(34)x = 34(34)(\text{mod } 89)$$

$$x = 1156 (\text{mod } 89)$$

$$x = 88$$

$$\text{iii)} \quad 89x \equiv 2 \pmod{232}$$

$$232 = 89 \cdot 2 + 54$$

$$89 = 54 \cdot 1 + 35$$

$$54 = 35 \cdot 1 + 19$$

$$35 = 19 \cdot 1 + 16$$

$$19 = 16 \cdot 1 + 3$$

$$16 = 3 \cdot 5 + 1$$

$$3 = 1 \cdot 3 + 0$$

Already done in question 3 part iv).

$$1 = 73(89) - 28(232)$$

$$89(73)x = 2(73) \pmod{232}$$

$$x = 146 \pmod{232}$$

$$x = 146$$

$$\text{iv)} \quad 34x \equiv 77 \pmod{89}$$

$$89 = 34 \cdot 2 + 21 \Rightarrow 21 = 89 - 2(34)$$

$$34 = 21 \cdot 1 + 13 \Rightarrow 13 = 34 - 1(21)$$

$$21 = 13 \cdot 1 + 8 \Rightarrow 8 = 21 - 1(13)$$

$$13 = 8 \cdot 1 + 5 \Rightarrow 5 = 13 - 1(8)$$

$$8 = 5 \cdot 1 + 3 \Rightarrow 3 = 8 - 1(5)$$

$$5 = 3 \cdot 1 + 2 \Rightarrow 2 = 5 - 1(3)$$

$$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 3 - 1(2)$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 3 - 1(2)$$

$$1 = 3 - 1(5 - 1(3))$$

$$1 = 1(3) - 1(5) + 1(3)$$

Date _____

$$1 = -1(5) + 2(3)$$

$$1 = -1(5) + 2(1(8) - 1(5))$$

$$1 = -1(5) + 2(8) - 2(5)$$

$$1 = 2(8) - 3(5)$$

$$1 = 2(8) - 3(1(13) - 1(8))$$

$$1 = 2(8) - 3(13) + 3(8)$$

$$1 = -3(13) + 5(8)$$

$$1 = -3(13) + 5(1(21) - 1(8))$$

$$1 = -3(13) + 5(21) - 5(8)$$

$$1 = 5(21) - 8(13)$$

$$1 = 5(21) - 8(1(34) - 1(21))$$

$$1 = 5(21) - 8(34) + 8(21)$$

$$1 = -8(34) + 13(21)$$

$$1 = -8(34) + 13(1(89) - 2(34))$$

$$1 = -8(34) + 13(89) - 26(34)$$

$$1 = -34(34) + 13(89)$$

-34 and 13 are bezout coefficients.

$$34(-34) = 77(-34) \pmod{89}$$

$$x = -2618 \pmod{89}$$

$$x = 52$$

$$v. \quad 144x \equiv 4 \pmod{233}$$

$$233 = 144 \cdot 1 + 89 \Rightarrow 89 = 1(233) - 1(144)$$

$$89 = 144 \cdot 1 + 55 \Rightarrow 55 = 1(144) - 1(89)$$

$$89 = 55 \cdot 1 + 34 \Rightarrow 34 = 1(89) - 1(55)$$

$$55 = 34 \cdot 1 + 21 \Rightarrow 21 = 1(55) - 1(34)$$

$$34 = 21 \cdot 1 + 13 \Rightarrow 13 = 1(34) - 1(21)$$

$$21 = 13 \cdot 1 + 8 \Rightarrow 8 = 1(21) - 1(13)$$

$$13 = 8 \cdot 1 + 5 \Rightarrow 5 = 1(13) - 1(8)$$

$$8 = 5 \cdot 1 + 3 \Rightarrow 3 = 1(8) - 1(5)$$

$$5 = 3 \cdot 1 + 2 \Rightarrow 2 = 1(5) - 1(3)$$

$$3 \cdot 1 = 2 \cdot 1 + 1 \Rightarrow 1 = 1(3) - 1(2)$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 1(3) - 1(2)$$

$$1 = 1(3) - 1(1(5) - 1(3))$$

$$1 = 1(3) - 1(5) + 1(3)$$

$$1 = -1(5) + 2(3)$$

$$1 = -1(5) + 2(1(8) - 1(3))$$

$$1 = -1(5) + 2(8) - 2(3)$$

$$1 = 2(8) - 3(3)$$

$$1 = 2(8) - 3(1(13) - 1(8))$$

$$1 = 2(8) - 3(13) + 3(8)$$

$$1 = -3(13) + 5(8)$$

$$1 = -3(13) + 5(1(21) - 1(13))$$

$$1 = -3(13) + 5(21) - 5(13)$$

$$1 = 5(21) - 8(13)$$

$$1 = 5(21) - 8(1(34) - 1(21))$$

$$1 = 5(21) - 8(34) + 8(21)$$

$$1 = -8(34) + 13(21)$$

$$1 = -8(34) + 13(1(55) - 1(34))$$

$$1 = -8(34) + 13(55) - 13(34)$$

$$1 = 13(55) - 21(134)$$

$$1 = 13(55) - 21(1(89) - 1(55))$$

$$1 = 13(55) - 21(89) + 21(55)$$

$$1 = -21(89) + 34(55)$$

$$1 = -21(89) + 34(1(144) - 1(89))$$

$$1 = -21(89) + 34(144) - 34(89)$$

$$1 = 34(144) - 55(89)$$

$$1 = 34(144) - 55(1(233) - 1(144))$$

$$1 = 3(144) - 55(233) + 55(144)$$

$$1 = 58(144) - 55(233)$$

58 and -55 are bezout coefficients.

$$144(58) = 4(58) \pmod{233}$$

$$x = 232 \pmod{233}$$

$$x = 232$$

$$vi) 200x \equiv 3 \pmod{232}$$

$$232 = 200 \cdot 1 + 32$$

$$200 = 32 \cdot 6 + 8$$

$$32 = 8 \cdot 4 + 0$$

~~gcd~~ No inverse possible

DATE _____

DAY

M	T	W	T	F	S	S
---	---	---	---	---	---	---

QUESTION # 05

QUESTION # 07

$$h(K) = K \bmod 97$$

$$a) 1234566554.$$

$$24$$

$$b) 3574953579.$$

$$52.$$

$$c) 7346309359$$

$$3$$

$$d) 73483684348$$

$$47$$

QUESTION # 6.

$$a) 1234566554.$$

$$23$$

$$b) 3574953579.$$

$$100$$

$$c) 7346309359$$

$$23. \Rightarrow 23 + 1 \Rightarrow 24.$$

$$d) 7348364348$$

$$66.$$

$$h(K) = K \bmod 31$$

$$h(218) = 218 \bmod 31 = 1$$

$$h(220) = 220 \bmod 31 = 3$$

$$h(100) = 100 \bmod 31 = 7$$

$$h(007) = 007 \bmod 31 = 8$$

$$h(310) = 310 \bmod 31 = 0$$

$$h(111) = 111 \bmod 31 = 18$$

$$h(048) = 048 \bmod 31 = 17$$

DATE _____

DAY M T W T F S S

QUESTION #08

$$x_{n+1} = (3x_n + 2) \bmod 13 \quad x_0 = 1$$

$$x_{0+1} = (3(1) + 2) \bmod 13$$

$$x_1 = 5$$

$$x_{1+1} = (3(5) + 2) \bmod 13$$

$$x_2 = 4$$

$$x_{2+1} = (3(4) + 2) \bmod 13$$

$$x_3 = 1$$

$$x_{3+1} = (3(1) + 2) \bmod 13$$

$$x_4 = 5$$

$$x_{4+1} = (3(5) + 2) \bmod 13$$

$$x_5 = 4$$

QUESTION #09

$$x_{n+1} = (4x_n + 2) \bmod 13 \quad \text{Seed } x_0 = 3$$

$$x_{0+1} = (4(3) + 2) \bmod 13$$

$$x_1 = 1$$

$$x_{1+1} = (4(1) + 2) \bmod 13$$

$$x_2 = 6$$

$$x_{2+1} = (4(6) + 2) \bmod 13$$

$$x_3 = 0$$

$$x_{3+1} = (4(0) + 2) \bmod 13$$

$$x_4 = 2$$

$$x_{4+1} = (4(2) + 2) \bmod 13$$

$$x_5 = 10$$

$$x_{5+1} = (4(10) + 2) \bmod 13$$

$$x_6 = 3$$

$$x_{6+1} = (4(3) + 2) \bmod 13$$

$$x_7 = 1$$



QUESTION # 10.

007119881

$$1(0) + 2(0) + 3(7) + 4(1) + 5(1) + 6(9) + 7(8) + 8(8) + 9(1) =$$

$$21 + 4 + 5 + 54 + 36 + 64 + 9$$

$$231 \bmod 11 = 4$$

check digit $\Rightarrow 4$.

QUESTION # 11

Attached screenshot.

QUESTION # 12.

i. 1, 5

$$5 = 5 \cdot 1 + 0$$

$$\gcd \Rightarrow 0$$

v. 1111111, 1111111

$$1111111 = 111111 \cdot 1 + 1$$

$$\gcd \Rightarrow 1$$

ii) 123, 277

$$277 = 123 \cdot 2 + 31$$

$$123 = 31 \cdot 3 + 30$$

$$31 = 30 \cdot 1 + 1$$

$$\gcd \Rightarrow 1$$

iii) 100, 101

$$101 = 100 \cdot 1 + 1$$

$$\gcd \Rightarrow 1$$

$$188 = 35 \cdot 5 + 13$$

$$35 = 13 \cdot 2 + 9$$

$$13 = 9 \cdot 1 + 4$$

$$9 = 4 \cdot 2 + 1$$

iv) 1539, 14039

$$14039 = 1539 \cdot 9 + 188$$

$$1539 = 188 \cdot 8 + 35$$

$$\gcd \Rightarrow 1$$

DATE _____

DAY

M	T	W	T	F	S	S
---	---	---	---	---	---	---

QUESTION # 13.

vi) 1, 5

$$1 = 1^0 \quad 5 = 5^1 \times 1^0$$

$$\begin{aligned} \gcd(1, 5) &= 1^{\min(0,0)} \cdot 5^{\min(0,1)} \\ &= 1^0 \cdot 5^0 \\ &= 1 \end{aligned}$$

vii) 123, 277

$$123 = 3^1 \times 41^1$$

$$277 = 277^1$$

$$\begin{aligned} \gcd(123, 277) &= 3^{\min(1,0)} \cdot 41^{\min(1,0)} \cdot 277^{\min(0,1)} \\ &= 3^0 \cdot 4^0 \cdot 277^0 \\ &= 1 \end{aligned}$$

viii) 100, 101

$$100 = 2^2 \times 5^2$$

$$101 = 101^1$$

$$\begin{aligned} \gcd(100, 101) &= 2^{\min(2,0)} \cdot 5^{\min(2,0)} \cdot 101^{\min(0,1)} \\ &= 2^0 \cdot 5^0 \cdot 101^0 \\ &= 1 \end{aligned}$$

ix) 1539, 14039

$$1539 = 3^4 \times 19^1$$

$$14039 = 101^1 \cdot 139^1$$

$$\begin{aligned} \gcd(1539, 14039) &= 3^{\min(4,0)} \cdot 19^{\min(1,0)} \cdot 101^{\min(0,1)} \cdot 139^{\min(0,1)} \\ &= 3^0 \cdot 19^0 \cdot 101^0 \cdot 139^0 \\ &= 1 \end{aligned}$$

x) 1111111, 1111111

$$1111111 = 239^1 \times 4649^1$$

$$1111111 = 73^1 \times 101^1 \times 137^1$$

$$\begin{aligned} \gcd(1111111, 1111111) &= 239^{\min(1,0)} \cdot 4649^{\min(1,0)} \cdot 73^{\min(0,1)} \\ &\quad \cdot 101^{\min(0,1)} \cdot 137^{\min(0,1)} \\ &= 1 \end{aligned}$$

DATE _____

DAY

M	T	W	T	F	S	S
---	---	---	---	---	---	---

QUESTION #14

0	1	2	3	4	5	6	7	8	9	10	11
A	B	C	D	E	F	G	H	I	J	K	L
12	13	14	15	16	17	18	19	20	21	22	23
M	N	O	P	Q	R	S	T	U	V	W	X
24	25										
Y	Z										

Message	(i) $(p+2) \bmod 26$	(ii) $(p+13) \bmod 26$	(iii) $(p+7) \bmod 26$
I	$10 \Rightarrow K$	$21 \Rightarrow V$	$15 \Rightarrow P$
A	$2 \Rightarrow C$	$13 \Rightarrow N$	$7 \Rightarrow H$
M	$14 \Rightarrow O$	$25 \Rightarrow Z$	$19 \Rightarrow T$
L	$13 \Rightarrow N$	$24 \Rightarrow Y$	$18 \Rightarrow S$
E	$6 \Rightarrow G$	$17 \Rightarrow R$	$11 \Rightarrow L$
A	$2 \Rightarrow C$	$13 \Rightarrow N$	$7 \Rightarrow H$
R	$19 \Rightarrow T$	$4 \Rightarrow E$	$24 \Rightarrow Y$
N	$15 \Rightarrow P$	$0 \Rightarrow A$	$20 \Rightarrow U$
I	$10 \Rightarrow K$	$21 \Rightarrow V$	$15 \Rightarrow P$
N	$15 \Rightarrow P$	$0 \Rightarrow A$	$20 \Rightarrow U$
G	$8 \Rightarrow I$	$19 \Rightarrow T$	$18 \Rightarrow S$
D	$5 \Rightarrow F$	$16 \Rightarrow Q$	$10 \Rightarrow K$
I	$10 \Rightarrow K$	$21 \Rightarrow V$	$15 \Rightarrow P$
S	$20 \Rightarrow U$	$5 \Rightarrow F$	$25 \Rightarrow Z$
C	$4 \Rightarrow E$	$15 \Rightarrow P$	$9 \Rightarrow J$
R	$19 \Rightarrow T$	$4 \Rightarrow E$	$24 \Rightarrow Y$
E	$6 \Rightarrow G$	$17 \Rightarrow R$	$11 \Rightarrow L$
T	$21 \Rightarrow V$	$6 \Rightarrow G$	$6 \Rightarrow A$
E	$6 \Rightarrow G$	$17 \Rightarrow R$	$11 \Rightarrow L$
S	$20 \Rightarrow U$	$5 \Rightarrow F$	$25 \Rightarrow Z$
T	$21 \Rightarrow V$	$6 \Rightarrow G$	$0 \Rightarrow A$

DATE

DAY M T W T F S S

R	19 \Rightarrow T	4 \Rightarrow E	24 \Rightarrow G
U	22 \Rightarrow W	7 \Rightarrow H	1 \Rightarrow B
C	4 \Rightarrow E	15 \Rightarrow P	9 \Rightarrow J
T	21 \Rightarrow V	6 \Rightarrow G	0 \Rightarrow A
U	22 \Rightarrow W	7 \Rightarrow H	1 \Rightarrow B
R	19 \Rightarrow T	4 \Rightarrow E	24 \Rightarrow G
E	6 \Rightarrow G	17 \Rightarrow R	11 \Rightarrow L

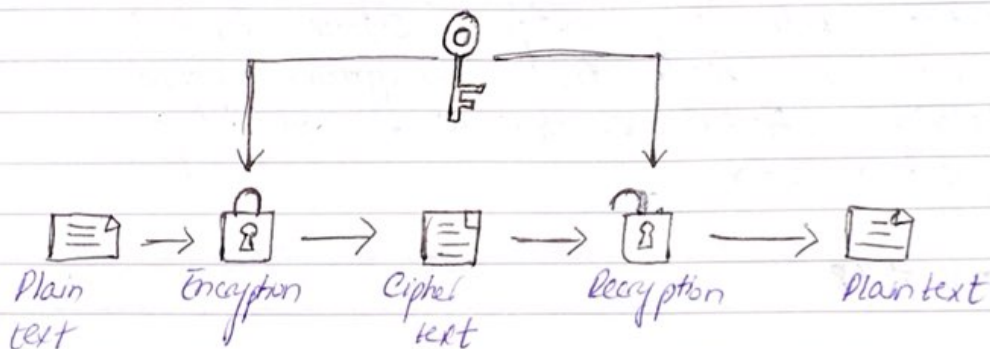
QUESTION # 15

Message	(N) $(2p+2) \bmod 26$	(V) $(2p+13) \bmod 26$	(V') $(2p+7) \bmod 26$
M	10 \Rightarrow A	11 \Rightarrow L	5 \Rightarrow F
Y	22 \Rightarrow W	9 \Rightarrow J	3 \Rightarrow D
N	2 \Rightarrow C	13 \Rightarrow N	7 \Rightarrow H
A	2 \Rightarrow C	13 \Rightarrow N	7 \Rightarrow H
m	1 \Rightarrow A	11 \Rightarrow L	5 \Rightarrow F
E	10 \Rightarrow K	21 \Rightarrow E	15 \Rightarrow P
I	18 \Rightarrow S	3 \Rightarrow D	23 \Rightarrow X
S	12 \Rightarrow M	23 \Rightarrow X	17 \Rightarrow R
K	22 \Rightarrow W	7 \Rightarrow H	1 \Rightarrow B
H	16 \Rightarrow Q	1 \Rightarrow B	21 \Rightarrow V
A	2 \Rightarrow C	13 \Rightarrow N	7 \Rightarrow H
N	2 \Rightarrow C	13 \Rightarrow N	7 \Rightarrow H

QUESTION # 16.

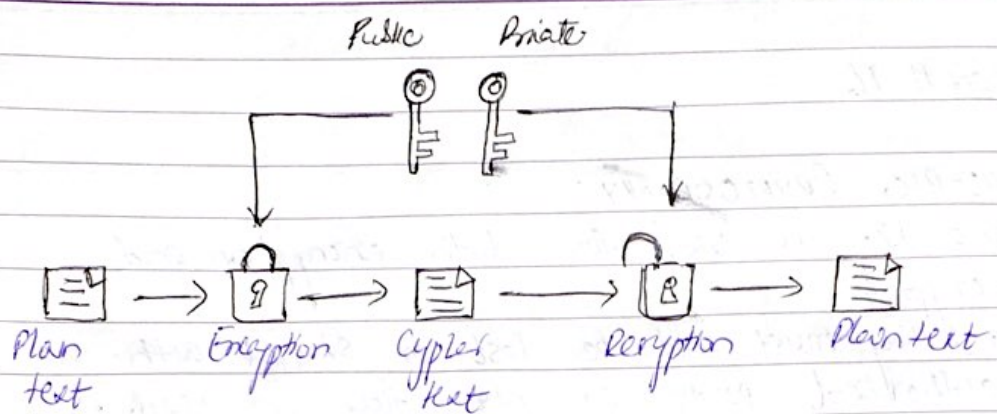
SYMMETRIC CRYPTOGRAPHY:

1. same key is used for both encryption and decryption.
2. Secret key must not be lost or shared with unauthorized parties or else they can read message.
3. Its faster and functions without lot of overheads on network or CPU resources.



ASYMMETRIC CRYPTOGRAPHY:

1. Asymmetric uses pair of related keys - a public and a private key.
2. Public key is accessible to everyone and used to encrypt a plain text message before sending.
3. Private key is needed to decrypt the message.
4. Time required is greater.
5. It offers high level security.



QUESTION # 17

Chinese Remainder Theorem is widely used with computing with large integers. Chinese Remainder theorem is used for encryption sequence numbering, Fast Fourier transform and Range ambiguity resolution.

QUESTION # 18

GRAPHS:

- In computer science, graphs are used to represent computer networks, data organization and the flow of computation.
- Link between websites is shown using undirected graph.
- It is also used to study molecules in chemistry and physics.
- It is used in geometry.

MATRICES:

- Matrices are used in science to show reflection and for refraction
- Matrices are used in electrical circuits and quantum mechanics and conversion of electrical energy.
- Matrices are also used to solve network equations
- Matrices are used 3D visualisation of objects in gaming.

NUMBER THEORY:

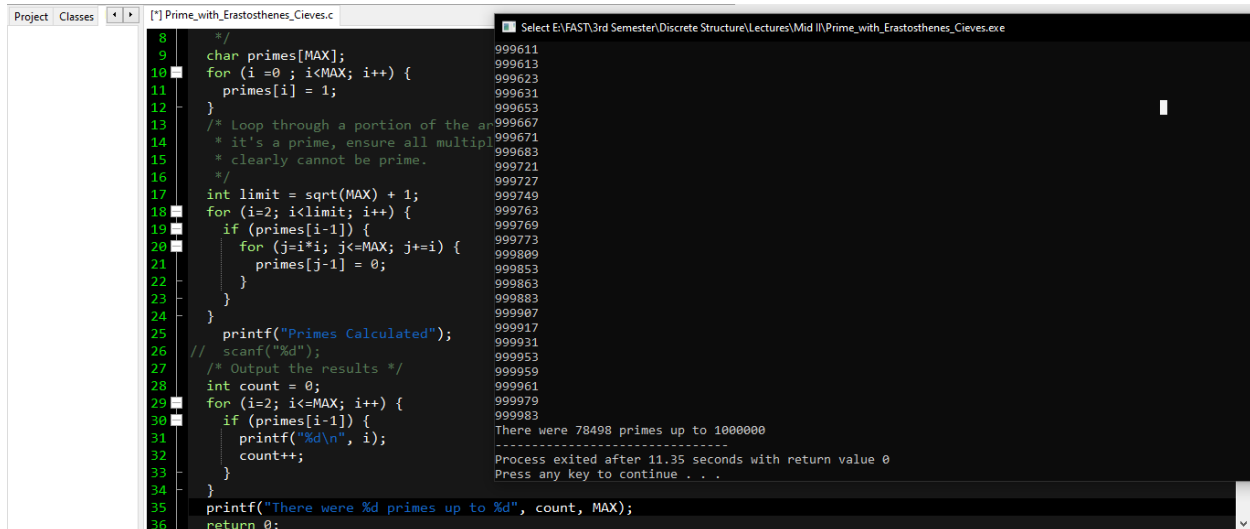
- Results generated from Number theory have countless application in mathematics as well as practical applications including security, memory management, authentication, coding theory etc.

CRYPTOGRAPHY:

Cryptography is at the intersection of discipline of mathematics, computer science, electrical engineering, communication and physics. Application of cryptography include electronic commerce, payment cards, digital currency, computer passwords and military communication.

Question#11:

- Prime with Eratosthenes



```
Project Classes [1] Prime_with_Eratosthenes_Cieves.c
8  /*
9  char primes[MAX];
10 for (i =0 ; i<MAX; i++) {
11     primes[i] = 1;
12 }
13 /* Loop through a portion of the array
14 * it's a prime, ensure all multiples
15 * clearly cannot be prime.
16 */
17 int limit = sqrt(MAX) + 1;
18 for (i=2; i<limit; i++) {
19     if (primes[i-1]) {
20         for (j=i*i; j<=MAX; j+=i) {
21             primes[j-1] = 0;
22         }
23     }
24 }
25 printf("Primes Calculated");
26 // scanf("%d");
27 /* Output the results */
28 int count = 0;
29 for (i=2; i<=MAX; i++) {
30     if (primes[i-1]) {
31         printf("%d\n", i);
32         count++;
33     }
34 }
35 printf("There were %d primes up to %d", count, MAX);
36 return 0;
```

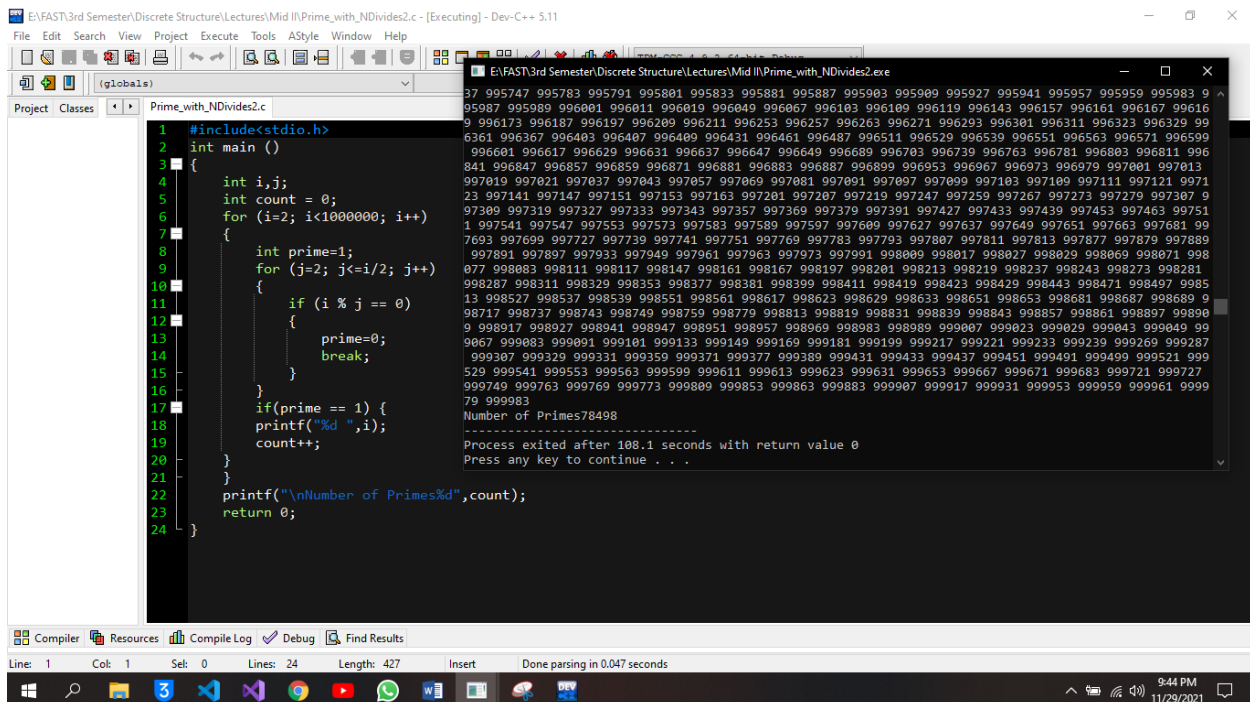
Select E:\FAST\3rd Semester\Discrete Structure\Lectures\Mid I\Prime_with_Eratosthenes_Cieves.exe

999611
999613
999623
999631
999653
999667
999671
999683
999721
999727
999749
999763
999769
999773
999809
999853
999863
999883
999907
999917
999931
999953
999959
999961
999979
999983
There were 78498 primes up to 1000000

Process exited after 11.35 seconds with return value 0
Press any key to continue . . .

Time Complexity: $O(N \log(\log N))$

- Prime with N divides 2



```
E:\FAST\3rd Semester\Discrete Structure\Lectures\Mid I\Prime_with_NDivides2.c - [Executing] - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
(globals)
Project Classes Prime_with_NDivides2.c
1  #include<stdio.h>
2  int main ()
3  {
4      int i,j;
5      int count = 0;
6      for (i=2; i<10000000; i++)
7      {
8          int prime=1;
9          for (j=2; j<=i/2; j++)
10             {
11                 if (i % j == 0)
12                 {
13                     prime=0;
14                     break;
15                 }
16             }
17             if(prime == 1) {
18                 printf("%d ",i);
19                 count++;
20             }
21         }
22         printf("\nNumber of Primes%d",count);
23         return 0;
24     }
```

E:\FAST\3rd Semester\Discrete Structure\Lectures\Mid I\Prime_with_NDivides2.exe

9995747 9995783 9995791 9995801 9995833 9995881 9995887 9995903 9995909 9995927 9995941 9995957 9995959 9995983 9
9995987 9995989 9996001 9996011 9996019 9996049 9996067 9996103 9996109 9996119 9996143 9996157 9996161 9996167 999616
9996173 9996187 9996197 9996209 9996211 9996253 9996257 9996263 9996271 9996293 9996301 9996311 9996323 9996329 99
9996367 9996403 9996407 9996409 9996431 9996461 9996487 9996511 9996529 9996539 9996551 9996563 9996571 9996599
9996601 9996617 9996629 9996631 9996637 9996647 9996649 9996689 9996703 9996739 9996763 9996781 9996803 9996811 996
841 9996847 9996857 9996859 9996871 9996881 9996883 9996887 9996899 9996953 9996967 9996973 9996979 9997001 9997013
9997019 9997021 9997037 9997043 9997057 9997069 9997081 9997091 9997097 9997099 9997103 9997109 9997111 9997121 99971
23 9997141 9997147 9997151 9997153 9997163 9997201 9997207 9997219 9997247 9997259 9997267 9997273 9997279 9997307 9
997309 9997319 9997327 9997333 9997343 9997357 9997369 9997379 9997391 9997427 9997433 9997439 9997453 9997463 999751
1 9997547 9997549 9997553 9997573 9997583 9997589 9997597 9997609 9997627 9997637 9997649 9997651 9997663 9997681 99
7693 9997699 9997727 9997739 9997741 9997751 9997769 9997783 9997793 9997807 9997811 9997813 9997877 9997879 9997889
9997891 9997897 9997933 9997949 9997961 9997963 9997973 9997991 9998009 9998017 9998027 9998029 9998069 9998071 998
077 9998083 9998111 9998117 9998147 9998161 9998167 9998197 9998201 9998213 9998219 9998237 9998243 9998273 9998281
9998287 9998311 9998329 9998353 9998377 9998381 9998399 9998411 9998419 9998423 9998429 9998443 9998471 9998497 99985
13 9998527 9998537 9998539 9998551 9998561 9998617 9998623 9998629 9998633 9998651 9998653 9998681 9998687 9998689 9
998717 9998737 9998743 9998749 9998759 9998779 9998813 9998819 9998831 9998839 9998843 9998857 9998861 9998897 999890
9 9998917 9998927 9998941 9998947 9998951 9998957 9998969 9998983 9998989 9999007 9999023 9999029 9999043 9999049 99
9067 9999083 9999091 9999101 9999133 9999149 9999169 9999181 9999199 9999217 9999221 9999233 9999239 9999269 9999287
9999307 9999329 9999331 9999359 9999371 9999377 9999389 9999431 9999433 9999437 9999451 9999491 9999499 9999521 999
529 9999541 9999553 9999563 9999599 9999611 9999613 9999623 9999631 9999653 9999667 9999671 9999683 9999721 9999727
9999749 9999763 9999769 9999773 9999809 9999853 9999863 9999883 9999907 9999917 9999931 9999953 9999959 9999961 9999
79 999983
Number of Primes78498

Process exited after 108.1 seconds with return value 0
Press any key to continue . . .

Time Complexity: $O(\log(N))$

- **Prime with sort of sqrt limit**

```
1 #include<stdio.h>
2 int main ()
3 {
4     int i,j, prime;
5     int count = 0;
6     for (i=2; i<10000000; i++)
7     {
8         prime=1;
9
10        for (j=2; j*j<=i; j++)
11        {
12            if (i % j == 0)
13            {
14                prime=0;
15                break;
16            }
17        }
18        if(prime == 1) {
19            printf("%d \n",i);
20            count++;
21        }
22    }
23    printf("\nNumber of Primes%d",count);
24    return 0;
25 }
```

999721
999727
999749
999763
999769
999773
999809
999853
999863
999883
999907
999917
999931
999953
999959
999961
999979
999983
Number of Primes78498
.....
Process exited after 8.166 seconds with return value 0
Press any key to continue . . .

Line: 1 Col: 1 Sel: 0 Lines: 25 Length: 442 Insert Done parsing in 0.062 seconds

Time Complexity: $O(\sqrt{N})$

BEST:

The best algorithm to find prime number is Eratosthenes because of its best time complexity.