Date

BASIL ALI KHAN
20K-0477

ASSIGNMENT # 03

QUESTION # 01

$x = 6 \pmod{11}$
$x = 13 \pmod{16}$
$x = 9 \pmod{21}$
$x = 19 \pmod{25}$

$m_1 = 11$
$m_2 = 16$
$m_3 = 21$
$m_4 = 25$

$m = m_1 \times m_2 * m_3 \times m_4$
$m = 11 \times 16 * 21 \times 25$
$m = 92400$

$M_1 = \frac{92400}{11}$ $M_2 = \frac{92400}{16}$ $M_3 = \frac{92400}{21}$ $M_4 = \frac{92400}{25}$

$M_1 = 8400$ $M_2 = 5775$ $M_3 = 4400$ $M_4 = 3696$

$M_1 y_1 = 1 \pmod{m_1}$
$8400 y_1 = 1 \pmod{11}$ — ①

$8400 = 11 \cdot 763 + 7 \Rightarrow 7 = 8400 - 763(11)$
$11 = 7 \cdot 1 + 4 \Rightarrow 4 = 11 - 1(7)$
$7 = 4 \cdot 1 + 3 \Rightarrow 3 = 7 - 1(4)$
$4 = 3 \cdot 1 + 1 \Rightarrow 1 = 4 - 1(3)$
$3 = 1 \cdot 3 + 0$

Signature No.

Date

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

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

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

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

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

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

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

$1 = 2(11) - 3(8400) - 763(11)$.

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

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

$-3 \Rightarrow$ inverse

$M_2 y_2 = 1 \pmod{16}$

$5775 y_2 = 1 \pmod{16}$ — (2)

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

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

$15 = 1 \cdot 15 + 0$

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

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

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

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

$-1 \Rightarrow$ inverse

$M_3 y_3 = 1 \pmod{21}$

$4400 y_3 = 1 \pmod{21}$ — (3)

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

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

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

$10 = 1 \cdot 10 + 0$

Signature

No.

Date

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

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

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

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

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

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

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

$2 \Rightarrow$ inverse.

$M_4 y_4 = 1 \pmod{25}$

$3696\, y_4 = 1 \pmod{25}$ — (4)

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

$25 = 21 \cdot 1 + 4$. $\quad 4 = 25 - 1(21)$

$21 = 4 \cdot 5 + 1 \quad 1 = 21 - 5(4)$.

$4 = 1 \cdot 4 + 0$

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

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

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

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

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

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

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

$6 \Rightarrow$ inverse.

Signature

No.

Date

① ⇒ $8400\, y_1 = 1 \pmod{11}$

$8400\,(-3) = 1(-3) \bmod 11$

$y_1 = 8$

② ⇒ $5775\, y_2 = 1 \pmod{16}$

$5775\,(-1) = 1(-1) \bmod 16$

$y_2 = -1 \bmod 16$

$y_2 = 15$

③ ⇒ $4400\, y_3 = 1 \pmod{21}$

$4400\,(2) = 1(2) \bmod 21$

$y_3 = 2 \bmod 21$

$y_3 = 2$

④ ⇒ $3696\, y_4 = 1 \pmod{25}$

$3696\,(6) = 1(6) \bmod 25$

$y_4 = 6 \bmod 25$

$y_4 = 6$

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

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4$

$x = (6)(8)(8400) + (13)(15)(5775) + (9)(2)(4400) + (19)(6)(3696)$

$x = 403200 + 1126125 + 79200 + 421344$

$x = 2029869$

$x = 2029869 \pmod{92400}$

$x = 89469 \pmod{92400}$

Signature

No.

Date

QUESTION # 02:

$x \equiv 2 \pmod 5$
$x \equiv 3 \pmod 7$
$x \equiv 10 \pmod{11}$

$m_1 = 5$
$m_2 = 7$
$m_3 = 11$
$m = m_1 \times m_2 + m_3$
$m = 5 \times 7 \times 11$
$m = 385$

$M_1 = \frac{385}{5}$ $\quad M_2 = \frac{385}{7}$ $\quad M_3 = \frac{385}{11}$

$M_1 = 77$ $\quad M_2 = 55$ $\quad M_3 = 35$

$M_1 y_1 = 1 \pmod{m_1}$
$77 y_1 = 1 \pmod 5 \rightarrow (1)$

$77 = 5 \cdot 15 + 2 \Rightarrow 2 = 77 - 15(5)$
$5 = 2 \cdot 2 + 1 \qquad 1 = 5 - 2(2)$
$2 = 1 \cdot 2 + 0$

$1 = 5 - 2(2)$
$1 = 1(5) - 2(1(77) - 15(5))$
$1 = 1(5) - 2(77) + 30(5)$
$1 = 31(5) - 2(77)$

$-2 \Rightarrow$ inverse

Signature

No.

Date

$M_2 y_2 = 1 \pmod 7$.
$55 y_2 = 1 \pmod 7 \rightarrow (2)$

$55 = 7 \cdot 7 + 6 \Rightarrow 6 = 55 - 7(7)$
$7 = 6 \cdot 1 + 1 \qquad 1 = 7 - 1(6)$.
$6 = 1 \cdot 6 + 0$.

$1 = 1(7) - 1(6)$
$1 = 1(7) - 1(55) - 7(7)$
$1 = 1(7) - 1(55) + 7(7)$.
$1 = 8(7) - 1(55)$

$-1 \Rightarrow$ inverse

$M_3 y_3 = 1 \pmod{11}$
$35 y_3 = 1 \pmod{11} \rightarrow (3)$

$35 = 11 \cdot 3 + 2 \Rightarrow 2 = 35 - 3(11)$
$11 = 2 \cdot 5 + 1 \qquad 1 = 11 - 5(2)$.
$2 = 1 \cdot 2 + 0$

$1 = 1(11) - 5(2)$
$1 = 1(11) - 5(1(35) - 3(11))$.
$1 = 1(11) - 5(35) + 15(11)$
$1 = 16(11) - 5(35)$

$-5 \Rightarrow$ inverse

Signature

No.

Date

① ⇒ $77 y_1 = 1 \pmod 5$.

$77(-2) = 1(-2) \bmod 5$

$y_1 = -2 \bmod 5$

$y_1 = 3$.

② ⇒ $55 y_2 = 1 \pmod 7$

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

$y_2 = -1 \bmod 7$

$y_2 = 6$.

③ ⇒ $35 y_3 = 1 \pmod{11}$

$35(-5) = 1(-5) \bmod 11$

$y_3 = -5 \bmod 11$

$y_3 = 6$.

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

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

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

$x = 462 + 990 + 2100$.

$x = 3552$.

$x = 3552 \pmod{385}$

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

87.

Signature

No.

Date

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 the bezout coefficient

Signature

No.

Date

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

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

$89 = 55 \cdot 1 + 34$ $\Rightarrow 34 = 89 - 1(55)$
$55 = 34 \cdot 1 + 21$ $\Rightarrow 21 = 55 - 1(34)$
$34 = 21 \cdot 1 + 13$ $\Rightarrow 13 = 34 - 1(21)$
$21 = 13 \cdot 1 + 8$ $\Rightarrow 8 = 21 - 1(13)$.
$13 = 8 \cdot 1 + 5$ $\Rightarrow 5 = 13 - 1(8)$.
$8 = 5 \cdot 1 + 3$ $\Rightarrow 3 = 8 - 1(5)$
$5 = 3 \cdot 1 + 2$ $\Rightarrow 2 = 5 - 1(3)$
$3 = 2 \cdot 1 + 1$ $\Rightarrow 1 = 3 - 1(2)$.
$2 = 1 \cdot 2 + 0$

$1 = 1(3) - 1(2)$
$1 = 1(3) - 1(1(5) - 1(3))$
$1 = 2(3) - 1(5)$.
$1 = -1(5) + 2(1(8) - 1(5))$
$1 = -1(5) + 2(8) - 2(5)$
$1 = 2(8) - 3(5)$
$1 = 2(8) - 3(1(13) - 1(8))$
$1 = 2(8) - 3(13) + 3(8)$
$1 = -3(13) + 5(8)$
$1 = -3(13) + 5(1(21) - 1(13))$
$1 = -3(13) + 5(21) - 5(13)$.
$1 = 5(21) - 8(13)$.

Signature No.

Date

$1 = 5(21) - 8(1(34) - 1(21))$
$1 = 5(21) - 8(34) + 8(21)$
$1 = -8(34) + 13(21)$
$1 = -8(34) + 13(1(55) - 1(34))$
$1 = -8(34) + 13(55) - 13(34)$
$1 = -21(34) + 13(55)$
$1 = 13(55) - 21(1(89) - 1(55))$
$1 = 13(55) - 21(89) + 21(55)$
$1 = 34(55) - 21(89)$

34 and -21 are bezout coefficients of 55 and 89

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

iv) $a = 89 \quad m = 232$
$x = 89 \pmod{232}$

$232 = 89 \cdot 2 + 54 \Rightarrow 54 = 232 - 2(89)$
$89 = 54 \cdot 1 + 35 \Rightarrow 35 = 89 - 1(54)$
$54 = 35 \cdot 1 + 19 \Rightarrow 19 = 54 - 1(35)$
$35 = 19 \cdot 1 + 16 \Rightarrow 16 = 35 - 1(19)$
$19 = 16 \cdot 1 + 3 \Rightarrow 3 = 19 - 1(16)$
$16 = 3 \cdot 5 + 1 \Rightarrow 1 = 16 - 5(3)$
$3 = 1 \cdot 3 + 0$

$1 = 16 - 5(3)$
$1 = 16 - 5(1(19) - 1(16))$
$1 = 16 - 5(19) + 5(16)$
$1 = 6(16) - 5(19)$
$1 = -5(19) + 6(35 - 1(19))$
$1 = -5(19) + 6(35) - 6(19)$
$1 = 6(35) - 11(19)$

Signature

No.

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 coeffient of 89 and 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 No.

Date

$1 = 3(19) - 7(1(141) - 7(19))$
$1 = 3(19) - 7(141) + 49(19)$.
$1 = 52(19) - 7(141)$

52 and -7 are bezout coefficient of 19 and 141.

$19(52)x \equiv 4(52) \pmod{141}$
let $x = (19)(52)x$
$x \equiv 208 \pmod{141}$
$x = 67$.

ii) $55x \equiv 34 \pmod{89}$

$89 = 55 \cdot 1 + 34 \Rightarrow$
$55 = 34 \cdot 1 + 21$
$34 = 21 \cdot 1 + 13$
$21 = 13 \cdot 1 + 8$
$13 = 8 \cdot 1 + 5$
$8 = 5 \cdot 1 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$

Already solved this in question # 03 part (iii)

$1 = 34(55) - 21(89)$
34 and -21 are bezout coefficient

$55(34)x \equiv 34(34) \pmod{89}$
$x \equiv 1156 \pmod{89}$
$x = 88$

Signature

No.

Date

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

$232 = 89 \cdot 2 + 54$
$89 = 54 \cdot 1 + 35$
$54 = 35 \cdot 1 + 19$
$35 = 19 \cdot 1 + 16$
$19 = 16 \cdot 1 + 3$
$16 = 3 \cdot 5 + 1$
$3 = 1 \cdot 3 + 0$

Already done in question 3 part iv).

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

$89(73)x = 2(73) \pmod{232}$.
$x = 146 \pmod{232}$
$x = 146$.

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

$89 = 34 \cdot 2 + 21 \Rightarrow 21 = 89 - 2(34)$
$34 = 21 \cdot 1 + 13 \Rightarrow 13 = 34 - 1(21)$
$21 = 13 \cdot 1 + 8 \Rightarrow 8 = 21 - 1(13)$
$13 = 8 \cdot 1 + 5 \Rightarrow 5 = 13 - 1(8)$
$8 = 5 \cdot 1 + 3 \Rightarrow 3 = 8 - 1(5)$
$5 = 3 \cdot 1 + 2 \Rightarrow 2 = 5 - 1(3)$
$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 3 - 1(2)$
$2 = 1 \cdot 2 + 0$

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

Signature No.

Date

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

-34 and 13 are bezout coefficients.

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

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

$x = 52$

Signature

No.

Date

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

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

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

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

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

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

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

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

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

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

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

$2 = 1 \cdot 2 + 0$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Signature

No.

Date

$1 = 13(55) - 21(34)$.
$1 = 13(55) - 21(1(89) - 1(55))$
$1 = 13(55) - 21(89) + 21(55)$.
$1 = -21(89) + 34(55)$.
$1 = -21(89) + 34(1(144) - 1(89))$
$1 = -21(89) + 34(144) - 34(89)$.
$1 = 34(144) - 55(89)$.
$1 = 34(144) - 55(1(233) - 1(144))$
$1 = 3(144) - 55(233) + 55(144)$.
$1 = 58(144) - 55(233)$.

58 and -55 are bezout coefficients.

$144(58) = 4(58) \pmod{233}$
$x = 232 \pmod{233}$.
$x = 232$.

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

$232 = 200 \cdot 1 + 32$
$200 = 32 \cdot 6 + 8$
$32 = 8 \cdot 4 + 0$

No inverse possible

Signature

No.

DATE DAY M T W T F S S

QUESTION # 05

$h(K) = K \bmod 97$

a) 1234566554.
24

b) 3574953579.
52.

c) 7346309359
3

d) 7348364348
47

QUESTION # 6.

a) 1234566554.
23

b) 3574953579.
100

c) 7346309359
23. => 23 + 1 => 24.

d) 7348364348
66.

QUESTION # 07

$h(K) = K \bmod 31$

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

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

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

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

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

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

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

DATE

DAY M T W T F S S

QUESTION #08

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

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

$x_1 = 5$

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

$x_2 = 4$

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

$x_3 = 1$

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

$x_4 = 5$

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

$x_5 = 4$

QUESTION #09

$x_{n+1} = (4x_n + 2) \bmod 13 \qquad$ seed $x_0 = 3.$

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

$x_1 = 1.$

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

$x_2 = 6.$

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

$x_3 = 0.$

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

$x_4 = 2$

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

$x_5 = 10$

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

$x_6 = 3.$

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

$x_7 = 1.$

DATE

DAY M T W T F S S

QUESTION # 10.

0071198 8 1

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

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

$231 \bmod 11 = 4$

check digit $\Rightarrow$ 4.

QUESTION # 11

Attached screenshot.

QUESTION # 12.

i. 1, 5

$5 = 5 \cdot 1 + 0$

gcd $\Rightarrow$ 0

v. 1111111, 11111111

$11111111 = 1111111 \cdot 1 + 1$

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

iv) 1539, 14039

$14039 = 1539 \cdot 9 + 188$

$1539 = 188 \cdot 8 + 35$

$188 = 35 \cdot 5 + 13$

$35 = 13 \cdot 2 + 9$

$13 = 9 \cdot 1 + 4$

$9 = 4 \cdot 2 + 1$

gcd $\Rightarrow$ 1

Page No.

DATE DAY M T W T F S S

QUESTION # 13.

vi) 1, 5

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

$\gcd(1,5) = 1^{\min(0,0)} \cdot 5^{\min(0,1)}$.

$= 1^0 \cdot 5^0$

$= 1$

vii) 123, 277

$123 = 3^1 \times 41^1$ $277 = 277^1$

$\gcd(123, 277) = 3^{\min(1,0)} \cdot 41^{\min(1,0)} \cdot 277^{\min(0,1)}$

$= 3^0 \cdot 4^0 \cdot 277^0$.

$= 1$

viii) 100, 101

$100 = 2^2 \times 5^2$ $101 = 101^1$

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

$= 2^0 \cdot 5^0 \cdot 101^0$

$= 1$

ix) 1539, 14039.

$1539 = 3^4 \times 19^1$ $14039 = 101^1 \cdot 139^1$

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

$= 3^0 \cdot 19^0 \cdot 101^0 \cdot 139^0$

$= 1$

x) 1111111, 11111111

$1111111 = 239^1 \times 4649^1$ $11111111 = 73^1 \times 101^1 \times 137^1$

$\gcd(1111111, 11111111) = 239^{\min(0,0)} \cdot 4649^{\min(1,0)} \cdot 73^{\min(0,1)} \cdot 101^{\min(0,1)} \cdot 137^{\min(0,1)}$

$= 1$

Page No.

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

Page No.

DATE DAY M T W T F S S

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

QUESTION # 15

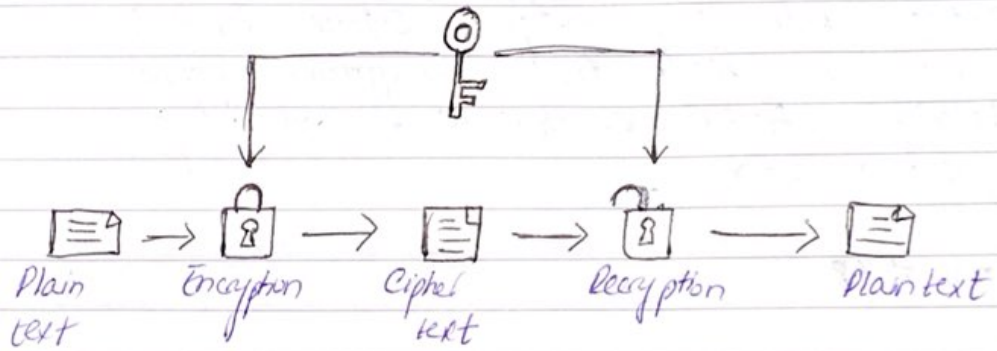
Message	(iv) $(2p+2) \bmod 26$	(v) $(2p+13) \bmod 26$	(vi) $(2p+7) \bmod 26$
M	1 ⇒ A	11 ⇒ L	5 ⇒ F
Y	22 ⇒ W	9 ⇒ J	3 ⇒ D
N	2 ⇒ C	13 ⇒ N	7 ⇒ H
A	2 ⇒ C	13 ⇒ N	7 ⇒ H
M	1 ⇒ A	11 ⇒ L	5 ⇒ F
E	10 ⇒ K	21 ⇒ E	15 ⇒ P
I	18 ⇒ S	3 ⇒ D	23 ⇒ X
S	12 ⇒ M	23 ⇒ X	17 ⇒ R
K	22 ⇒ W	7 ⇒ H	1 ⇒ B
H	16 ⇒ Q	1 ⇒ B	21 ⇒ V
A	2 ⇒ C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

DATE DAY M T W T F S S

QUESTION # 16.

SYMMETRIC CRYPTOGRAPHY:

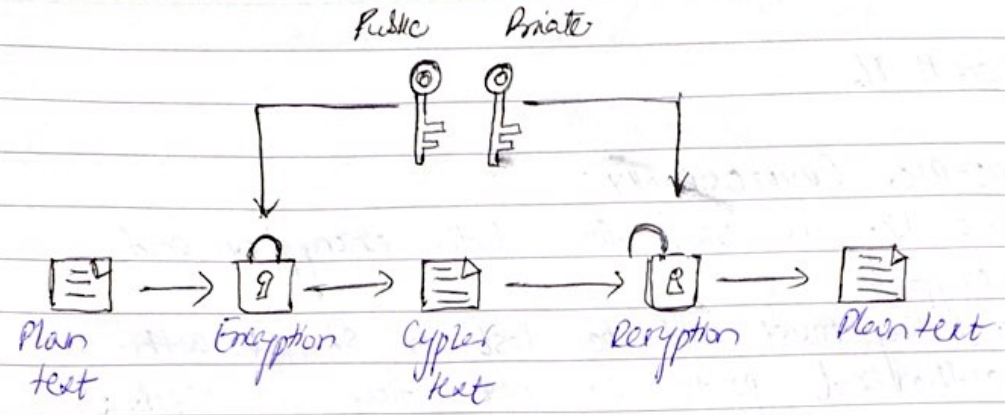
1. same key is used for both encryption and Decryption.
2. Secret key must not be lost or shared with unauthorized parties or else they can read message
3. It's faster and functions without lot of overheads on network or CPU resources.



ASSYMMETRIC CRYPTOGRAPHY:

1. Assymmetric 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.

DATE _____ DAY M T W T F S S



QUESTION # 17

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

QUESTION # 18

GRAPHS:

- In Computer Science, graphs is used to represent computer networks, data organization and the flow of computation.
- link between websites is showed using undirected graph.
- It is also used to study molecules in Chemistry and physics
- It is used in genetics.

DATE DAY M T W T F S S

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 use to ~~solve~~ network equations
- Matrices are used 3D visualisation of objects in gaming.

NUMBER THEORY:

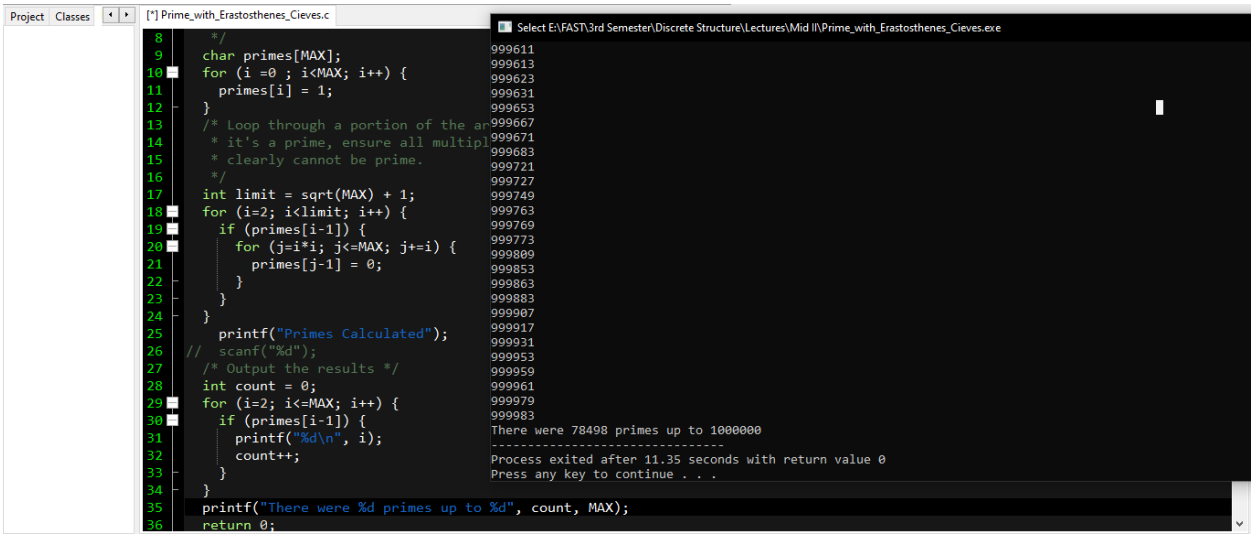
- Results generated from Number theory have countless application in mathematics as well as practical applications including security, memory management, authentication, coding theory etc.

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.

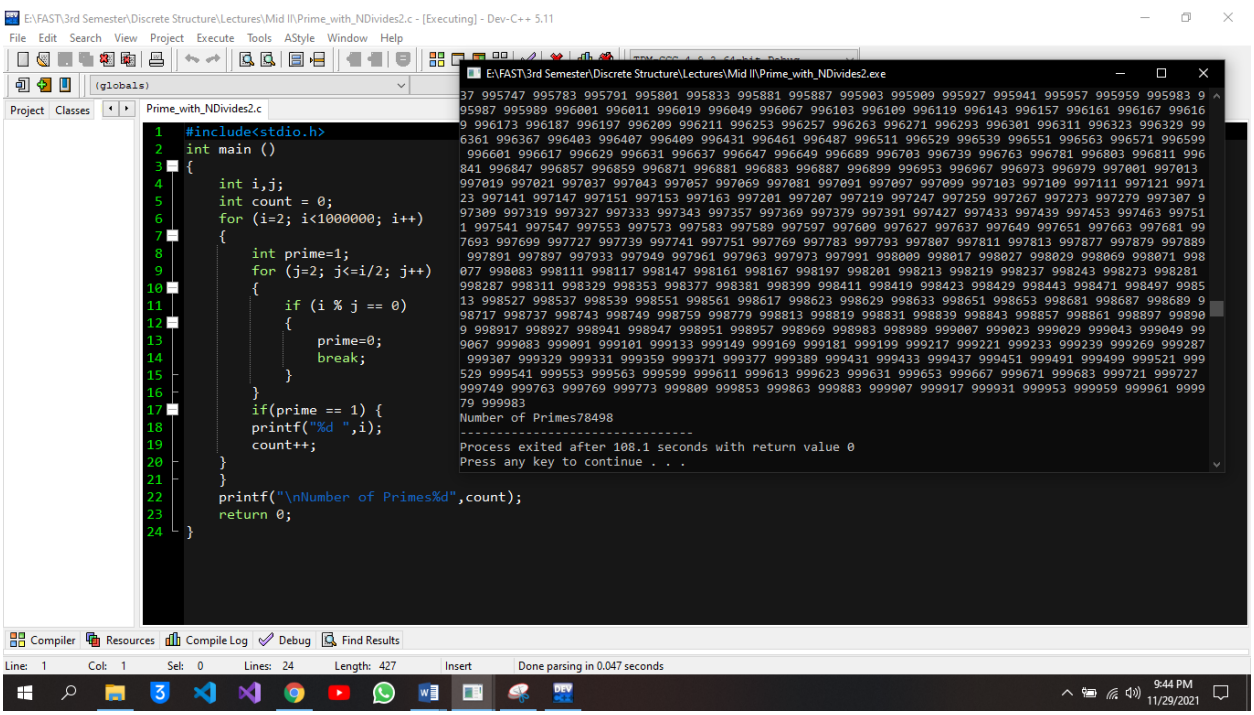
Question#11:

- **Prime with Eratosthenes**



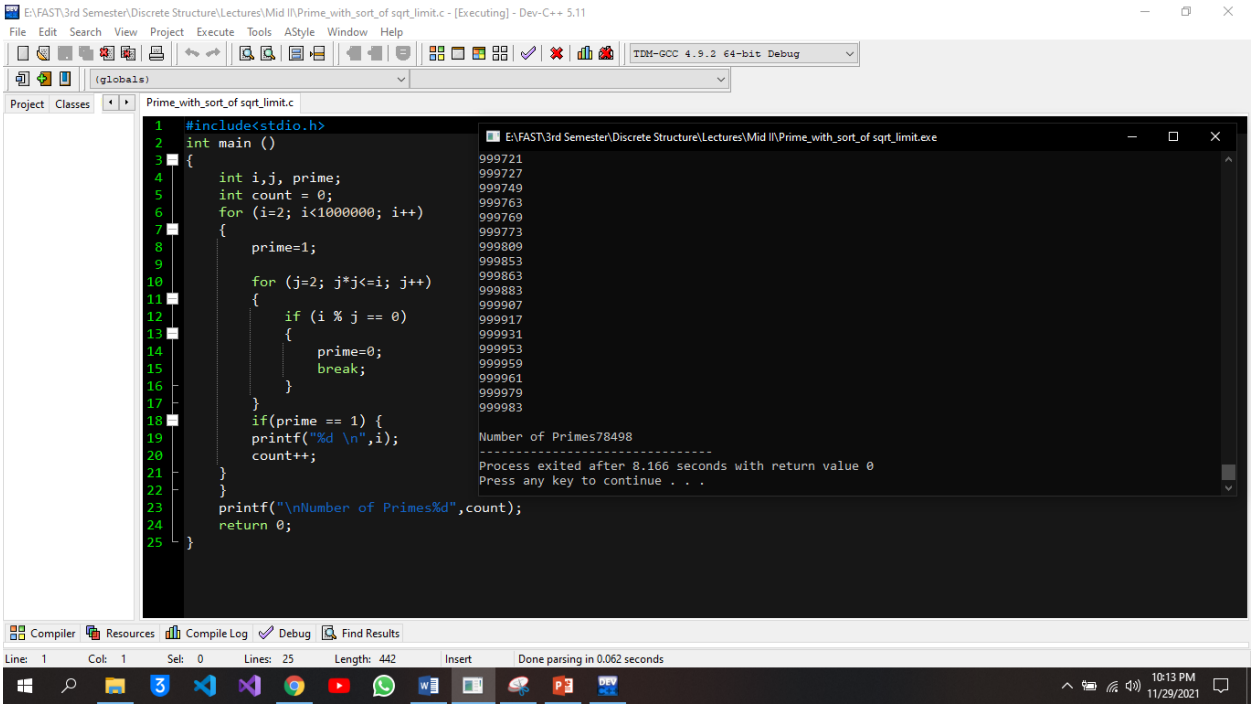
Time Complexity: O (N log (log N))

- **Prime with N divides 2**



Time Complexity: O (log (N))

- **Prime with sort of sqrt limit**



Time Complexity: O (sqrt(N))

BEST:

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