Date

Q5

(a)

(i) $55x \equiv 34 \pmod{89}$

inverse of 55 mod 89

$89 = 1(55) + 34$

$55 = 1(34) + 21$

$34 = 1(21) + 13$

$21 = 1(13) + 8$

$13 = 1(8) + 5$

$8 = 1(5) + 3$

$5 = 1(3) + 2$

$3 = 1(2) + 1$

Now, backward substitution

$1 = 3 - 1(2) \Rightarrow 3 - 1[5 - 1(3)]$

$1 \equiv 3 - 1(5) + 1(3) \rightarrow 2(3) - 1(5)$

$1 \equiv 2[8 - 1(5)] - 1(5) \rightarrow 2(8) - 2(5) - 1(5)$

$1 \equiv 2(8) - 3(5)$

$1 \equiv 2(8) - 3(13 - 1(8)]$

Signature

No.

Date

$1 \equiv 2(8) - 3(13) + 3(8)$

$1 \equiv 5(8) - 3(13)$

$1 \equiv 5(21 - 1(13)) - 3(13)$

$1 \equiv 5(21) - 5(13) - 3(13)$

$1 \equiv 5(21) - 8(13)$

$1 \equiv 5(21) - 8(34 - 1(21))$

$1 \equiv 5(21) - 8(34) + 8(21)$

$1 \equiv 13(21) - 8(34)$

$1 \equiv 13(55 - 1(34)) - 8(34)$

$1 \equiv 13(55) - 13(34) - 8(34)$

$1 \equiv 13(55) - 21(34)$

$1 \equiv 13(55) - 21(89 - 1(55))$

$1 \equiv 13(55) - 21(89) + 21(55)$

$1 \equiv 34(55) - 21(89)$

34 inverse

$55 \times 34 \equiv 34 \times 34 \pmod{89}$

$x = 1156 \bmod 89$ $\boxed{x \equiv 88}$

Signature

No

Date

(ii) $89x \equiv 2 \pmod{232}$

Sol.

$232 \equiv 2(89) + 54$

$89 \equiv 1(54) + 35$

$54 \equiv 1(35) + 19$

$35 \equiv 1(19) + 16$

$19 \equiv 1(16) + 3$

$16 \equiv 5(3) + 1 \rightarrow \gcd$

$\gcd(89, 232) = (33)(89) + (-232)(-89) \equiv 1$

80 inverse 73

$89 \times 73x \equiv 2 \times 73 \pmod{232}$

$x = 146 \mod 232$

$\boxed{x \equiv 146}$

$\boxed{Q6}$

i) $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.

$M = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 6 \cdot 7 = 210$

$M_1 = M/m_1 = 210/5 = 42$

$M_2 = M/m_2 = 210/6 = 35$

$M_3 = M/m_3 = 210/7 = 30$

M_1^{-1} = inverse of 42 mod 5

$42 = 8(5) + 2$

$5 = 2(2) + 1$

No.

Signature

Date

$1 \equiv 5 - 2(2)$
$1 \equiv 5 - 2[42 - 8(5)]$
$1 \equiv 5 - 2(42) + 16(5)$
$1 \equiv 17(5) - 2(42)$

$5 - 2 = 3$

$\boxed{m_1^{-1} = 3}$

m_2^{-1} inverse of 35 mod 6

$35 = 5(6) + 05$
$6 = 1(5) + 1$

$1 = 6 - 1(5)$
$1 \equiv 6 - 1(35 - 5(6))$
$1 \equiv 6(6) - 1(35)$

$6 - 1 \equiv 5$

$\boxed{m_2^{-1} = 5}$

m_3^{-1}
inverse of 30 mod 7

$30 \equiv 4(7) + 2$
$7 \equiv 3(2) + 1$

$1 \equiv 7 - 3(2)$
$1 \equiv 7 - 3[30 - 4(7)]$
$1 \equiv 7 - 3(30) + 7(7)$
$1 \equiv 8(7) - 3(30)$

$7 - 3 \equiv 4$

$\boxed{m_3^{-1} = 4}$

Date

$x = a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} \pmod{M}$

$x = 1 \cdot 42 \cdot 3 + 2 \cdot 35 \cdot 5 + 3 \cdot 30 + 4 \pmod{210}$

$x = 836 \pmod{210}$ ~~= 336~~

$\boxed{x \equiv 206}$

(ii) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$
$x \equiv 4 \pmod{11}$

$M = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 2 \cdot 3 \cdot 5 \cdot 11 = 330$

$M_1 = M/m_1 = 330/2 = 165$

$M_2 = 330/3 = 110$

$M_3 = 330/5 = 66$

$M_4 = 330/11 = 30$

$M_1^{-1} = 1$ $\quad M_2^{-1} = 2$ $\quad M_3^{-1} = 1$ $\quad M_4^{-1} = 7$

$x = a_1 M_1 \cdot M_1^{-1} + a_2 M_2 M_2^{-1} \text{ ——— } \pmod{M}$

$x = 1643 \pmod{330}$

$\boxed{x = 323}$ Ans

No.

Date

Q 7

a) $a = 2, m = 17$

Sol

$17 \equiv 8(2) + 1$

$1 \equiv 17 - 8(2)$

$17 - 8 \equiv 9$

inverse $\bar{a} \equiv 9$

b) $a = 34 \quad m = 89$

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

$89 - 34 = 55$

inverse $\bar{a} = 55$

c) $a = 144 \quad m = 233$

$\gcd(144, 233) = (89)(144) + (-23)(233)$

inverse $= 89$

inverse $\bar{a} = 89$

Date

d) $a = 200 \quad m = 1001$

$\gcd(200, 1001) = 1(1001) + (-5)\,200 = 1$

$-5 + 1001$

$\Rightarrow 996$

$\boxed{\bar{a} = 996}$

$\boxed{Q\,8}$

(a) (i)

$f(p) = (p+4) \cdot \bmod 26$

S	T	O	P	P	O	L	U	T	I	O	N	
18	19	14	15	15	14	11	11	20	19	08	14	13

After applying

W	X	S	T	T	S	P	P	Y
22	23	18	19	19	18	15	15	24

Y	M	S	R
23	12	18	19

(ii) $f(p) = f(p+21) \bmod 26$

After applying

13	14	09	10	10	9	6	6	15	14	3	9	8
N	O	J	K	K	J	G	G	P	O	D	J	I

Signature

No.

Date

$f(p) = (p + 10) \bmod 26$

i) C E B B O X N O B X Y B

02 04 01 01 14 23 13 14 01 23 24 06

decrypted.

SURRENDER NOW

(ii) L O W T P B S O X N

11 14 22 08 15 01 18 14 23 13

decrypted

BE MY FRIEND

Q 9

i) $5^{2003} \bmod 7$

$5^6 \equiv 1 \bmod 7$

$(5^6)^{333} \cdot 5^5 \bmod 7 = 5^5 \bmod 7$

$625 \bmod 7 = 3$ A

ii) $5^{2003} \bmod 11$

$5^{10} \equiv 1 \bmod 11$

$(5^{10})^{200} \cdot 5^3 = 5^3 \bmod 11$

$125 \bmod 11 = 14$ A

Date

iii) $5^{2003} \bmod 13$

$5^{12} = 1 \bmod 13$

$(5^{12})^{166} \cdot 5^{11} \bmod 13 = 5^{11} \bmod 13$

$\Rightarrow 8$

(b)

A	I	I	A	C	K
00	19	19	00	2	16

$n = 43 \cdot 59 = 2594$

$k = (43-1)(59-1) = 2436$

$c = 13$

encryption.

$c = 0019^{13} \bmod 2537$

$c = 1900^{13} \bmod 2537$

$c = 0710^{1} \bmod 2537$

$\boxed{Q10}$

(a)

i)

I	L	O	V	E	D	I	S	C	R	E	T	E	M	A	T	H	E	M	A	T
08	11	14	21	04	3	8	18	2	19	4	19	4	12	00	19	07	04	12	00	19

I	C	S
08	02	18

Date

Applying upper case

$\Rightarrow : f(p) = f(p+3) \bmod 26$.

encrypted msg.

LORYA VFUITWH PDWKHDPWLPV

(b)

i) PLGWZR DVVLJOPHOW

using lower upper case algo

$f(p) = (1-3) \bmod 26$

~~to~~ decrypted msg

MID TWO ASSIGNMENT.

ii) IDVW QXFHV XQLYHUVLWB

$f(p) = (1-3) \bmod$

decrypted ms

'FAST NUCES UNIVERSITY'

Date

C ounting Techniques.

Q1

a)

$^8C_3 = 56$ ways to choose school

b) $^{12}C_6 = 924$ ways to select elective

c) $^9C_5 = 126$ diff teams can be selected

Q2

a) $^{20}P_5 = 1,860,480$

ways to choose chair, assis chair, treasurer, record keeper and advisor.

b) $^{16}P_4 = 43680$ way to coach can select students to compete in race

c) $^{15}P_2 = 210$ ways students can be chosen for 2 pos.

Q3

a) Sol.

$^5C_1 \times {}^5C_2 \times {}^4C_1 \times {}^6C_3$

$5 \times 6 \times 4 \times 20 = 1200$ diff sandwiches

(b)

$48 \times 24 \times 34 \times 28 \times 28 = 460,815,680$ faces

Signature

No.

Date

Q4

(a)

Sol.

A = begin with 0s = $2^7 = 128$

B " " two 0s = $2^8 = 256$

$A \cap B = 2^5 = 32$

$A \cup B = A + B - A \cap B$

$\Rightarrow 128 + 256 - 32$

$\Rightarrow 252$ Ans

(b)

Sol. A = Begin with 0s = $2^4 = 16$

B = " end " two 1s = $2^3 = 8$

$A \cap B = 2^2 = 4$

$A \cup B = A + B - A \cap B$

$= 16 + 8 - 4 \Rightarrow 28$ Ans

Q5

(a)

no. of bases from 1 to 12.

6 pair whose sum 13

Signature

No.

Date

(1,12), (2,11), (3,10), (4,9), (5,8), (6,7).

- If 7 nos are chosen from 12, by pigeonhole principle at least one pair of numbers will be chosen that sum to 13.

(b)

7 days a week.

If 8 people are chosen by pigeonhole principle at least 7 of them must have been selected.

Signature

No.