20K-1052.

Date:

$f(P) = (P+21) \bmod 26$

S T O P P O L L U T I O N

18, 19, 14, 15, 15, 14, 11, 11, 20, 19, 8, 14, 13

$f(S) = (18+21) \bmod 26 = 13$ (N)
$f(T) = (19+21) \bmod 26 = 14$ (O)
$f(O) = (14+21) \bmod 26 = 9$ (J)
$f(P) = (15+21) \bmod 26 = 10$ (K)
$f(L) = (11+21) \bmod 26 = 6$ (G)
$f(I) = (8+21) \bmod 26 = 3$ (D)
$f(N) = (13+21) \bmod 26 = 13$ (8)

encrypted message is:
NOJK KJGGPODJI

b) Decrypt using Shift Ciphee $f(P) = (P \mp 10) \bmod 26$

i) CEBBOXNOBXYG.

2, 4, 1, 1, 14, 23, 13, 14, 1, 23, 24, 6

$f(C) = (2 \mp 10) \bmod 26 = \cancel{12} -8+26 = 18$ (S)
$f^{-1}(E) = (4 \mp 10) \bmod 26 = \cancel{14} -6+26 = 20$ (U)
$f^{-1}(O) = (14-10) \bmod 26 = 4$ (E)
$f^{-1}(X) = (23-10) \bmod 26 = 13$ (N)
$f^{-1}(Y) = (24-10) \bmod 26 = 14$ (O)
$f^{-1}(G) = (6-10) \bmod 26 = -4+26 = 22$ (W)
$f^{-1}(B) = (1-10) \bmod 26 = -9+26 = 17$ (R)

SURRENDER NOW

ii) LO WI PBSOXN

11, 14, 22, 8, 15, 1, 18, 14, 23, 13

$P^{-1}(L) = (11-10) \bmod 26 = 1$ (B)

$P^{-1}(O) = (14-10) \bmod 26 = 4$ (E)

$P^{-1}(W) = (22-10) \bmod 26 = 12$ (M)

$P^{-1}(I) = (8-10) \bmod 26 = -2+26 = 22$

$P^{-1}(P) = (15-10) \bmod 26 = 5$ (F) (W)

$P^{-1}(B) = (1-10) \bmod 26 = -9+26 = 17$ (R)

$P^{-1}(S) = (18-10) \bmod 26 = 8$ (I)

$P^{-1}(X) = (23-10) \bmod 26 = 13$ (N)

$P^{-1}(N) = (13-10) \bmod 26 = 3$ (D)

BE MY FRIEND

Q.19 Use Fermat's little theorem

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

$a^{P-1} = 1 \bmod p$

$5^{7-1} = 1 \bmod 7$

$5^6 = 1 \bmod 7$

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

$2003 = 6(333) + 5$

$5^5 \times 1 \bmod 7$

$3125 \bmod 7$

3

20K-1052

Date:

) $5^{2003} \bmod 11$

$5^{11-1} = 1 \bmod 11$

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

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

$1 \times 125 \bmod 11$

4.

$2003 = 10(200) + 3$

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

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

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

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

$1 \times 5^{11} \bmod 13$

$48828125 \bmod 13$

8.

$2003 = 12(166) + 11$

Q.20 Encrypt using Caesal Ciphel (key=3)

a) I LOVE DISCRETE MATHEMATICS.

$f(p) = (p+3) \bmod 26$

$f(I) = (8+3) \bmod 26 = 11$

$f(L) = (11+3) \bmod 26 = 14$

$f(O) = (14+3) \bmod 26 = 17$

$f(V) = (21+3) \bmod 26 = 24$

$f(E) = (4+3) \bmod 26 = 7$

$f(D) = (3+3) \bmod 26 = 6$

$f(S) = (18+3) \bmod 26 = 21$

$f(C) = (2+3) \bmod 26 = 5$

$f(R) = (17+3) \bmod 26 = 20$

$f(T) = (19+3) \bmod 26 = 22$

$f(M) = (12+3) \bmod 26 = 15$

$f(A) = (0+3) \bmod 26 = 3$

$f(H) = (7+3) \bmod 26 = 10$

f

Encrypted text would be

"L ORYH GLVFUH WH PDWKHPDWLFV"

Victory

Page No.

b) Decrypt using Caesar Cipher.

i) PLGWZR DVVLJQPHQW

$f(P) = (P-3) \bmod 26$

$f^{-1}(P) = (15-3) \bmod 26 = 12$ (M)
$f^{-1}(L) = (11-3) \bmod 26 = 8$ (I)
$f^{-1}(G) = (6-3) \bmod 26 = 3$ (D)
$f^{-1}(W) = (22-3) \bmod 26 = 19$ (T)
$f^{-1}(Z) = (25-3) \bmod 26 = 22$ (W)
$f^{-1}(R) = (17-3) \bmod 26 = 14$ (O)
$f^{-1}(D) = (3-3) \bmod 26 = 0$ (A)
$f^{-1}(V) = (21-3) \bmod 26 = 18$ (S)
$f^{-1}(J) = (9-3) \bmod 26 = 6$ (G)
$f^{-1}(Q) = (16-3) \bmod 26 = 13$ (N)
$f^{-1}(H) = (7-3) \bmod 26 = 4$ (E)

Decrypted message is

MID TWO ASSIGNMENT

20K-1050.

Date:

) IDVW QXFHV XQLYHUVLWB

$f(P) = (P-3) \bmod 26$

$f^{-1}(I) = (8-3) \bmod 26 = 5$ (F)
$f^{-1}(D) = (\cancel{9}3-3) \bmod 26 = 0$ (A)
$f^{-1}(V) = (2\cancel{0}1-3) \bmod 26 = 17$ ($\cancel{R}$ S)
$f^{-1}(W) = (22-3) \bmod 26 = 19$ (T)
$f^{-1}(Q) = (16-3) \bmod 26 = 13$ (N)
$f^{-1}(X) = (23-3) \bmod 26 = 20$ (U)
$f^{-1}(f) = (5-3) \bmod 26 = 2$ (C)
$f^{-1}(H) = (7-3) \bmod 26 = 4$ (E)
$f^{-1}(X) = (23-3) \bmod 26 = 20$ (U)
$f^{-1}(L) = (11-3) \bmod 26 = 8$ (I)
$f^{-1}(Y) = (24-3) \bmod 26 = 21$ (V)
$f^{-1}(U) = (20-3) \bmod 26 = 17$ (R)
$f^{-1}(B) = (1-3) \bmod 26 = -2+26 = 24$ (Y)

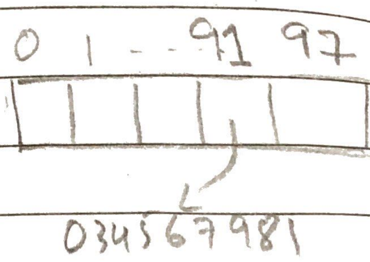
Decrypted Message is

FAST NUCES UNIVERSITY

Q.21 h(K) = K mod 97

i) 034567981

034567981 mod 97 = 91



ii) 183211232

183211232 mod 97 = 57

iii) 220195744

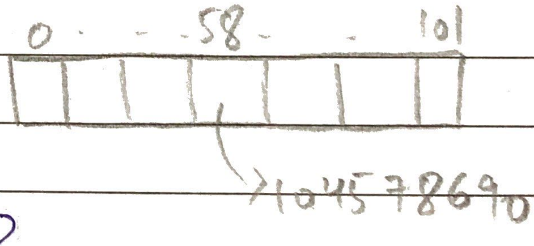
220195744 mod 97 = 21

iv) 987255335

987255335 mod 97 = 5

b) h(K) = K mod (101)

i) 104578690



104578690 mod 101 = 58

ii) 432222187

432222187 mod 101 ~~6~~ = 60

iii) 372201919

372201919 mod 101 = 32

20K-1050.

Date:

iv) 501338753

$501338753 \bmod 101 = 3$

Q.22

$x_{n+1} = (4x_n + 1) \bmod 7$ with seed $x_0 = 3$

$x_1 = (4 \times 3 + 1) \bmod 7$
$= (13) \bmod 7 = 6$

$x_2 = (4 \times 6 + 1) \bmod 7$
$= (25) \bmod 7 = 4$

$x_3 = (4 \times 4 + 1) \bmod 7$
$= (17) \bmod 7 = 3$

$x_4 = (4 \times 3 + 1) \bmod 7$
$= (13) \bmod 7 = 6$ ✓

$x_5 = (4 \times 6 + 1) \bmod 7$
$= (25) \bmod 7 = 4$ ✓

$x_6 = (4 \times 4 + 1) \bmod 7$
$= (17) \bmod 7 = 3$ ✓

Date:

Q.23 check digit for the UPCs (11 digits)

i) 73232184434

$7\times3+3+2\times3+3+2\times3+1+8\times3+4+4\times3+3\times3+4\times x_{12}=0 \bmod 10$

$21+3+6+3+6+1+24+4+12+3+12+x_{12}=0 \bmod 10$

$95+x_{12}=0 \bmod 10$

Check digit is $x_{12}=5$

ii) 63623991346

$6\times3+3+6\times3+2 * 3\times3+9+9\times9+1+3\times3+4+6\times3+x_{12}=0 \bmod 10$

$18+3+18+2+9+9+27+1+9+4+18+x_{12}=0 \bmod 10$

$118+x_{12}=0 \bmod 10$

Check digit is $x_{12}=2$

20K-1052.

Date:

b) 12 digit UPC code is valid or not.

i) 036000291452

$0\times3+3+6\times3+0+0+0+2\times3+9+1\times3+4+5\times3$
$+2 = 0 \bmod 10$

$0+3+18+0+0+0+6+9+3+4+15+2 = 0 \bmod 10$
$60 = 0 \bmod 10$

Valid UPC code

ii) 012345678903

$0\times3+1+2\times3+3+4\times3+5+6\times3+7+8\times3+9+0\times3$
$+3 = 0 \bmod 10$

$1+6+3+12+5+18+7+24+9+3 = 0 \bmod 10$

$88 \neq 0 \bmod 10$

Q.24 ISBN-10

0-07-119881 (first nine digits).

Check digit?

$1\times 0 + 2\times 0 + 7\times 3 + 1\times 4 + 1\times 5 + 9\times 6 + 8\times 7 \times 8\times 8 + 9\times 1$
$+ x_{10} = 0 \bmod 11$

$21 + 4 + 5 + 54 + 56 + 64 + 9 + x_{10} = 0 \bmod 11$
$213 + x_{10} = 0 \bmod 11$

Check digit, $x_{10} = 4$

b) 0-321-500Q1-8 Find Q, its value

$x_{10} = 1\times 0 + 2\times 3 + 3\times 2 + 1\times 4 + 5\times 5 + 8\times Q + 9\times 1 \bmod 11$

$= 6 + 6 + 4 + 25 + 8Q + 9 \bmod 11$
$= 8Q + 50 \bmod 11$

Check digit $= 8$

$8 = 8Q + 50 \bmod 11$ $\quad \therefore 50 \bmod 11 = 6$
$8 = 8Q + 6 \bmod 11$
$8 - 6 = 8Q + \cancel{6} \bmod 11$
$8Q \bmod 11 = 2$
$7 \times 8Q \bmod 11 = 2\times 7 \bmod 11$
$Q \bmod 11 = 14 \bmod 11$
$Q \bmod 11 = 3$

Q has to be 3 so that it is smaller than 11 and btw (0-9)

$Q = 3$
$3 \mod 11 = 3$ Proved

Q.25 Encrypt ATTACK using RSA system with $n = 43.59$ and $e = 13$

A T T A C K
00, 19, 19, 00, 02, 10

$n = p \times q$
$K = (p-1)(q-1)$
$1 < e < K$
$GCD(e, K) = 1$
$C = M^e \mod n$

$n = 43 \times 59 = 2537$
$K = (43-1)(59-1) = 2436$
$e = 13$

$C = \overset{A}{00}\overset{T}{19}^{13} \mod 2537$
$C = 1900^{13} \mod 2537$
$C = 0210^{13} \mod 2537$

Q.26 First five terms of the sequence.

i) $2^n - 1$

$n = 1 \quad 2^1 - 1 = 2$
$n = 2 \quad 2^2 - 1 = 3$
$n = 3 \quad 2^3 - 1 = 7$
$n = 4 \quad 2^4 - 1 = 15$
$n = 5 \quad 2^5 - 1 = 24$

Date:

ii) $10 - \frac{3}{2}n$

$n=1$ $\quad 10-\frac{3}{2}=\frac{17}{2}$

$n=2$ $\quad 10-\frac{3}{2}\times 2=7$

$n=3$ $\quad 10-\frac{3\times 3}{2}=\frac{11}{2}$

$n=4$ $\quad 10-\frac{3\times 4}{2}=4$

$n=5$ $\quad 10-\frac{3\times 5}{2}=5$

iii) $\frac{(-1)^n}{n^2}$

$n=1$ $\quad (-1)^1/(1)^2=-1$

$n=2$ $\quad (-1)^2/(2)^2=1/4$

$n=3$ $\quad (-1)^3/(3)^2=-1/9$

$n=4$ $\quad (-1)^4/(4)^2=1/16$

$n=5$ $\quad (-1)^5/(5)^2=-1/(25)$

20K-1050.

Date:

iv) $\dfrac{3n+4}{2n-1}$

$n=1$ $\quad \dfrac{3(1)+4}{1} = 7$

$n=2$ $\quad 3(2)+4/3 = 10/3$

$n=3$ $\quad 3(3)+4/5 = 13/5$

$n=4$ $\quad 3(4)+4/7 = 16/7$

$n=5$ $\quad 3(5)+4/9 = 19/9$

b) Identify as A.P or G.P

i) $-15, -22, -29, -36 \; \ldots$ 11^{th} term.

$T_2 - T_1 = T_3 - T_2$

$-22-(-15) = -29-(-22)$

$-7 = -7$

$T_4 - T_3 = -36-(-29) = -7$

Same common difference so A.P

11^{th} term $= a+10d$

$= (-15)+10(-7)$

$= -85$

Date:

ii) $a-42b, a-39b, a-36b, a-33b \ldots 15^{th}$

$T_2 - T_1 = T_3 - T_2$

$a - 39b - (a-42b) = a-36b-(a-39b)$

$\cancel{a} - 39b - \cancel{a} + 42b = a - 36b - a + 39b$

$3b = 3b$

Same common difference so A.P

iii) 15^{th} Term $= a + 14d$

$= (a-42b) + 14(3b)$

$= a - 42b + 42b$

$= a$

iii) $4, 3, \frac{9}{4} \ldots 17^{th}$ term.

$\frac{T_2}{T_1} = \frac{T_3}{T_2}$

$\frac{3}{4} = \frac{9/4}{3} = 0.75$

Same ratio so G.P

17^{th} term $= ar^{n-1}$

$= 4 \times \left(\frac{3}{4}\right)^{17-1}$

$= \frac{4 \times 3^{16}}{4^{16}}$

20K-1052.

Date:

v) $32, 16, 8 \ldots$ 9th term.

$$\frac{16}{32} = \frac{8}{16} = \frac{1}{2} \quad \text{so G.P}$$

$$9^{th} \text{ term} = ar^{n-1}$$
$$= 32\left(\frac{1}{2}\right)^{9-1}$$
$$= 32 \times 2^{-8}$$
$$= 2^{5-8}$$
$$= \frac{1}{8}$$

Q.27. i) $T_3 = 10 \quad T_5 = 2\frac{1}{2}$

$$ar^2 = 10$$
$$ar^4 = \frac{5}{2}$$

$$\frac{10}{r^2} = \frac{5}{2r^4}$$

$$r^2 = \frac{5}{10}$$
$$r^2 = \frac{1}{2}$$
$$r = \pm\sqrt{\frac{1}{2}}.$$

$$r^2 = \frac{10}{a}$$
$$a = \frac{10}{(1/\sqrt{2})^2} = 20$$

$$T_n = ar^{n-1}$$
$$= 20\left(\frac{1}{\sqrt{2}}\right)^{n-1}$$

Date:

ii) $T_5 = 8$ and $T_8 = \frac{-64}{27}$

$ar^4 = 8$

$ar^7 = -\frac{64}{27}$

$r^4 = \frac{8}{a}$

$r^7 = \frac{-64}{27a}$

$\frac{8}{r^4} = \frac{-64}{27r^7}$

$r^3 = \frac{-64}{27 \times 8}$

$r = \frac{-2}{3}$

$a = \frac{8}{r^4}$

$= \frac{8}{(-2/3)^4} = \frac{81}{2}$

$T_n = ar^{n-1}$

$= \frac{81}{2}\left(\frac{-2}{3}\right)^{n-1}$

b) $T_4 = 7$ $T_{16} = 31$

$a + 3d = 7$

$-(a + 15d = 31)$

$-12d = -24$

$d = 2$

$a = 7 - 3(2)$

$= 1$

$T_n = (a + (n-1)d)$

$= 1 + (n-1)(2)$

$= 1 + 2n - 2$

$= 2n - 1$

Victory

Page No.

$T_5 = 86$

20K-1052.

Date:

1) $T_5 = 86$ and $T_{10} = 146$

$a + 4d = 86$

$-(a + 9d = 146)$

$-5d = -60$

$d = 12$

$T_n = a + (n-1)d$

$= 38 + (n-1)12$

$= 12n + 26.$

$a = 86 - 4(12)$

$= 38$

Q.28 a) N nos div btw 789 and 256 by 7

$= \frac{789 - 256}{7} = 76$ numbers.

$\text{sum} = \frac{n}{2}(a+l) = \frac{76}{2}(789+256) = 39{,}710.$

b) $a = \frac{1}{n}$ $\quad l = \frac{n^2 - n + 1}{n}$

Sum of first n terms.

$= \frac{n}{2}(a+l)$

$= \frac{n}{2}\left(\frac{1}{n} + \frac{n^2 - n + 1}{n}\right)$

$= \frac{\cancel{n}}{2}\left(\frac{n^2 - n + 2}{\cancel{n}}\right)$

$= \frac{n^2 - n + 2}{2}$

Q.29 Sum of first 100 terms of $a_j = \frac{1}{j}$
for $j = 1, 2, 3 \ldots$

$$= \sum_{j=1}^{100} \left(\frac{1}{j}\right)$$

$$= \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} \text{ - - - - } \frac{1}{100}$$

$= 5.187.$ (calculater based answer).

b) i) $\sum_{k=4}^{8} (-1)^k$

$$= (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7 + (-1)^8$$
$$= 1 - 1 + 1 - 1 + 1$$
$$= 1$$

ii) $\sum_{j=1}^{5} (j)^2$

$$= (1)^2 + (2)^2 + (3)^2 + (4)^2 + (5)^2$$
$$= 55$$

20K-1052.

Date:

Q.30 First six terms of recurrence relations.

a) $a_n = -2a_{n-1}, a_0 = -1$

$a_1 = -2a_0$
$= -2(-1) = 2$

$a_2 = -2(2) = -4$

$a_3 = -2(-4) = 8$

$a_4 = -2(8) = -16$

$a_5 = -2(-16) = 32.$

$a_6 = -2(32) = -64$

b) $a_n = a_{n-1} - a_{n-2}, a_0 = 2, a_1 = -1$

$a_2 = a_1 - a_0 = -1 - (2) = -3$

$a_3 = a_2 - a_1 = -3 - (-1) = -2$

$a_4 = a_3 - a_2 = -2 - (-3) = 1$

$a_5 = a_4 - a_3 = -2 - (-2) = 0$

$a_6 = a_5 - a_4 = 0 - (1) = 1$

c) $a_n = 3a^2_{n-1}, a_0 = 1$

$a_1 = 3(1)^2 = 3$

$a_2 = 3(3)^2 = 27$

$a_3 = 3(27)^2 = 2187$

$a_4 = 3(2187)^2 = 14348907$

$a_5 = 3(a_4)^2 = 6.17 \times 10^{14}$

$a_6 = 3(a_5)^2 = 1.14 \times 10^{30}$

20K-1052.

Date:

d) $a_n = na_{n-1} + a_{n-2}^2, a_0 = -1, a_1 = 0$

~~$a_2 = 2 \times a_0 +$~~

$a_2 = 2 \times a_1 + a_0^2 = 2(0) + (-1)^2 = 1$

$a_3 = 3 \times a_2 + a_1^2 = 3 \times (1) + (0)^2 = 3$

$a_4 = 4 \times a_3 + a_2^2 = 4 \times (3) + (1)^2 = 13$

$a_5 = 5 \times a_4 + a_3^2 = 5 \times (13) + (3)^2 = 92$

$a_6 = 6 \times a_5 + a_4^2 = 6 \times (92) + (13)^2 = 721$