USAMA SARWAR
FA17-BCS-090-B

Question # 01

$$a \bmod 13 = (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 13$$
$$= [(a_n \times 10^n) \bmod 13 + \dots + (a_1 \times 10^1) \bmod 13 + a_0 \bmod 13] \bmod 13$$
$$= \dots + a_5 \times (4) + a_4 \times (3) + a_3 \times (-1) + a_2 \times (-4) + a_1 \times (-3)$$
$$+ a_0 \times (1)] \bmod 13$$

For Example

$$631453672 \bmod 13 = [(-4)6 + (-3)3 + (1)1 + (4)4 + (3)5$$
$$+ (-1)3 + (-4)6 + (-3)7 + (1)2] \bmod 13$$
$$= 3 \bmod 13$$

Question # 02

a) First, calculate the freauency of letters in Ciphertext. If the frequency matches with the standard letter freqency, ~~transportatio~~ transposition cipher is in use else substitution cipher is used.

b) Exhaustive Search. First, she would try all keys for the substitution Cipher. If failed, then try all keys for the multiplicative cipher. Finally all keys for affine cipher.

c) She can find block size by Exhaustive Search.

Question # 04.

Cipher Text: "The house is being sold tonight"

a) Vigenere Cipher

Key: dollars

P	The house is being soldtonight
P's Value	19 7 4 7 14 20 18 4 8 18 1 4 8 13 6 18 14 11 3 19 14 13 8 6 7 19
key	3 14 11 11 0 17 18 3 14 11 11 0 17 18 3 14 11 11 0 17 18 3 14 11 11 0
C's Value	22 21 15 18 14 37 36 7 22 29 12 4 25 31 9 32 25 22 33 36 32
Cipher Text	W V P S O L K H W D M E Z F J G Z W D K G

16	22	17	18	19
Q	W	R	S	T

Encryption: $C_i = P_i + K_i$

Cipher Text: WVPSOLKHWDMEZFJGZWDKGQWRST

b) Auto key Cipher

Key = 7

Encryption $C = (P_i + k_i) \bmod 26$

$K = (K_1, P_1, P_2, P_3 \dots)$

P	T h e h o u s e i s b e i n g s o l d tonight
P's Value	19 7 4 7 14 20 18 4 8 18 1 4 8 13 6 18 14 11 3 19 14 13 8 6 7 19
Key	7 19 7 4 7 14 20 18 4 8 18 1 4 8 13 6 18 14 11 3 19 14 13 8 6 7
C's Value	0 0 11 11 21 8 12 22 12 0 19 5 12 21 19 24 6 25 14 22 7 12 14 1 30
Cipher Text	A A L L V I M W M A T F M V T Y G Z OWHBVONA

c) Playfair Cipher

Th → WE	eh → CE	ou → IX
se → HO	is → NO	be → EI
in → FI	gs → DV	ol → BX
dt → BW	on → IS	ig → BR
ht → EW		

Cipher Text: WECEIXHONOEIFIDVBXBWISBREW

Question # 03

(a)

$$P = \begin{bmatrix} L(11) & e(04) & t(19) & U(20) \\ s(18) & m(12) & e(04) & e(04) \\ t(19) & n(13) & o(14) & w(22) \\ x(23) & y(24) & z(25) & b(01) \end{bmatrix}$$

∵ Introducing bogus row making square matrix

We know that

$$K = P^{-1}C$$

$$P = \begin{bmatrix} 11 & 04 & 19 & 20 \\ 18 & 12 & 04 & 04 \\ 19 & 13 & 14 & 22 \\ 23 & 29 & 25 & 01 \end{bmatrix}_{(4\times4)}$$

$$C = \begin{bmatrix} H(07) & B(01) & C(02) \\ P(03) & F(05) & N(13) \\ O(14) & P(15) & I(08) \\ K(10) & L(11) & B(01) \end{bmatrix}_{4\times3}$$

$$C = \begin{bmatrix} 07 & 01 & 02 \\ 03 & 05 & 13 \\ 14 & 15 & 08 \\ 10 & 11 & 01 \end{bmatrix}$$

No. of col ≠ No. of Rows

Can't find Multiplicative Inverse

Q 3 (b)

Shift of 4 chars

X V I E W Y W I

t r e a s u r e