Answer Key

(2). $7^{-1} \bmod 26$

$$26 = 3 \times 7 + 5$$
$$7 = 1 \times 5 + 2$$
$$5 = 2 \times 2 + 1$$

Since Remainder is '1', 7 & 26 are relatively prime and inverse exists.

$$1 = 5 - 2 \times 2$$
$$= 5 - 2 \times [7 - 1 \times 5] = 5 - 2 \times 7 + 2 \times 5 = 3 \times 5 - 2 \times 7$$
$$= 3 \times [26 - 3 \times 7] - 2 \times 7 = 3 \times 26 - 9 \times 7 - 2 \times 7$$
$$= 3 \times 26 - 11 \times 7$$

$\therefore\ 7^{-1} \bmod 26 = -11$ or $15 \bmod 26$.

(3) Fermat's theorem states that

$a^{P-1} \equiv 1 \bmod P$ where P is a prime number & a is a positive integer.

if $a = 3$ and $P = 7$ then

$$3^{7-1} \equiv 1 \bmod 7$$
$$3^6 = (3^3)^2 = (27 \bmod 7)^2$$
$$= (6 \bmod 7)^2 = 36 \bmod 7 = 1 \bmod 7$$

$$\Rightarrow 3^{7-1} \equiv 1 \bmod 7$$

(4) First three letters of any plaintext is encrypted

(i) using Vigenere – keyword = 'CAT' ⇒ 2 0 19 (CAT → numerical equivalent)

(ii) using general Caesar – Key = 2

⇒ Indicates first letter of every 3 letters of ciphertexts obtained from Vig & Cas. will be same (∵ key is same & also operation)

(8) Play fair Cipher.

Key Digram →

C	R	Y	P	T
O	G	A	H	B
D	E	F	I/J	K
L	M	N	Q	S
U	V	W	X	Z

Plain Text : she sells sea shells at sea shore

After grouping as two,

sh / es / el / ls / se / as / he / lx / ls / at / se / as / ho / re

↑ adding filler letter

Rules
(1)
(2)
(3)

Cipher Text:

QB / KM / DM / ML / MK / BN / G I/J / QU / ML / BY / MK / BN / BG / GM

GB KM DM ML MK BN G I/J QU ML BY MK BN BG GM

(9) Hill Cipher

Encryption:

$C = P.K \bmod 26$

$P = army \Rightarrow \begin{bmatrix} 0 & 17 \\ 12 & 24 \end{bmatrix}$

$\Rightarrow C = \begin{bmatrix} 0 & 17 \\ 12 & 24 \end{bmatrix} \begin{bmatrix} 5 & 18 \\ 17 & 3 \end{bmatrix} = \begin{bmatrix} 289 & 51 \\ 468 & 288 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 3 & 25 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} D & Z \\ A & C \end{bmatrix}$

Cipher Text = DZAC

$21^{-1} \bmod 26$

$26 = 1 \times 21 + 5$

$21 = 4 \times 5 + 1$

$1 = 21 - 4 \times 5$

$= 21 - 4 \times [26 - 1 \times 21]$

$= 5 \times 21 - 4 \times 26$

$= 5$

Decryption:

$P = C.K^{-1} \bmod 26$

$K^{-1} = \begin{bmatrix} 5 & 18 \\ 17 & 3 \end{bmatrix}^{-1} = 21^{-1} \begin{bmatrix} 3 & -18 \\ -17 & 5 \end{bmatrix} = 5 \begin{bmatrix} 3 & -18 \\ -17 & 5 \end{bmatrix} = \begin{bmatrix} 15 & -12 \\ -7 & 25 \end{bmatrix}$

$P = \begin{bmatrix} 3 & 25 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 15 & -12 \\ -7 & 25 \end{bmatrix} = \begin{bmatrix} 0 & 589 \\ -14 & 50 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 & 17 \\ 12 & 24 \end{bmatrix}$

= army