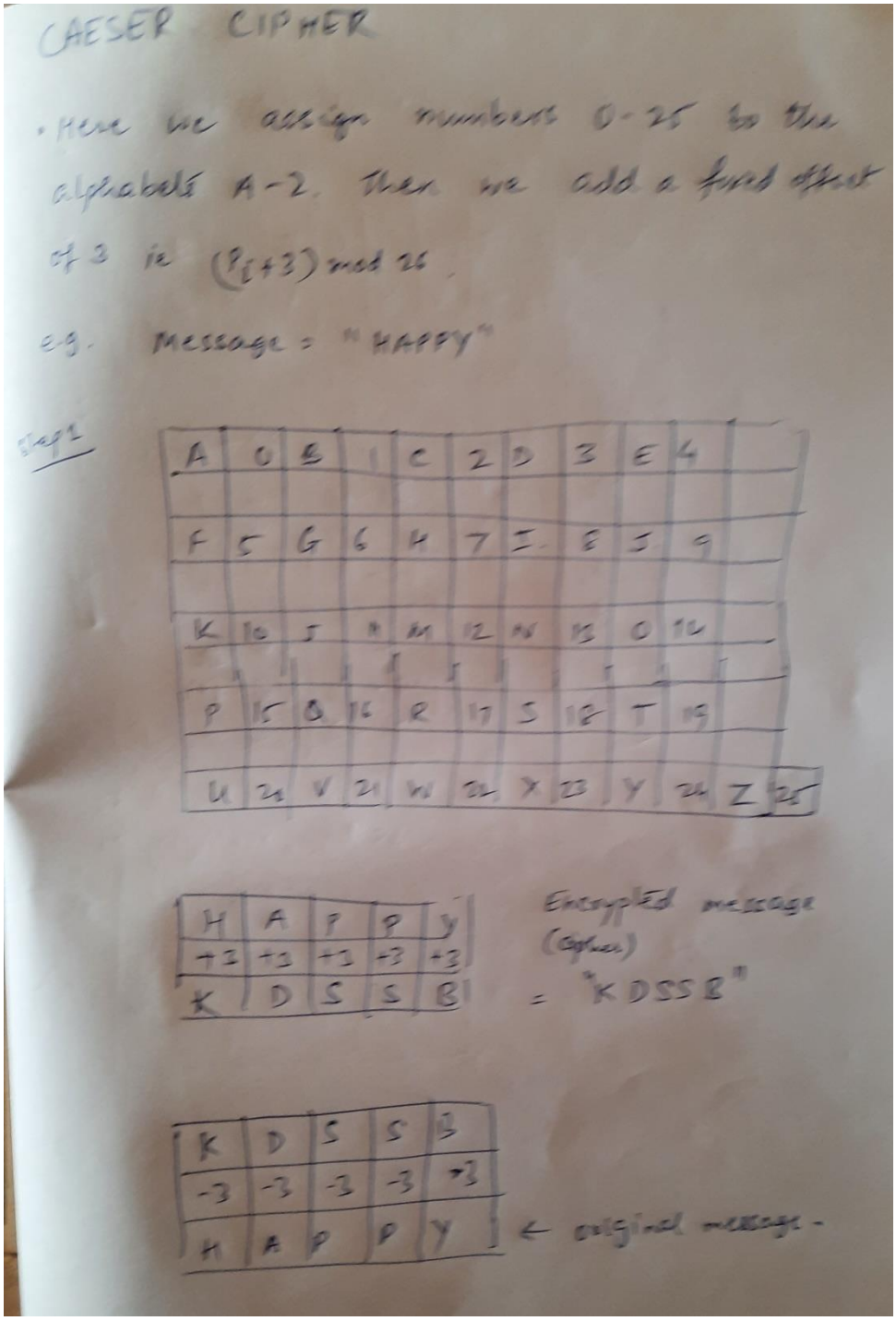
CAESER CIPHER



VIGENERE CIPHER

VIGENERE CIPHER

- Mostly used for text message encoding and decoding.
- We use a text "key" to encode a text "message"
- For encoding we use the formula

  $C_i = (P_i + K_i) \bmod 26$.

  where

  C_i = code corresponding to P_i (plain text)

  P_i = ith letter in the message.

  K_i = key element
- We assign numbers 0-25 to the letters A-Z
- For decoding (reverse process) we use

  $P_i = (C_i - K_i) \bmod 26$.

  * if $(C_i - K_i) < 0$ we add 26.

Show how you can encode and decode the message "MILLION" using the Vigenere cipher. The encryption key is "SKY".

1. We assign values to letters A-Z:

A	0	B	1	C	2	D	3	E	4	F	5	G	6	H	7
I	8	J	9	K	10	L	11	M	12	N	13	O	14	P	15
Q	16	R	17	S	18	T	19	U	20	V	21	W	22	X	23
Y	24	Z	25												

p2

M	I	L	L	I	O	N
S	K	Y	S	K	Y	S

p3

$P_i + K_i$	C_i	$C_i \% 26$	
M + S	12 + 18	04	E
I + K	8 + 10	18	S
L + Y	11 + 24	09	J
L + S	11 + 18	03	D
I + K	8 + 10	18	S
O + Y	14 + 24	12	M
N + S	13 + 18	05	F

The cipher or encrypted message is "ESJDSMF"

For decryption:

step 1: Use the same table in encryption

step 2:

E	S	J	D	S	M	F
S	K	Y	S	K	Y	S

step 3:

$C_i - K_i$	P_i	$P_i \% 26$	P.m
E - S	4 - 18	12	M
S - K	18 - 10	08	I
J - Y	9 - 24	11	L
D - S	3 - 18	11	L
S - K	18 - 10	08	I
M - Y	12 - 24	14	O
F - S	5 - 18	13	N

If the difference is negative, add 26.

AFFINE CIPHER

Affine cipher uses the formula

$c = (ax+b) \bmod m$.

Here $a=9$, $b=2$, $m=26$.

$c = (9x+2) \bmod 26$.

m	U	K	R	A	I	N	E
x	20	10	17	0	8	13	4
c = (9x+2)%26	A	M	Z	C	W	P	M

ciphertext = "AMZCWPM"

We have to find inverse of a (call it y)

Such that $a \cdot y \equiv 1 \bmod m$.

ie $(a \cdot y) \bmod m = 1$

ie $(9 \cdot y) \bmod 26 = 1$

y	a·y	(a·y)%26
1	9	9
2	18	18
3	27	1

$\therefore y = 3$.

For decryption we use the formula

$m = y(c-b) \bmod 26 \quad .= 3(c-2)\%26$

c ⇒	A	m	Z	C	W	P	m
x ⇒	0	12	25	2	22	15	12
m ⇒	U	K	R	A	I	N	E

$(x-2)\%26$