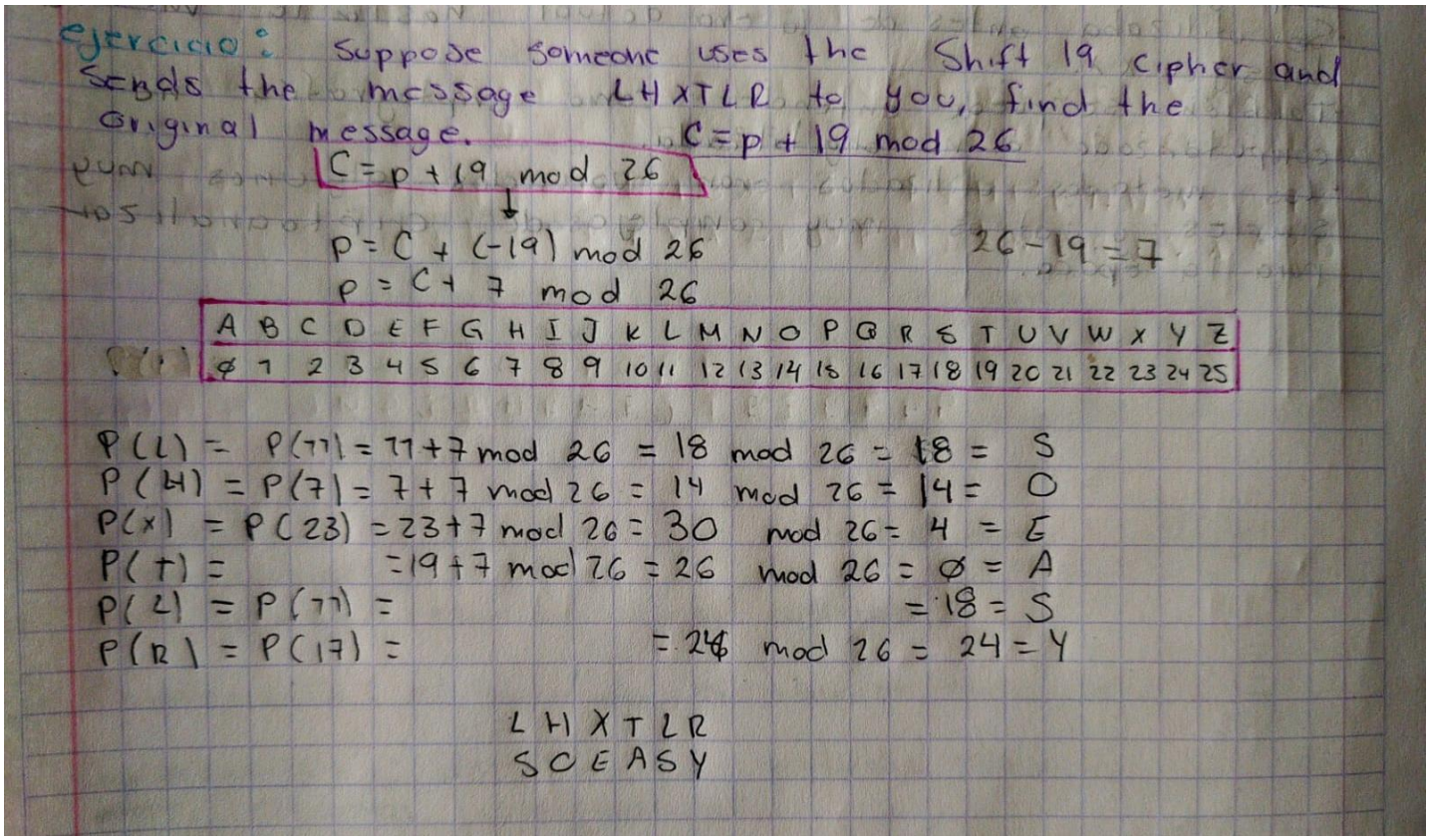


Ejercicio: Suppose someone uses the Shift 19 cipher and sends the message LHXTLR to you, find the original message. $C = p + 19 \mod 26$

$C = p + 19 \mod 26$

$p = C + (-19) \mod 26$ $\quad 26 - 19 = 7$

$p = C + 7 \mod 26$

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

$P(L) = P(11) = 11 + 7 \mod 26 = 18 \mod 26 = 18 = S$

$P(H) = P(7) = 7 + 7 \mod 26 = 14 \mod 26 = 14 = O$

$P(X) = P(23) = 23 + 7 \mod 26 = 30 \mod 26 = 4 = E$

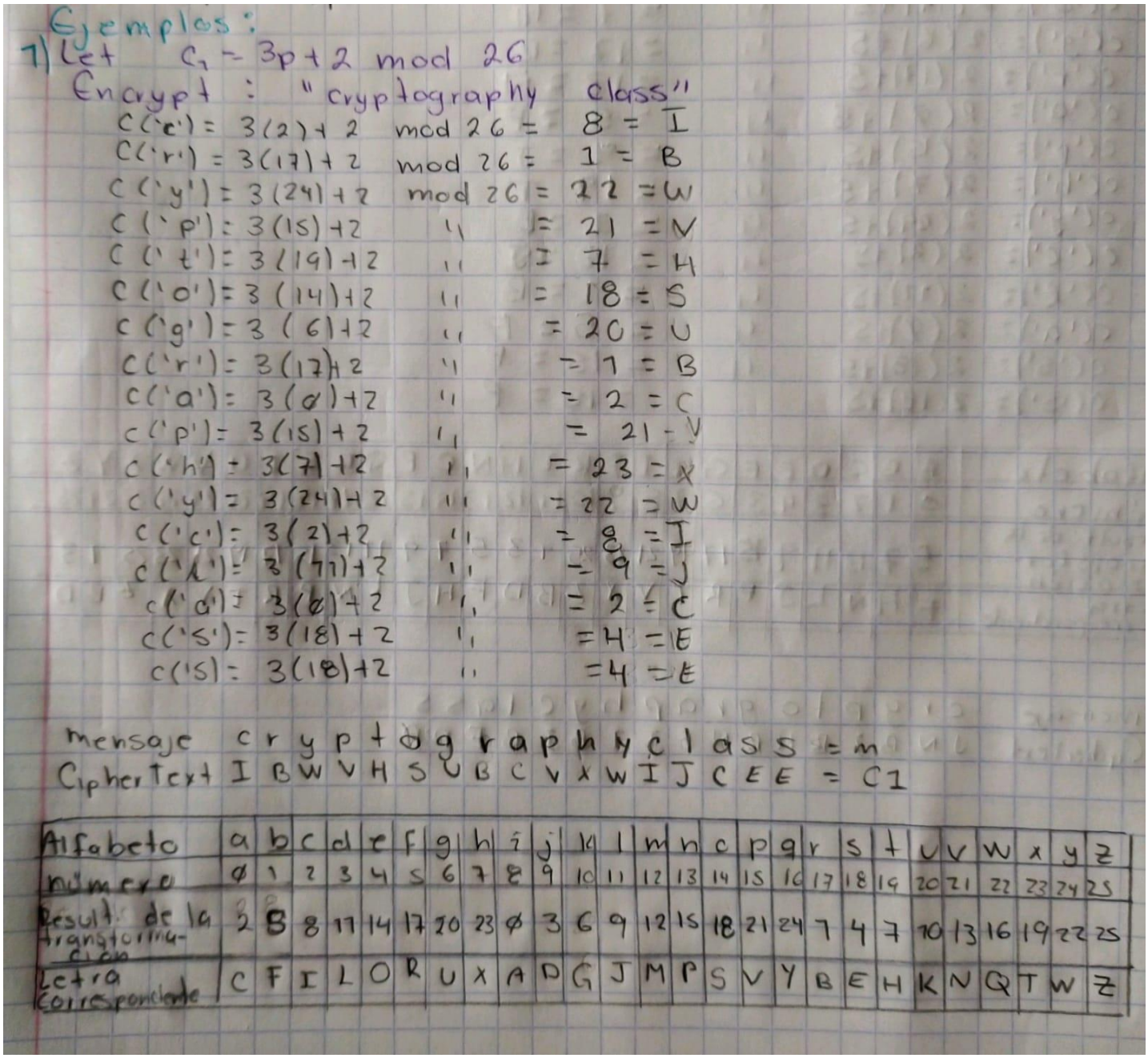
$P(T) = 19 + 7 \mod 26 = 26 \mod 26 = 0 = A$

$P(L) = P(11) = 18 = S$

$P(R) = P(17) = 24 \mod 26 = 24 = Y$

L H X T L R

S O E A S Y



Ejemplos:

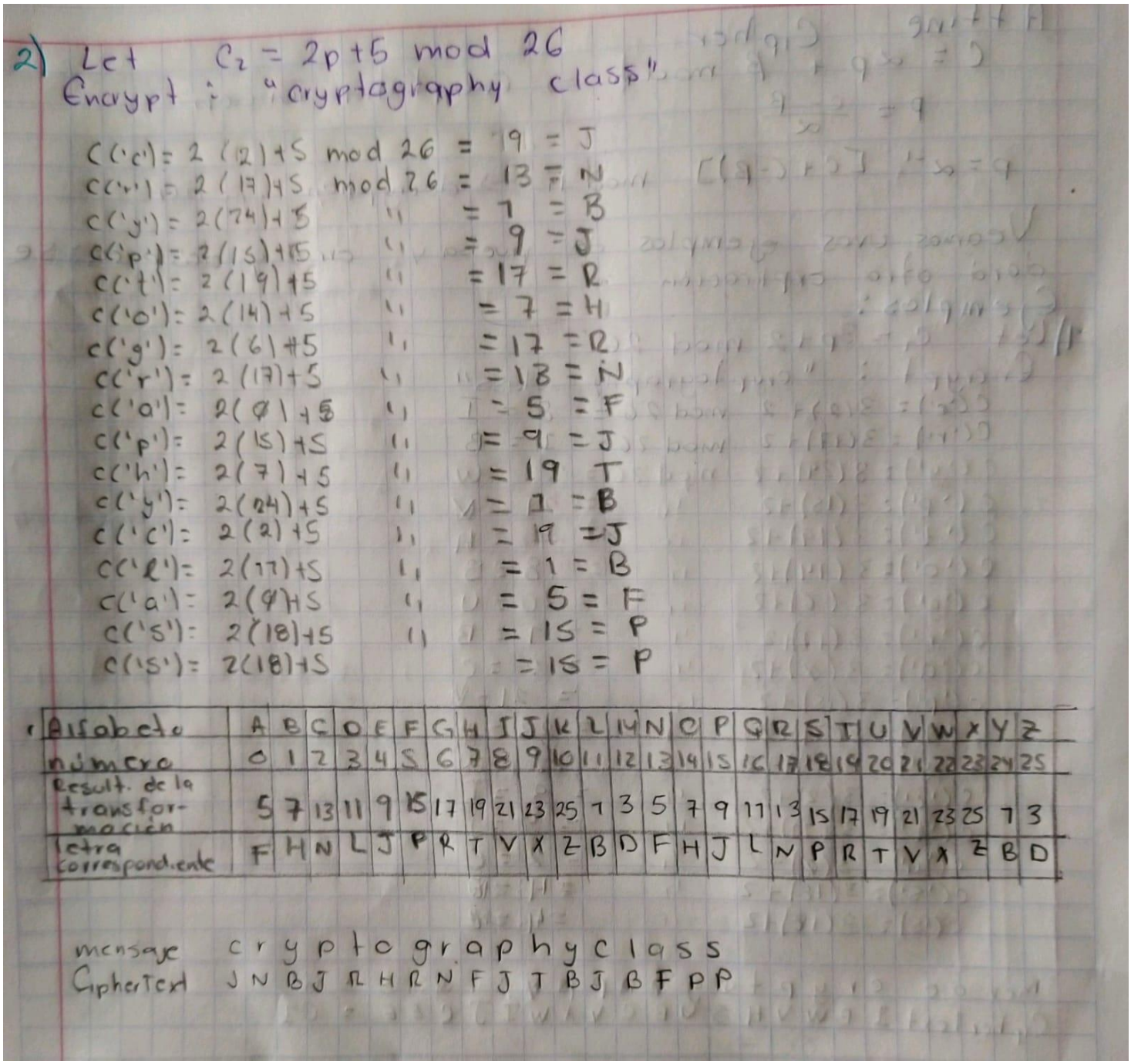
1) Let $C_1 = 3p + 2 \mod 26$

Encrypt: "cryptography class"

c('c') = 3(2) + 2 mod 26 = 8 = I
c('r') = 3(17) + 2 mod 26 = 1 = B
c('y') = 3(24) + 2 mod 26 = 22 = W
c('p') = 3(15) + 2 " = 21 = V
c('t') = 3(19) + 2 " = 7 = H
c('o') = 3(14) + 2 " = 18 = S
c('g') = 3(6) + 2 " = 20 = U
c('r') = 3(17) + 2 " = 1 = B
c('a') = 3(0) + 2 " = 2 = C
c('p') = 3(15) + 2 " = 21 = V
c('h') = 3(7) + 2 " = 23 = X
c('y') = 3(24) + 2 " = 22 = W
c('c') = 3(2) + 2 " = 8 = I
c('l') = 3(11) + 2 " = 9 = J
c('a') = 3(0) + 2 " = 2 = C
c('s') = 3(18) + 2 " = 4 = E
c(15) = 3(18) + 2 " = 4 = E

mensaje c r y p t o g r a p h y c l a s s = m
CipherText I B W V H S U B C V X W I J C E E = C1

Alfabeto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
número	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Result. de la transformación	2	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	7	4	7	10	13	16	19	22	25
Letra correspondiente	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z



2) Let $C_2 = 2p + 5 \bmod 26$

Encrypt: "cryptography class"

c('c') = 2(2)+5 mod 26 = 9 = J
c('r') = 2(17)+5 mod 26 = 13 = N
c('y') = 2(24)+5 " = 7 = B
c('p') = 2(15)+5 " = 9 = J
c('t') = 2(19)+5 " = 17 = R
c('o') = 2(14)+5 " = 7 = H
c('g') = 2(6)+5 " = 17 = R
c('r') = 2(17)+5 " = 13 = N
c('a') = 2(0)+5 " = 5 = F
c('p') = 2(15)+5 " = 9 = J
c('h') = 2(7)+5 " = 19 = T
c('y') = 2(24)+5 " = 1 = B
c('c') = 2(2)+5 " = 9 = J
c('l') = 2(11)+5 " = 1 = B
c('a') = 2(0)+5 " = 5 = F
c('s') = 2(18)+5 " = 15 = P
c('s') = 2(18)+5 = 15 = P

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

mensaje c r y p t o g r a p h y c l a s s
CipherText J N B J R H R N F J T B J B F P P