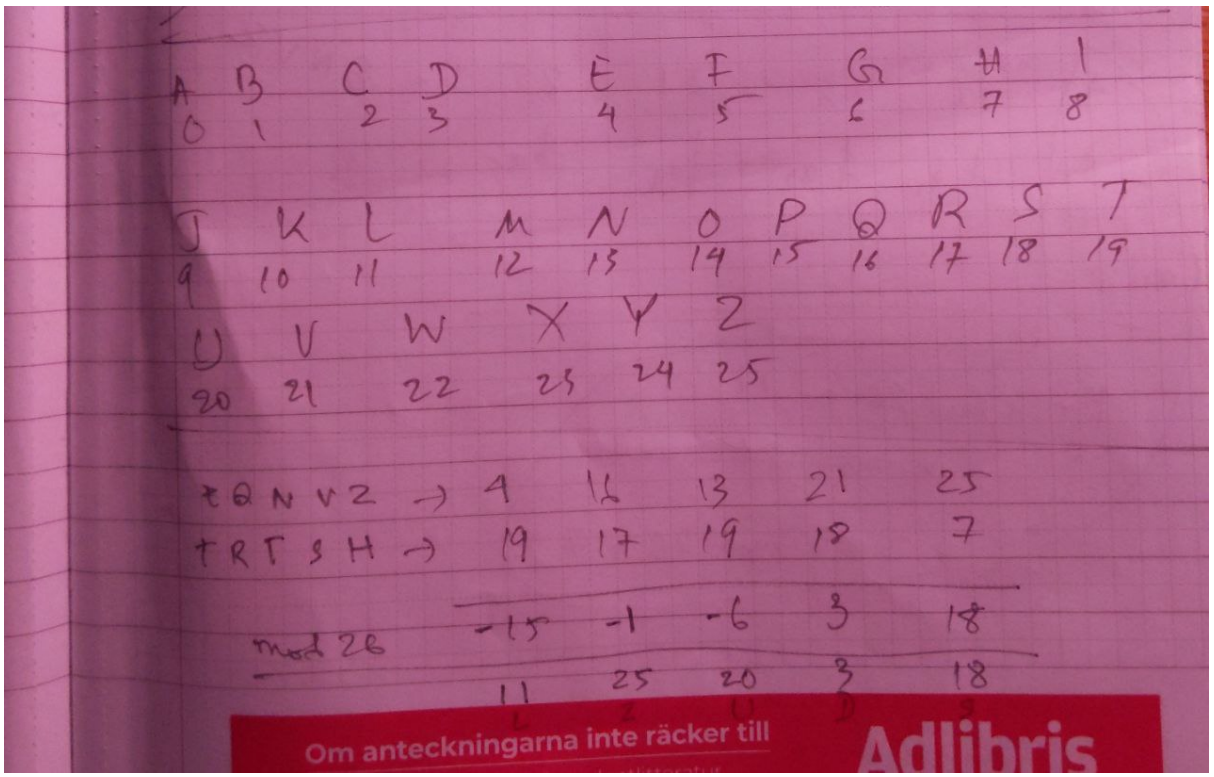
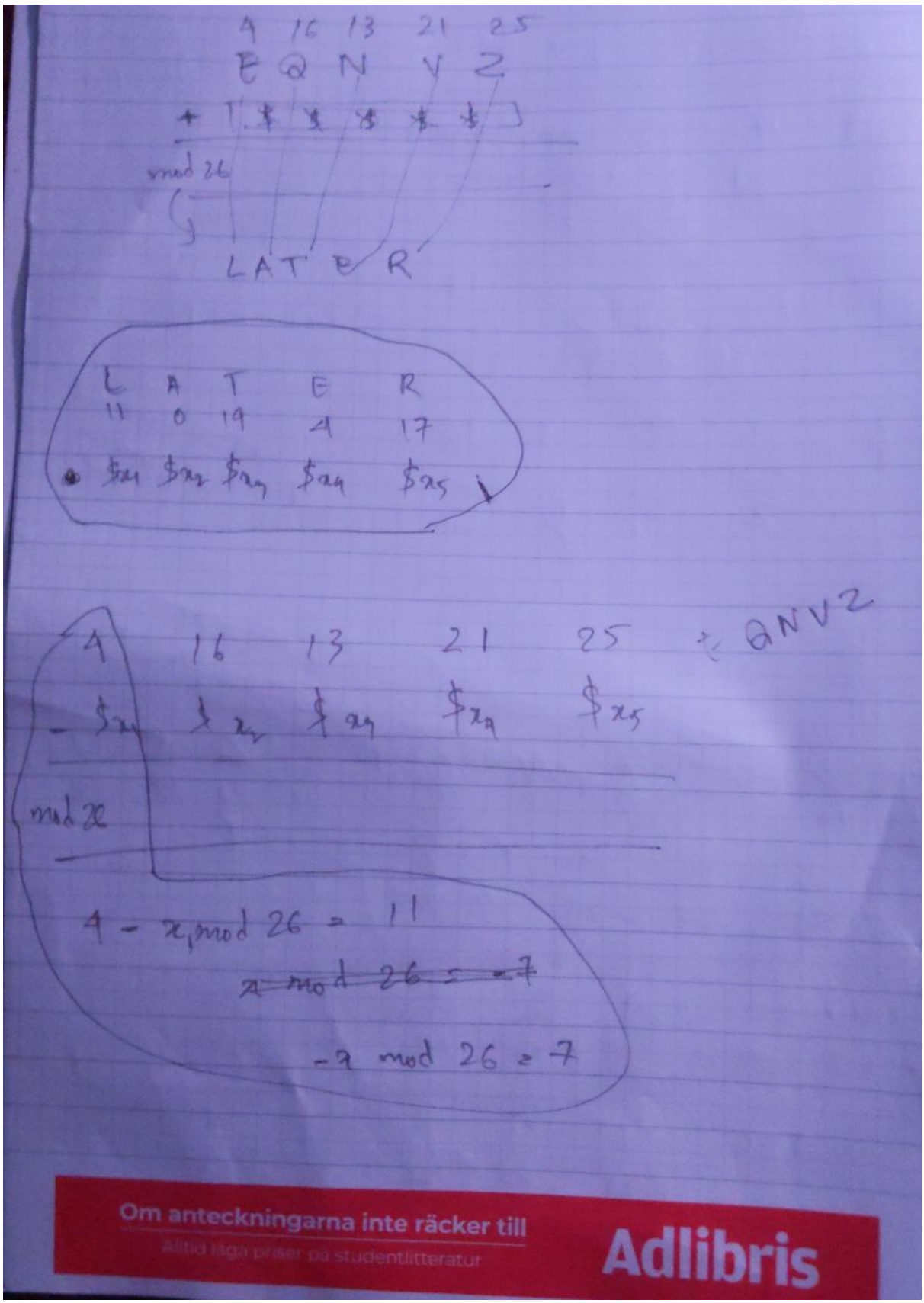

A B C D E F G H I
0 1 2 3 4 5 6 7 8
J K L M N O P Q R S T
9 10 11 12 13 14 15 16 17 18 19
U V W X Y Z
20 21 22 23 24 25
TQNVZ → 4 16 13 21 25
THISH → 19 17 19 18 7
-15 -1 -6 3 18
mod 26
11 25 20 3 18
Om anteckningarna inte räcker till
Adlibris



$(A - x_1) \bmod 26 = 11$ — eq 1

$(16 - x_2) \bmod 26 = 0$ — eq 2

$(13 - x_3) \bmod 26 = 19$ — eq 3

$(21 - x_4) \bmod 26 = 4$ — eq 4

$(25 - x_5) \bmod 26 = 17$ — eq 5

T	Q	U	R	I

is the key. We roll back from 2 to A for negative index.

~~22 16 13 21 25~~ 7 4 11 11 14

~~19~~

\+ 19 16 20 17 8

26 20 31 18 22

mod 26

0 20 5 18 22

A U F S W

Verification

$E_n = Q N V^2$

E	4	16	13	21	25
TAURI	19	16	20	17	9
	-15	0	-7	4	17

mod 26

11	0	19	4	17
L	A	T	E	R

(Q3) P = 7, Q = 11 (prime)

N = P × Q = 7 × 11 = 77

W = (P-1) × (Q-1) = (7-1) × (11-1) = 6 × 10 = 60

E = ?

"Public Exponent E : E < W ∧ E is relatively prime to W."

E = 17 chosen

D = ?

~~D = E^-1 mod 77~~

~~D = 17^-1 mod 77~~

~~D = 1/17 mod 77~~

~~17 × D mod 77 = 1~~

D = E^-1 mod W

= 17^-1 mod 60

= 53

Public Key = { N, E } = { 77, 17 }

Private key = { N, D } = { 77, 53 }

Encryption ⇒ C = M^E mod N

Decryption ⇒ D = C^D mod N.

Example message ⇒ M = 65

Encrypt ⇒ C = 65^17 mod 77 = 32

Decrypt ⇒ D = 32^53 mod 77 = 65