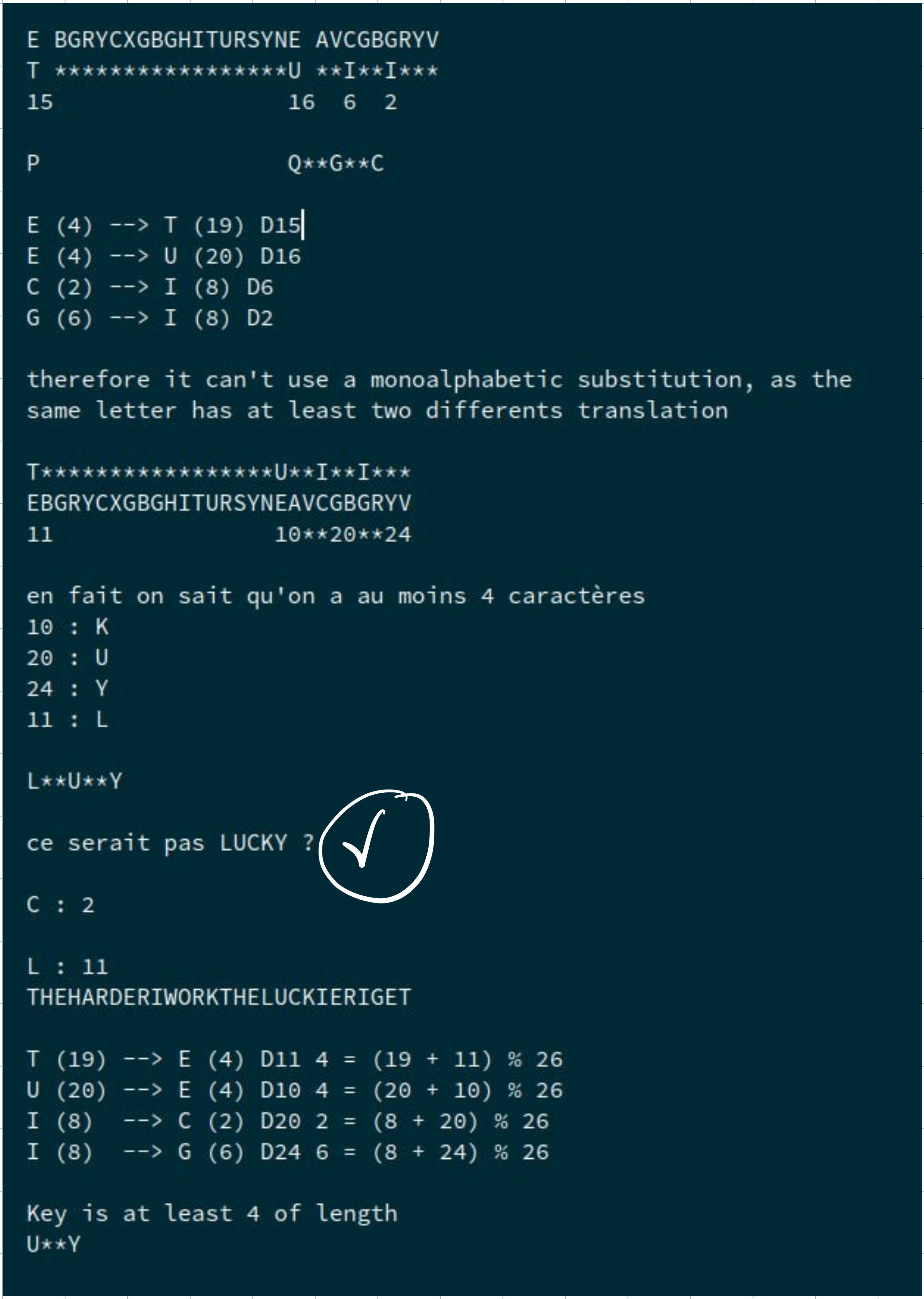

```
E BGRYCXGBGHITURSYNE AVCGBGRYV
T *****************U **I**I***
15                 16  6  2

P                  Q**G**C

E (4) --> T (19) D15
E (4) --> U (20) D16
C (2) --> I (8) D6
G (6) --> I (8) D2

therefore it can't use a monoalphabetic substitution, as the
same letter has at least two differents translation

T*****************U**I**I***
EBGRYCXGBGHITURSYNEAVCGBGRYV
11                10**20**24

en fait on sait qu'on a au moins 4 caractères
10 : K
20 : U
24 : Y
11 : L

L**U**Y

ce serait pas LUCKY ? ✓

C : 2

L : 11
THEHARDERIWORKTHELUCKIERIGET

T (19) --> E (4) D11 4 = (19 + 11) % 26
U (20) --> E (4) D10 4 = (20 + 10) % 26
I (8)  --> C (2) D20 2 = (8 + 20) % 26
I (8)  --> G (6) D24 6 = (8 + 24) % 26

Key is at least 4 of length
U**Y
```

Problem 5.2

① perfect secrecy $\Rightarrow$ $H(T) \leq H(K)$

$\Downarrow$

key and plaintext statistically independent

~~I would say yes because it's just a "mapping".~~

no -> it gives us information.

for example if the 1st and the nth plaintext are the same, we will know it is the same letter

$$\underset{\log(26^{n})}{\underset{\downarrow}{H(K)}} \geq \underset{\log(26^{2n})}{\underset{\downarrow}{H(M)}}$$

aabaab
idc idc

BUT IT CAN PROVIDE PERFECT SECRECY

it depends on the entropy of the msg

the $H(M)$ could be reduced enough so $H(k) \geq H(M)$. For example if the message is really not random. For instance:

Let M : $\begin{cases} 111111 \\ 000000 \end{cases}$

$\Rightarrow H(M) = 1$

1111111

Let $\{0,1\}$ be the alphabet of the key of length 2.

$\Rightarrow H(k) = 4$ because $\begin{cases} 1/4 & 01 \\ 1/4 & 10 \\ 1/4 & 00 \\ 1\ 4 & 11 \end{cases}$ because our key could be anything from this

② ⓐ No. It's just two mappings:

T → N

E → Z

T → N

E → Z

ⓑ Yes it does. It's like a 2n key.
It does not require a uniform
distribution ⇒ it's just a bijection

T → N

E → Z

T → W

E → X

③

k * * *   * * * *

i o l g   i e l z

so it's the same key twice we know it's gonna be a k

k * * *   k * * *

i o l g   i e l z

k * * *   k y l e

i o l g -21 i e l z

offset 21

$$(x + 21) \% 26 = 6 \rightarrow G$$

$$\Rightarrow x = 11$$

$$= l$$

kill kyle

ki ** ****

offset 22 gikd -22 iale

g: 6

k: 10

i: 8

m: 12

$(X + 22) \% 26 = 8$

$-4 + 26$

$\Rightarrow X = 12$

ki ** matt

gikd -11 iale offset 11

t: 19

e: 4

$26 - (19-4)$

$= 11$

$(Y + 11) \% 26 = 3$

d: 3

$Y = 18 \Rightarrow s$

kiss matt

ki** **** ki** ****

xwcx lzkj xwje nbsy

one is kiss, one is kill

$\Delta(l \to s)$
$= 7$

$\Delta(c \to j)$
$= 7$

kill **** kiss ****

xwcx lzkj xwje nbsy

$\Delta(m \to l) = 25$
$\Delta(k \to l) = 1$

$\Delta(a \to n) = 13$
$\Delta(k \to n) = 3$
$\Delta(m \to n) = 1$

might be interesting.

kill kyle and kiss matt?

$\Delta(t \to g) = 5$ $\Delta(e \to j) = 5$ ✓

kill kyle kiss matt