Problem 1

a.

```python
C = 'C UYGHARMZ IUWMPRWIR GAIR YVRMP MBHMZWMPUM C VMMXWPE YV PYR VCZ
F = {}
for i in range(ord('A'),ord('Z')+1):
    F[chr(i)] = 0
for letter in C:
    if letter != ' ':
        F[letter] += 1
F = dict(sorted(F.items()))
for alphabet in F.keys():
    print(f'{alphabet} : {F[alphabet]}')
```

PROBLEMS 8 OUTPUT DEBUG CONSOLE TERMINAL PORTS Code

```
A : 2
B : 2
C : 12
D : 6
E : 4
F : 0
G : 5
H : 3
I : 4
J : 0
K : 2
L : 1
M : 19
N : 5
O : 1
P : 12
Q : 2
R : 9
S : 3
T : 1
U : 6
V : 7
W : 9
X : 6
Y : 12
Z : 9
```

b.

Table 3: Ciphertext to plaintext mapping

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

c.

C = 9P + 2 (mod 30)

d.

a = 9, b = 2

e.

Key size is **26!**

Yes, it is approximately equal to 2^88.

Problem 2

a.

Φ(30) * 30 = 8 * 30 = **240**

b.

a = 1: a^(-1) = 1, since 1 * 1 ≡ 1 (mod 30)

a = 7: a^(-1) = 13, since 7 * 13 ≡ 91 ≡ 1 (mod 30)

a = 11: a^(-1) = 11, since 11 * 11 ≡ 121 ≡ 1 (mod 30)

a = 13: a^(-1) = 7, since 13 * 7 ≡ 91 ≡ 1 (mod 30)

a = 17: a^(-1) = 23, since 17 * 23 ≡ 391 ≡ 1 (mod 30)

a = 19: a^(-1) = 19, since 19 * 19 ≡ 361 ≡ 1 (mod 30)

a = 23: a^(-1) = 17, since 23 * 17 ≡ 391 ≡ 1 (mod 30)

a = 29: a^(-1) = 29, since 29 * 29 ≡ 841 ≡ 1 (mod 30)

c.

8 = 4a + b (mod 30)

26 = 10a + b (mod 30)

7 = 27a + b (mod 30)

Trial-and-error : **a = 13, b = 16**

d.

13 * 7 = 1 (mod 30)

$y = 13x + 16 \pmod{30}$

⇨ $x = (y - 16)/13 \pmod{30}$

⇨ $x = 7(y - 16) \pmod{30}$

⇨ $x = 7y - 112 \pmod{30}$

⇨ $x = 7y + 8 \pmod{30}$

c = 7, d =8