(1.) a.) $|M| = 26^9 = 5.43 \times 10^{12}$

$\lg |M| = 42.3$ ✓

b.) $(26^9)^{26^9}$ ✓ and $\lg(M \to M) =$

$9 \times 26^9 \log 26$ ✓

c.) $|M|$ is the size of the message/cipher space ✓

$|M \to M|$ is the number of all possible encryption schemes ✓

Very Good

(2.) a.)

in	1	2	3	4	5	6	7	8	9
out	4	6	1	5	3	7	9	2	8
	v	l	o	o	i	b	u	y	s

o b v i o u s l y ✓

1 2 3 4 5 6 7 8 9

b.) $|K| = 9! =$
362880 ✓

so any permutation of $\{1, \ldots 9\}$ ✓

Can be represented as 19 bits ✓
$\lceil \log_2(9!) \rceil$

c.) See if all the output letters appear exactly the same as the input but just shuffled around.

Input 'aaaaaaaaa' there is a $1/26^9$ chance that it is randomly outputted, but an 100%.

Adv - is what?

d.) Encrypt 'abcdefghi' and track where all the letters go.

(Mention how you need 3 attempts to deduce k as well)

3

a.) computers

b.) $|K| = 26! \approx 4.03 \times 10^{26}$

So 89 bits

The keyspace is the permutation of every letter of the alphabet appearing once.

c.) Input a string of 26 a's.
The real output will be 26 of the same letter. The random cipher has a much lower chance of this.

Sure

$$Adv = 1 - \frac{26}{26^{26}}$$

(Though input size is implicitly 9, but you used the right ideas)

d.) Input 'abc...xyz'. The output will show you, in order where every letter maps to.

Good ✓

(4) a.)

$D_{(k_1,k_2,k_3,k_4)}(c)$:

$m \leftarrow S_{k_4}^{-1}\left(P_{k_3}^{-1}\left(S_{k_2}^{-1}\left(P_{k_1}^{-1}(c)\right)\right)\right)$

return m

Very Good ✓

b.) It does the same thing twice, so if one can be broken then so can the other.

$$E_{k_1,k_2,k_3,k_4} = P_{k_1} \circ S_{k_2} \circ P_{k_3} \circ S_{k_1}$$

$$= P_{k_1} \circ P_{k_3} \circ S_{k_2} \circ S_{k_1}$$ ✓

Saying $\exists k_4, k_5$ st. $P_{k_4} \circ S_{k_5} = P_{k_1} \circ P_{k_3} \circ S_{k_2} \circ S_{k_1}$ is enough (due to transitivity argument)

$$= P_{k_1 \circ k_3} \circ S_{k_2 \circ k_1}$$

k_2, k_1 aren't functions!

Let $k_5 = k_1 \circ k_3$ and $k_6 = k_2 \circ k_1$ ✓

$$\therefore E_{k_5,k_6} = P_{k_5} \circ S_{k_6}$$

c.) Input a string of a's of length l. Shuffling should have to effect, and we expect that a substitution should return any character l times. If there is more than 1 letter returned then you can be sure it is random. ✓

$$Adv = 1 - \frac{26}{}$$

Very good You solved

26^l general case too!

d.) Input a string of a's of length l, because this will mean the shuffling part does nothing, and you can focus on substitution. Then input all b's to get it's substitution and repeat for all letters i.e. 26 times. This gives you k_6. ✓

Next you can work on k_5. Input 'a...z' (split this multiple times if l does not allow) (or fill the rest with any letter if $l > 26$) and use k_6 to get the shuffle and k_5 ✓

Overall this can be done in $O(52)$

Very good ✓

very good
I got this in O(27) but this is okay

(5) a.) k_g does draw from k uniformly at random shown by the line $k \leftarrow\$ \{a, \ldots, z\}^q$ ✓

To find a unique key,

$$k[i] := c[i] - m[i] \pmod{26}$$ ✓

for all i up to the length of m/c.

Interesting!

a.)

$$k_5 = k_1 \circ k_3 \quad ???$$

$$k_6 = k_2 + k_4$$

?

b) Pass as large a string as possible into the cipher. Then perform an analysis on the ciphertext to see if some letters appear more than others. If they match a known frequency chart, then you should

hopefully be able to conclude that it was produced by the encryption scheme.

Overkill but correct ✓

c.)

Vigenere is a periodic function

Use 'aaaaaaaa...' to eliminate Substitution to only get the Vigenere behaviour.