4CR3 A2

1.

a.

A secure encryption function must not be linear because linearity makes the relationship between plaintexts, ciphertexts, and keys predictable and solvable. If the equation:
$e(k, x + y) = e(k, x) + e(k, y)$
is true, then the function can be represented with a system of linear equations over the bits of plaintext/ciphertext. If an attacker is able to get access to plaintext and ciphertext pairs, they can set up a system of equations and use gaussian elimination to solve it.

Suppose Trudy, an attacker, is able to listen in and get access to some bits of plaintext and cipher text. Suppose he gets access to the plaintext/cipher text of the encryption of 2 and 3. Suppose he also wants to know the ciphertext of the encryption of 10. From $e(k, x + y) = e(k, x) + e(k, y)$, he would be able to find that $e(k,10)=e(k,2+2+3+3)=e(k,2)+e(k,2)+e(k,3)+e(k,3)$. From this, we can see he is able to calculate the encryption of 10, even without knowing what the key is.

b.

A linear s-box would ensure that for all x and y, f(x+y) = f(x) + f(y). To show this does not hold for the given s-box, we can do:
Choose:
x = 34, y = 27, therefore x+y = 61
From the s-box we can lookup the following:
f(34) = 18, f(27) = CC, f(61) = EF
18+CC = E4
Since E4 does not equal EF, this proves that the s-box given is not linear.

2.

The hash of the given message using the changed functions is:
a909986f702bf8d63dd741ff69ebb34c6ed957da7a9609322e43791edb7746b
The source code in python is attached.

3.

Yes, we can say that h is collision resistant. Suppose h_1 is collision resistant, but h_2 is not. Assume h is not collision resistant. This means that for some x_1, x_2, where $x_1 \neq x_2$, $h(x_1) = h(x_2)$. Thus, we can get $h_1(x_1) \mathbin{/\!/} h_2(x_1) = h_1(x_2) \mathbin{/\!/} h_2(x_2)$. For this to be true, the first n bits of $h(x_1)$ must equal the first n bits of $h(x_2)$. However, this would mean that $h_1(x_1) = h_1(x_2)$, meaning that h_1 is not collision resistant, which goes against the assumption, proving that h is collision resistant by contradiction.