Question 3

For a function to be a valid substitution cipher, it must have a one-to-one relationship between the plaintext alphabet and the ciphertext alphabet. This means that for every input x, there must be a unique output f(x) and for every output y, there must be a unique input x such that f(x) = y which means that the function must be invertible.

The given function f(x)=x^k(mod26) to be invertible, it must be a permutation modulo 26. A function of the form x^k(mod n) is a permutation if and only if gcd(k,ϕ(n))=1.

In this case, n = 26. Euler's totient function ϕ(26)=26(1−1/2)(1−1/13)=26(1/2)(12/13)=1×12=12.

Therefore, for f(x) = x^k (mod 26) to be a valid cipher, we must have gcd(k,12) = 1.

However, the problem states that k > 1. We can find many values of k > 1 for which gcd(k,12) does not equal to 1.

Example:

If k = 2, then gcd (2,12) = 2 and not equal to 1.

Consider the encryption of x = 1 and x = 25 using f(x) = x^k (mod 26):

F (1) = 1

F (25) = 1

Since f (1) and f (25) are two different plaintext values mapped to the same ciphertext value means that the mapping is not one-to-one and decryption would be ambiguous.

Because there exist values of k > 1 for which the condition gcd (k,12) is not met the function f(x)=x^k(mod26) cannot universally be used as a cipher for any k >1.