

quiz 01.1

(1) The ciphertext DROBKSXSXCZKSXPKVVCWKSXVIYXDROQKBKQO was encrypted with a shift cipher, from an English plaintext. Decrypt it *efficiently* without knowing the key. Show your work. Explain.

(2) Find a multiplicative inverse of 13 modulo 47 (without using the Euclidean algorithm). Show your work. Explain.

(3) How many surjective functions are there from a 8-element set to a 2-element set?

(4) How many surjective functions are there from a 8-element set to a 7-element set?