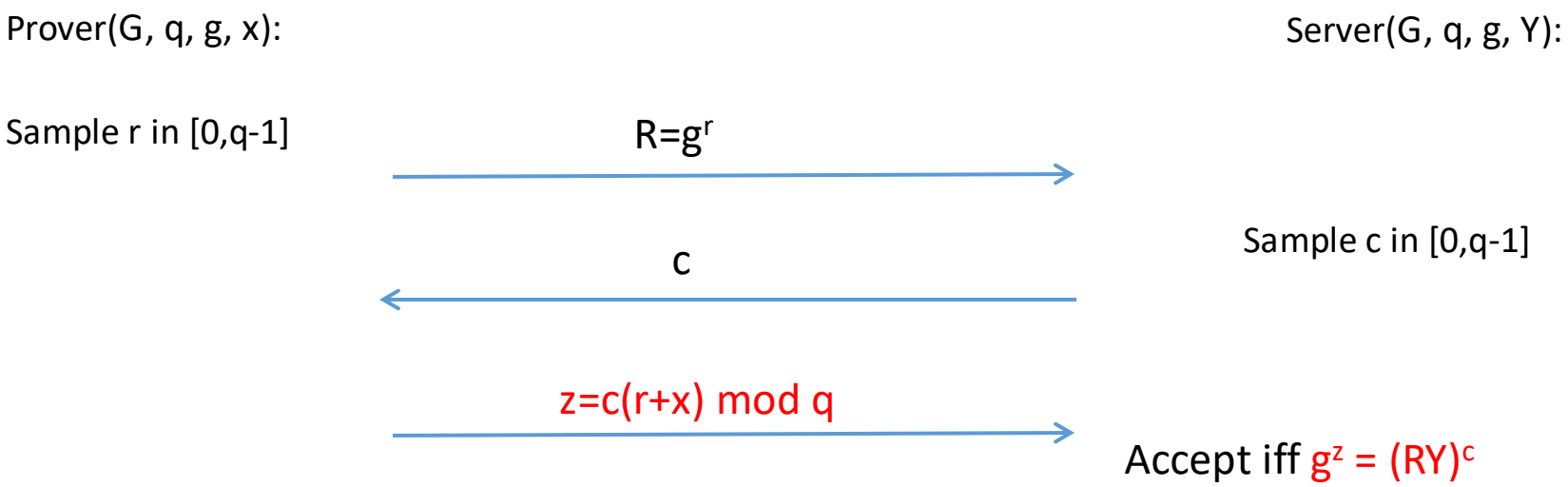
CSCI471/971
Modern Cryptography

Workshop

Question-1

Question 1. Please show that the following variant of Schnorr protocol is not secure.



Question-2

Question 2. Given a ciphertext $ct = (c_1, c_2)$ of the El Gamal encryption, please prove that you know a secret key x that can decrypt the ciphertext to 100 without leaking the secret key.

END