

CSCI471/971

Modern Cryptography

Workshop

Question-1

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

Prover(G, q, g, x):

Sample r in $[0, q-1]$

$R = g^r$

Server(G, q, g, Y):

Sample c in $[0, q-1]$

c

$z = c(r+x) \bmod q$

Accept iff $g^z = (RY)^c$

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