Πρωτόκολλα Μηδενικής Γνώσης

1. Η Μάρτζερι και η Εύα εκτελούν ένα Σ-πρωτόκολλο (δηλ. ένα πρωτόκολλο 3 κινήσεων (έστω a, c, s) με πληρότητα, ειδική εγκυρότητα και HVZK). Η Εύα είναι ο Verifier. Κατά το τέλος τη εκτέλεσης η Εύα ισχυρίζεται ότι ο υπολογιστής της λόγω διακοπής ρεύματος έσβυσε, χάνοντας τα μηνύματα c, s, οπότε ζητάει από την Μάρτζερι να συνεχίσουν την εκτέλεση από αυτό το σημείο. Έχοντας χάσει την τιμή του c, θα στείλει νέα τιμή c'. Η Μάρτζερι προτείνει, για οικονομία, να στείλει εκείνη στην Εύα την χαμένη τιμή του c μαζί με την απάντηση s. Ποιά από τις αντισυμβαλλόμενες έχει δίκιο;

2. Βασιζόμενοι στο πρωτόκολλο του Schnorr, διατυπώστε ένα Σ-πρωτόκολλο που αποδεικνύει την ισότητα δύο διακριτών λογαρίθμων (δηλ. ο λογάριθμός του h_1 ως προς το g_1 είναι ίδιος με το λογάριθμο του h_2 ως προς το g_2). Επιβεβαιώστε ότι είναι πλήρες, ειδικά έγκυρο και HVZK.

3. Αξιολογήστε την εγκυρότητα (όχι την ειδική εγκυρότητα) του παραπάνω πρωτοκόλου σε σχέση με αυτό του Schnorr.

4. Εξηγήστε πως μπορούμε να δείξουμε ότι ένα κρυπτογραφημένο μήνυμα $c = \langle u, v \rangle$ με ElGamal περιέχει ως μήνυμα είτε την τιμή m_1 είτε την τιμή m_2, χωρίς να δώσουμε άλλη πληροφορία για αυτό.