שאלה 6

הסטודנט הזדוני יכול לחשב את הסוד המשותף של יעל ומיכל. נוכיח זאת באופן מתמטי: יהיו p, g מספרים שלמים ידועים לכל, $p > 3$ ראשוני, a, b מספרים שלמים זרים לp סודיים, ו $x \equiv g^a \pmod p$, $y \equiv g^b \pmod p$. אם ידוע a′ כך ש $x \equiv g^{a'}$ אזי

$$y^{a'} \equiv (g^b)^{a'} \equiv g^{ba'} \equiv (g^{a'})^b \equiv x^b \equiv (g^a)^b \equiv g^{ab} \equiv key$$

שאלה 6

הסטודנט הזדוני יכול לחשב את הסוד המשותף yek של יעל ומיכל. נוכיח זאת באופן מתמטי: יהיו g, p מספרים שלמים ידועים לכל, p < 3 ראשוני. יהיו a, b מספרים שלמיים זרים ל p סודיים. יהיו $x = g^a$ $y = g^b$