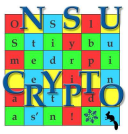

Problem 7. «Protocol»

Alena and Boris developed a new protocol for establishing session keys. It consists of the following three steps:

1. The system has a common prime modulus p and a generator g. Alena and Boris have their own private keys $\alpha_a \in \mathbb{Z}_{p-1}$, $\alpha_b \in \mathbb{Z}_{p-1}$ and corresponding public keys $P_a = g^{\alpha_a} \mod p$, $P_b = g^{\alpha_b} \mod p$.

2. To establish a session key Alena generates a random number $R_a \in \mathbb{Z}_{p-1}$, computes $X_a = (\alpha_a + R_a) \mod (p-1)$ and sends it to Boris. Then Boris generates his random number R_b, computes X_b in the same way as Alena and sends it back to her.

3. Alena computes the session key in the following way:

$$K_{a,b} = (g^{X_b} P_b^{-1})^{R_a} \mod p.$$

Bob computes the session key in the following way:

$$K_{b,a} = (g^{X_a} P_a^{-1})^{R_b} \mod p.$$

How can an attacker Evgeniy compute any future session key between Alena and Boris, if he steals the only one session key $K_{a,b}$?