Во время экспедиции до Сатурна вы будучи стажёром осваивали искусство космической навигации. У Михаила Антоновича – штурмана вашего корабля – уже рассчитан оптимальный маршрут, однако, он предлагает вам в качестве эксперимента использовать передовые методы практической криптографии и разработать новый маршрут, экономящий время и топливо.

Для начала вам нужно взять координаты точки прибытия – p и g (которое является образующим Zp). Затем каждый из вас использует свой идентификатор штурмана s1 и s2, являющиеся секретными ключами. На их основе вычисляются публичные ключи P1 и P2, которые вы вводите в навигационную систему для обмена:

* p = 102639592829741105772054196573991675900716567808038066803341933521790711307779
* g = 881
* P1 = g^s1 mod p
* P2 = g^s2 mod p

Теперь можно вычислить общий сессионный ключ. Для этого каждый из вас вычисляет *K = (g^X2 x P2^(-1))^R1 = (g^X1 x P1^(-1))^R2 mod p*, где

* R1, R2 – случайные числа из Zp-1, каждое из которых придумал член экипажа корабля
* X1 = (s1 + R1) mod (p-1)
* X2 = (s2 + R2) mod (p-1)

Сначала нужно проверить, что алгоритм работает. Для этого штурман предлагает зашифровать алгоритмом Виженера строку

* QWERTYUIOPASDFGHJKLZXCVBNMQWERTY

Вы вычислили свой публичный ключ P1, а штурман – P2:

* P1 = 56516939772931532635821653285644762495821877143130216404232117392978752267440
* P2 = 97805886540812976681425218438541565755807341852031368458611507727375441753270

Далее вы вычислили X1 и X2 и обменялись ими друг с другом:

* X1 = 38652903422450522699181012123230466356001155830352761873656490473686663026009
* X2 = 94752378781834466021883678445138712135909263389447354158934466425794157606855

Затем вы оба вычислили сессионный ключ K1. Вы вводите ключ в систему, чтобы убедиться, что вычисления прошли успешно, и система ответила, что ваши со штурманом ключи K1 совпали:

* K1 = 51577879999867728749865484874891374681132914277503819280420235433541037082619

Совпадение ключей означает, что можно зашифровать текстовую строку:

* открытый текст – QWERTYUIOPASDFGHJKLZXCVBNM
* закрытый текст – dfpecabpvixkrqpzr|xc`ucvvy

Теперь вы предлагаете использовать этот алгоритм для того, чтобы скрыть детали нового маршрута от посторонних людей. Параметры p, g, P1, P2 остались прежними. Вы со штурманом вычисляете новый сессионный ключ K2, для чего обменялись новыми X1 и X2:

* X1 = 26236964196109648184170800614822825706897303057186535363544243002207382749227
* X2 = 79975543150098709358818415763653860357853475638600240610978761443689835260179

Вычислив новый общий сессионный ключ K2, вы передаёте штурману параметры новой траектории полёта.

Какая информация о новом маршрута скрыта?