Система дистанционного обучения eLearn-2023 предполагает установление защищенного соединения между студентами и преподавателем с помощью криптографического протокола аутентифицированной выработки общего ключа, описанного ниже. По замыслу разработчиков системы, данный протокол позволяет преподавателю аутентифицировать студента, с которым происходит взаимодействие (для выдачи заданий и оценки результатов).

Пусть в системе зарегистрированы студенты Иванов, Петров, Сидоров и преподаватель (будем называть их участниками системы). Каждый участник обладает идентификатором и ключевой парой для схемы подписи RSA.

Обозначим соответствующее множество идентификаторов участников через $Users = \{\mathsf{I}, \mathsf{P}, \mathsf{S}, \mathsf{T}\}$, ключевую пару участника $\mathsf{A} \in Users$ — через (sk_A, pk_A). Соответствие открытых ключей участников и их идентификаторов заранее известно всем участникам системы.

Описание протокола. Пусть $\langle g \rangle$ — циклическая группа порядка q, $\mathbb{Z}_q^*$ — мультипликативная группа конечного поля $\mathbb{Z}_q$. Обозначим через $x \xleftarrow{\mathcal{U}} X$ случайный равновероятный выбор значения x из множества X, через $\perp$ — символ ошибки, через $\|$ — символ конкатенации, через Sign и Verify — алгоритмы формирования подписи (принимает ключ подписи и сообщение и возвращает значение подписи) и проверки подписи (принимает ключ проверки подписи, сообщение и значение подписи, возвращает 1(0), если подпись (не)корректная), определяемые схемой подписи RSA.

Протокол аутентифицированной выработки общего ключа между участниками $\mathsf{A}, \mathsf{B} \in Users$ определяется следующим образом.

A		B
$e_A \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$		
$r_A \leftarrow g^{e_A}$	$\xrightarrow{r_A}$	
		$e_B \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$
		$r_B \leftarrow g^{e_B}$
		$K \leftarrow r_A^{e_B}$
		$\sigma_B \leftarrow \mathsf{Sign}(sk_B, (r_B \parallel r_A \parallel K))$
	$\xleftarrow{\mathsf{B}, r_B, \sigma_B}$	
$K \leftarrow r_B^{e_A}$		
if $\mathsf{Verify}(pk_B, (r_B \parallel r_A \parallel K), \sigma_B) \neq 1$:		
return $\perp$		
$\sigma_A \leftarrow \mathsf{Sign}(sk_A, (r_A \parallel r_B \parallel K))$		
	$\xrightarrow{\mathsf{A}, \sigma_A}$	
		if $\mathsf{Verify}(pk_A, (r_A \parallel r_B \parallel K), \sigma_A) \neq 1$:
		return $\perp$
return K		**return** K

Задание. Опишите атаку на протокол, позволяющую выставить студенту Иванову оценку, которую заслужил студент Петров.