ИБ 10 _____

Бланк ответа на кейс-задание
(5 баллов)

Используйте для записи только отведённое для каждого вопроса место.
Не пишите на бланке свое имя, фамилию или другие сведения, которые могут указывать на авторство работы.
Никаких пометок в бланке ответов быть не должно!

Для совместной выработки общего секрета при обмене сообщениями только по общедоступному (незащищенному) каналу связи, два абонента могут воспользоваться протоколом Диффи-Хеллмана.

Для получения общего секрета абонентам нужно:

1) Выбрать простое число P и взаимно простое с ним меньшее число T.
2) Независимо выбрать произвольное число a и найти остаток от деления T^a на P (то есть найти T^a «по модулю P», записывается «mod P»).
3) Обменяться по общедоступному каналу связи полученными значениями $T^a \bmod P$.
4) Независимо возвести полученные значения в выбранные степени: $(T^{a2})^{a1} \bmod P$ (для второго абонента, соответственно, $(T^{a1})^{a2} \bmod P$).
5) Получившийся у обоих абонентов результат совпадет и будет общим секретом, который далее может использоваться в других криптографических алгоритмах.

Пусть P = 13 и T = 6.

А) Выберите число a и вычислите значение для передачи другому абоненту. (1 балл).

_____

_____

_____

_____

Б) От другого абонента Вами получено число 7. Вычислите общий секрет. (2 балла)

_____

_____

_____

_____

_____

_____

_____

В) Во время выработки еще одного общего секрета с теми же открытыми параметрами Вами получено от другого абонента число 5. Известно, что в канале может действовать нарушитель, способный перехватывать отправляемые абонентами сообщения и подменять их своими (то есть реализовывать атаку «человек посередине»). Другой абонент при выборе произвольных значений обычно пользуется кубиком с 8 гранями. Проверьте, получено ли данное число от Вашего абонента или от нарушителя. Приведите аргументы в пользу предлагаемого ответа, а также все проделанные вычисления. (2 балла)

_____

_____

_____

_____

_____

_____

ИБ 10 _____

_____

_____

_____

_____