ИБ 11 _____

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!

В асимметричной схеме шифрования RSA, используемой в качестве электронной подписи, каждый абонент имеет ключевую пару, в которую входит секретный ключ, используемый для подписывания сообщений, и открытый ключ – для проверки подписей. При этом любой желающий может проверить подпись, используя открытый ключ адресата, а для корректной выработки подписи потребуется знание секретного ключа, который, согласно схеме, известен лишь одному лицу.

Для обеспечения такой системы используются следующие математические операции.

1) Желающий сформировать ключевую пару абонент выбирает два простых числа – p и q. Далее вычисляется их произведение N = p*q.
2) Для полученного произведения вычисляется значения функции Эйлера, $\varphi(n) = (p - 1)(q - 1)$.
3) Выбирается натуральное число e, большее 1 и меньшее $\varphi(n)$, не имеющее общих делителей (взаимно простое) с $\varphi(n)$.
4) Отправитель для выработки подписи сообщения m должен вычислить остаток от деления числа m^d на n (или найти m^d по модулю n, записывается (mod n)), где d – секретная степень, вычисленная так, чтобы выполнялось условие: $d * e \equiv 1 \pmod{\varphi(n)}$, то есть произведение e и d равнялось 1 по модулю значения $\varphi(n)$. Число d вместе с исходными p и q хранится в секрете и составляет секретный ключ.
5) Получатель для проверки подписи сообщения m, являющегося целым числом от 1 до n, должен возвести его подписанное значение m^d в степень e также по модулю n. Пара (e, n) составляет открытый ключ, служащий для проверки подписи.

Пусть p = 13 и q = 23.

А) Создайте открытый ключ по описанному выше алгоритму. (1 балл)

_____

_____

_____

_____

Б) Вычислите секретное значение d. (2,5 балла)

_____

_____

_____

_____

_____

_____

_____

В) Подпишите сообщение m = 17 при помощи полученной ключевой пары. Проверьте получившуюся подпись, отразите ход подписи и проверки. (1,5 балла)

_____

_____

_____

ИБ 11 _____

_____

_____

_____

_____

_____