ИБ 9 _____

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 каждый абонент имеет ключевую пару, в которую входит открытый ключ, используемый для зашифрования сообщений, и секретный ключ – для расшифрования. При этом любой желающий может зашифровать сообщение, используя открытый ключ адресата, а для прочтения сообщения 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, φ(n) = (p – 1)(q – 1).
3) Выбирается натуральное число e, большее 1 и меньшее φ(n), не имеющее общих делителей (взаимно простое) с φ(n). Это число e вместе с N составляет открытый ключ. Для зашифрования сообщения m, являющегося целым числом от 1 до n, отправителю требуется вычислить остаток от деления числа m^e на n (или найти m^e по модулю n, записывается (mod n)).
4) Получатель для прочтения этого сообщения должен возвести полученное сообщение m^e в степень d также по модулю n, значение которой является секретным ключом. Ее значение должно быть таким, чтобы выполнялось условие: d * e ≡ 1 (mod φ(n)), то есть произведение e и d равнялось 1 по модулю значения φ(n). Число d вместе с исходными p и q хранится в секрете и составляет секретный ключ.

Пусть p = 7 и q = 11.

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

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

В) Зашифруйте сообщение m = 19 для другого абонента, чей открытый ключ: (e, n) = (11; 143). Укажите исходное сообщение (натуральное число), зашифрованное сообщене и отразите ход зашифрования. (1,5 балла)

_____

_____

_____

_____

_____