Московский физико-технический институт(национальный исследовательский университет)		
Кафедра радиотехники и систем управления		
Контрольная работа: Защита информации	11 ноября 2023 года	Билет № 16
Ф.И.О.	Гр.№	Сем.

0. Укажите в заголовке билета свои данные (фамилию, имя, отчество, группу, фамилию семинариста). Отсутствие указанных данных равносильно отсутствию работы. Работа должна быть выполнена чистым и аккуратным подчерком. В конце решения каждой задачи должны быть отдельно выписаны ответы.

1. Проверить, являются ли числа 52, 68, 73 свидетелями простоты числа 185 по Миллеру. p = 185. Степени, в которые нужно возводить: 23, 46, 92, 184
   Для числа 52 получаются 13, 169, 71, 46. То есть 52 не является свидетелем простоты по Миллеру, так как последовательность не заканчивается 1.
   Для числа 68 получаются 117, 184, 1, 1. То есть 68 является свидетелем простоты по Миллеру, так как последовательность содержит -1, после чего идут только 1.
   Для числа 73 получаются 147, 149, 1, 1. То есть 73 не является свидетелем простоты по Миллеру, так как последовательность содержит элемент, неравный -1, после чего идёт 1, т.е. в группе есть делители ноля.

2. Зашифровать сообщение по схеме RSA. Открытый ключ: n = 77; e = 23. Сообщение: m = 53. Результат шифрования: $c = m^e mod n, c = 53^{23} mod 77, c = 58$

3. Подписать сообщение по схеме RSA. Закрытый ключ: n = 77; d = 53. Сообщение: m = 18. $s = m^d mod n = 18^{53} mod 77 = 2$

4. Расшифровать сообщение по схеме RSA. Открытый ключ: n = 55; e = 13. Зашифрованное сообщение: c = 29. В ответе привести все промежуточные результаты вычислений. $p = 7, q = 11, d = 37, m = 39$

5. Зашифровать сообщение по схеме Эль-Гамаля. Открытый ключ: p = 13; g = 6; y = 8. Секретный ключ: x = 3. Сообщение: M = 4. Использовать следующий случайный параметр для шифрования: k = 11. $a = 11, b = 7$

6. Вычислить подпись по схеме Эль-Гамаля. Открытый ключ: p = 11; g = 7; y = 5. Секретный ключ: x = 2. Сообщение: M = 9. Использовать следующий случайный параметр для создания подписи: k = 3. $a = 2, b = 5$

7. Для точки A (1; 7) принадлежащей группе точек эллиптической кривой $y^2 = x^3 - 2x - 5$ над конечным полем F_{11} найти координаты точек B = 2 × A = A + A и $C = 3 \cdot A = A + A + A$. Точка A: (1; 7)
   Точка B: (3; 7)
   Точка C: (7; 4)

8. Для кривой $eu^2 + v^2 = 1 + du^2v^2 \ mod \ p$ где $P = 23, d = 11$ Расчитать точки кривой при $e = 3$ Ответ: (0,1) (0,22), (2,2), (2,21), (3,9), (3,14), (5,3), (5,20), (7,11), (7,12), (9,8), (9,15), (10, 0), (11, 6), (11,17), (12,6), (12,17), (13,0), (14,8), (14,15), (16,11), (16,12), (18,3), (18,20), (20,9),(20,14), (21,2) (21,21)