

Московский физико-технический институт (национальный исследовательский университет)		
Кафедра радиотехники и систем управления		
Контрольная работа: Защита информации	11 ноября 2023 года	Билет № 145
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 подчеркиком. В конце решения каждой задачи должны быть отдельно выписаны ответы.
1. Проверить, являются ли числа 49, 80, 438 свидетелями простоты числа 481 по Миллеру. $p = 481$. Степени, в которые нужно возводить: 15, 30, 60, 120, 240, 480
Для числа 49 получаются 454, 248, 417, 248, 417, 248. То есть 49 не является свидетелем простоты по Миллеру, так как последовательность не заканчивается 1.
Для числа 80 получаются 216, 480, 1, 1, 1, 1. То есть 80 является свидетелем простоты по Миллеру, так как последовательность содержит -1, после чего идут только 1.
Для числа 438 получаются 339, 443, 1, 1, 1, 1. То есть 438 не является свидетелем простоты по Миллеру, так как последовательность содержит элемент, неравный -1, после чего идёт 1, т.е. в группе есть делители нуля.
2. Зашифровать сообщение по схеме RSA. Открытый ключ: $p = 55$; $e = 27$. Сообщение: $m = 43$.
 $c = m^e \bmod n, c = 43^{27} \bmod 55, c = 32$
3. Подписать сообщение по схеме RSA. Закрытый ключ: $p = 55$; $d = 7$. Сообщение: $m = 16$. $s = m^d \bmod n = 16^7 \bmod 55 = 36$
4. Расшифровать сообщение по схеме RSA. Открытый ключ: $p = 55$; $e = 3$. Зашифрованное сообщение: $c = 4$. В ответе привести все промежуточные результаты вычислений. $p = 5, q = 11, d = 27, m = 49$
5. Зашифровать сообщение по схеме Эль-Гамала. Открытый ключ: $p = 13$; $g = 2$; $y = 6$. Секретный ключ: $x = 5$. Сообщение: $M = 7$. Использовать следующий случайный параметр для шифрования: $k = 11$. $a = 7, b = 12$
6. Вычислить подпись по схеме Эль-Гамала. 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 $A(1; 4)$ принадлежащей группе точек эллиптической кривой $y^2 = x^3 - 2x - 5$ над конечным полем F_{11} найти координаты точек $B = 2 \cdot A = A + A$ и $C = 3 \cdot A = A + A + A$. Точка $A: (1; 4)$
Точка $B: (3; 4)$
Точка $C: (7; 7)$
8. Для кривой $eu^2 + v^2 = 1 + du^2v^2 \bmod p$ 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)