

Московский физико-технический институт(национальный исследовательский университет)		
Кафедра радиотехники и систем управления		
Контрольная работа: Защита информации	11 ноября 2023 года	Билет № 131
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 157, 212, 257 свидетелями простоты числа 425 по Миллеру. $p = 425$. Степени, в которые нужно возводить: 53, 106, 212, 424
 Для числа 157 получаются 157, 424, 1, 1. То есть 157 является свидетелем простоты по Миллеру, так как последовательность содержит -1, после чего идут только 1.
 Для числа 212 получаются 247, 234, 356, 86. То есть 212 не является свидетелем простоты по Миллеру, так как последовательность не заканчивается 1.
 Для числа 257 получаются 32, 174, 101, 1. То есть 257 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: $n = 55$; $e = 7$. Сообщение: $m = 38$.
 $c = m^e \bmod n, c = 38^7 \bmod 55, c = 47$
3. Подписать сообщение по схеме RSA. Закрытый ключ: $n = 77$; $d = 53$. Сообщение: $m = 18$. $s = m^d \bmod n = 18^{53} \bmod 77 = 2$
4. Расшифровать сообщение по схеме RSA. Открытый ключ: $n = 77$; $e = 47$. Зашифрованное сообщение: $c = 18$. В ответе привести все промежуточные результаты вычислений. $p = 7, q = 11, d = 23, m = 2$
5. Зашифровать сообщение по схеме Эль-Гамала. Открытый ключ: $p = 11$; $g = 8$; $y = 9$. Секретный ключ: $x = 2$. Сообщение: $M = 5$. Использовать следующий случайный параметр для шифрования: $k = 3. a = 6, b = 4$
6. Вычислить подпись по схеме Эль-Гамала. Открытый ключ: $p = 13$; $g = 6$; $y = 10$. Секретный ключ: $x = 2$. Сообщение: $M = 3$. Использовать следующий случайный параметр для создания подписи: $k = 5. a = 2, b = 7$
7. Для точки $A(9; 10)$ принадлежащей группе точек эллиптической кривой $y^2 = x^3 - 8x - 7$ над конечным полем F_{11} найти координаты точек $B = 2 \times A = A + A$ и $C = 3 \cdot A = A + A + A$. Точка $A: (9; 10)$
 Точка $B: (8; 10)$
 Точка $C: (5; 1)$
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)