

Московский физико-технический институт (национальный исследовательский университет)		
Кафедра радиотехники и систем управления		
Контрольная работа: Защита информации	11 ноября 2023 года	Билет № 31
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 108, 233, 307 свидетелями простоты числа 377 по Миллеру. $p = 377$. Степени, в которые нужно возводить: 47, 94, 188, 376 Для числа 108 получаются 114, 178, 16, 256. То есть 108 не является свидетелем простоты по Миллеру, так как последовательность не заканчивается 1.
Для числа 233 получаются 233, 1, 1, 1. То есть 233 не является свидетелем простоты по Миллеру, так как последовательность содержит элемент, неравный -1, после чего идёт 1, т.е. в группе есть делители нуля.
Для числа 307 получаются 70, 376, 1, 1. То есть 307 является свидетелем простоты по Миллеру, так как последовательность содержит -1, после чего идут только 1.
2. Зашифровать сообщение по схеме RSA. Открытый ключ: $n = 55$; $e = 13$. Сообщение: $m = 3$. $c = m^e \bmod n, c = 3^{13} \bmod 55, c = 38$
3. Подписать сообщение по схеме RSA. Закрытый ключ: $n = 55$; $d = 27$. Сообщение: $m = 18$. $s = m^d \bmod n = 18^{27} \bmod 55 = 17$
4. Расшифровать сообщение по схеме RSA. Открытый ключ: $n = 55$; $e = 3$. 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: $p = 11$; $g = 8$; $y = 3$. Секретный ключ: $x = 6$. Сообщение: $M = 4$. Использовать следующий случайный параметр для создания подписи: $k = 7$. $a = 2, b = 6$
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 $B = 2 \times A = A + A$ и $C = 3 \cdot A = A + A + A$. Точка $A: (1; 7)$
Точка $B: (3; 7)$
Точка $C: (7; 4)$
8. Для кривой $eu^2 + v^2 = 1 + du^2v^2 \bmod p$ где $P = 23, d = 21$ Расчитать точки кривой при $e = 8$
Ответ: (0,1), (0,22), (1,6), (1,17), (3,9), (3,14), (4,10), (4,13), (6,7), (6,16), (7,0), (16,0), (17, 7), (17,16), (19,10), (19,10) (19,13), (20, 9), (20,14), (22,6), (22,17)