

|                                                                                     |                     |            |
|-------------------------------------------------------------------------------------|---------------------|------------|
| Московский физико-технический институт (национальный исследовательский университет) |                     |            |
| Кафедра радиотехники и систем управления                                            |                     |            |
| Контрольная работа: Защита информации                                               | 11 ноября 2023 года | Билет № 80 |
| 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 133, 227, 243 свидетелями простоты числа 305 по Миллеру.  $p = 305$ . Степени, в которые нужно возводить: 19, 38, 76, 152, 304  
 Для числа 133 получаются 172, 304, 1, 1, 1. То есть 133 является свидетелем простоты по Миллеру, так как последовательность содержит -1, после чего идут только 1.  
 Для числа 227 получаются 193, 39, 301, 16, 256. То есть 227 не является свидетелем простоты по Миллеру, так как последовательность не заканчивается 1.  
 Для числа 243 получаются 182, 184, 1, 1, 1. То есть 243 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:  $n = 77$ ;  $e = 23$ . Сообщение:  $m = 53$   
 $c = m^e \bmod n, c = 53^{23} \bmod 77, c = 58$
3. Подписать сообщение по схеме RSA. Закрытый ключ:  $n = 77$ ;  $d = 47$ . Сообщение:  $m = 42$ .  $s = m^d \bmod n = 42^{47} \bmod 77 = 70$
4. Расшифровать сообщение по схеме RSA. Открытый ключ:  $n = 77$ ;  $e = 47$ . Зашифрованное сообщение:  $c = 53$ . В ответе привести все промежуточные результаты вычислений.  $p = 7, q = 11, d = 53, m = 28$
5. Зашифровать сообщение по схеме Эль-Гамала. Открытый ключ:  $p = 13$ ;  $g = 7$ ;  $y = 8$ . Секретный ключ:  $x = 9$ . Сообщение:  $M = 10$ . Использовать следующий случайный параметр для шифрования:  $k = 11$ .  $a = 2, b = 11$
6. Вычислить подпись по схеме Эль-Гамала. Открытый ключ:  $p = 13$ ;  $g = 2$ ;  $y = 12$ . Секретный ключ:  $x = 6$ . Сообщение:  $M = 8$ . Использовать следующий случайный параметр для создания подписи:  $k = 7$ .  $a = 11, b = 2$
7. Для точки  $A (0; 7)$  принадлежащей группе точек эллиптической кривой  $y^2 = x^3 - 3x - 6$  над конечным полем  $F_{11}$  найти координаты точек  $B = 2 \times A = A + A$  и  $C = 3 \cdot A = A + A + A$ . Точка  $A: (0; 7)$   
 Точка  $B: (1; 5)$   
 Точка  $C: (3; 10)$
8. Для кривой  $eu^2 + v^2 = 1 + du^2v^2 \bmod p$  где  $P = 11, d = 2$  рассчитать точки кривой при  $e = 2$  Ответ:  $(0,1), (0, 10), (1,1), (1, 10), (2,1), (2,10), (3,1), (3,10), (4,1), (4,10), (5,1), (5,10), (6,1), (6,10), (7,1), (7,10), (8,1), (8,10), (9,1), (9, 10), (10, 1), (10, 10)$ .