

Московский физико-технический институт(национальный исследовательский университет)		
Кафедра радиотехники и систем управления		
Контрольная работа: Защита информации	11 ноября 2023 года	Билет № 38
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 312, 313, 394 свидетелями простоты числа 505 по Миллеру.  $p = 505$ . Степени, в которые нужно возводить: 63, 126, 252, 504  
 Для числа 312 получаются 333, 294, 81, 501. То есть 312 не является свидетелем простоты по Миллеру, так как последовательность не заканчивается 1.  
 Для числа 313 получаются 192, 504, 1, 1. То есть 313 является свидетелем простоты по Миллеру, так как последовательность содержит -1, после чего идут только 1.  
 Для числа 394 получаются 414, 201, 1, 1. То есть 394 не является свидетелем простоты по Миллеру, так как последовательность содержит элемент, неравный -1, после чего идёт 1, т.е. в группе есть делители поля.
2. Зашифровать сообщение по схеме RSA. Открытый ключ:  $p = 77$ ;  $e = 23$ . Сообщение:  $m = 53$ . Результат шифрования:  $c = m^e \bmod n, c = 53^{23} \bmod 77, c = 58$
3. Подписать сообщение по схеме RSA. Закрытый ключ:  $p = 55$ ;  $d = 27$ . Сообщение:  $m = 18$ .  $s = m^d \bmod n = 18^{27} \bmod 55 = 17$
4. Расшифровать сообщение по схеме RSA. Открытый ключ:  $p = 77$ ;  $e = 47$ . 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:  $p = 13$ ;  $g = 6$ ;  $y = 3$ . Секретный ключ:  $x = 8$ . Сообщение:  $M = 5$ . Использовать следующий случайный параметр для шифрования:  $k = 7$ .  $a = 7, b = 2$
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  $P = 11, d = 2$  рассчитать точки кривой при  $e = 2$  Ответ:  $(0,1), (0, 10), (1,1), (1, 10), (2,1), (2,10), (3,1), (3,10), (4,1), (4,10), (5,1), (5,10), (6,1), (6,10), (7,1), (7,10), (8,1), (8,10), (9,1), (9, 10), (10, 1), (10, 10)$ .