**Вопросы к экзамену по курсу**

**«Теоретико-числовые методы в криптографии»**

1. Свойства функций оценки сложности

2. Сложность арифметических операций с целыми числами

3. Сложность алгоритма Евклида

4. Сложность операций в кольце вычетов

5. Использование модульной арифметики

6. Вычисления с многочленами

7. Дискретное преобразование Фурье

8. Непрерывные дроби и их свойства

9. Квадратичные вычеты

10. Теорема Чебышева о распределении простых чисел

11. Решето Эратосфена

12. Критерий Вильсона

13. Тест на основе малой теоремы Ферма

14. Свойства чисел Кармайкла

15. Тест Соловея-Штрассена

16. Тест Рабина-Миллера

17. Полиномиальный тест распознавания простоты

18. Критерий Люка

19. Теорема Поклингтона

20. Теорема Диемитко

21. Метод Маурера

22. Метод Михалеску

23. (*n*+1)-методы

24. Числа Мерсенна

25. Метод Полларда

26. Алгоритм Полларда-Штрассена

27. Факторизация Ферма

28. Алгоритм Диксона

29. Алгоритм Брилхарта-Моррисона

30. (*p*-1)-метод факторизации Полларда