Вопросы к зачету
по дисциплине «криптографические методы защиты информации»
для специальности «Компьютерная безопасность»
составил: д.ф-м.н., профессор Рацеев Сергей Михайлович

9-й семестр

Примерный перечень вопросов к экзамену

Математические модели открытого текста

1. Детерминированная модель открытого текста.
2. Вероятностные модели открытого текста: модель независимых символов алфавита, модель независимых биграмм, модель марковски зависимых букв.

Шифры замены и перестановки

3. Одноалфавитные шифры замены: шифр простой замены, шифр сдвига. Методы взлома данных шифров.
4. Одноалфавитные шифры замены: аффинный шифр, преобразование биграмм аффинным шифром. Методы взлома данных шифров.
5. Многоалфавитные шифры замены. Шифр Виженера. Криптоанализ шифра Виженера.
6. Многоалфавитные шифры замены: многопетлевые подстановки, аффинный блочный шифр, шифр Холла. Криптоанализ аффинного блочного шифра.
7. Многоалфавитные шифры замены: табличное гаммирование, модульное гаммирование. Шифр Вернама.
8. Многоалфавитные шифры замены. Шифр пропорциональной замены (шифр омофонов).

Математическая модель шифра

9. Алгебраическая и вероятностная модели шифров.
10. Математическая модель некоторых шифров: шифр простой замены, шифр сдвига, аффинный шифр, шифр замены с конечным ключом, шифр Виженера, шифр перестановки.

Надежность шифров

11. Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра.
12. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона.
13. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей.
14. (k|y)-совершенные шифры: определение, эквивалентные условия.
15. Необходимые и достаточные условия (k|y)-совершенных шифров.
16. Необходимые и достаточные условия одновременно совершенных и (k|y)-совершенных шифров.

Математическая модель шифра замены с ограниченным и неограниченным ключом

17. Понятие опорного шифра, степени опорного шифра. Случайный и детерминированный генераторы ключевого потока. Примеры генераторов.
18. Определение шифра замены с ограниченным и неограниченным ключом.
19. Определение совершенного шифра замены, эквивалентные условия. Несовершенность в общем случае шифра замены с ограниченным ключом.

20. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом.

Имитостойкие шифры

21. Понятие имитации сообщений. Определение вероятности $P_{им}$. Нижняя оценка для вероятности имитации сообщения. Критерий достижимости нижней оценки. Примеры шифров с достижимой нижней оценкой имитации сообщений.
22. Понятие подмены сообщений. Определение вероятности $P_{подм}$. Нижняя оценка для вероятности подмены сообщения. Критерий достижимости нижней оценки. Примеры шифров с достижимой нижней оценкой подмены сообщений.
23. Совершенные имитостойкие шифры замены с неограниченным ключом.

Шифры, не распространяющие искажений

24. Шифры, не распространяющие искажений типа замены знаков: определение, эквивалентные условия.
25. Понятие изометрии. Свойства изометрий.
26. Теорема А.А.Маркова. Примеры шифров, не распространяющих искажения типа замены знаков.
27. Шифры, не распространяющие искажений типа пропуска знаков: основные понятия.
28. Критерий для шифров, не распространяющеих искажений типа пропуска знаков, в классе эндоморфных шифров.
29. Шифры, не распространяющие искажений типа вставки знаков

Схемы разделения секрета

30. Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ.
31. Схема разделения секрета Шамира.
32. Схемы разделения секрета на основе n-разрядных равновесных двоичных кодов.
33. Схема разделения секрета на основе китайской теоремы об остатках.
34. Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера.
35. Схема Ито-Саито-Нишизеки.

Симметричные блочные шифры

36. Итеративные блочные шифры. Обратимость итеративного блочного шифра.
37. Шифры Фейстеля и их обратимость.
38. Построение цикловой функции. Входное и выходное отображения.
39. Слабые ключи итеративного блочного шифра.
40. Режимы использования симметричных блочных шифров.
41. Шифр Магма из ГОСТ Р 34.12-2015.
42. Криптоанализ симметричных блочных шифров.

Криптография с открытым ключом

43. Алгоритм быстрого возведения в степень. Задачи, приводящие к криптографии с открытым ключом и их решение.
44. Схема Диффи-Хеллмана.
45. Криптосистема без передачи ключа (шифр Шамира).
46. Шифр Эль-Гамаля.
47. Шифр RSA.
48. Рюкзачные криптосистемы.

Хеш-функции

49. Хеш-функции. Требования, предъявляемые к хеш-функциям.

50. Криптографические хеш-функции. Способы построения криптографических хеш-функций.

Коды аутентификации

51. Понятие имитации и подмены кода аутентификации. Определение вероятностей $P_{им}$, $P_{подм}$.
52. Нижние оценки для вероятности имитации и подмены кода аутентификации. Критерий достижимости нижних оценок.
53. Оптимальные коды аутентификации. Достаточные условия оптимального кода аутентификации.

Электронные подписи

54. Электронная подпись RSA.
55. Электронная подпись Фиата-Шамира.
56. Электронная подпись Эль-Гамаля.
57. Электронная подпись Шнорра.
58. Электронная подпись с доверенным посредником на основе симметричной криптосистемы.