|  |  |
| --- | --- |
| Приложение 4 к рабочей программе дисциплины | |
| ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ | |
| **Фонд оценочных средств** | |
| Направление/ специальность подготовки | 09.04.04 Программная инженерия |
| Специализация/ профиль/ программа подготовки | Процессы и методы разработки программных продуктов |
| Уровень высшего образования | Магистратура |
| Форма обучения | Очная, заочная |
| Факультет | О Естественнонаучный |
| Выпускающая кафедра | О7 Информационные системы и программная инженерия |
| Кафедра-разработчик | И4 [Радиоэлектронные системы управления](https://www.voenmeh.ru/education/faculties-and-departments/faci/kaf-i4) |
| Год приема | 2023 |

**ФОС по дисциплине «ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ»**

**ОП ВО 09.04.04 Программная инженерия «Процессы и методы разработки программных продуктов», формы обучения очная, заочная**

ОПК-7 - способен применять при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях;

ОПК-5- способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;

ПСК-2.3 - способен организовывать разработку программного обеспечения для анализа, распознавания и обработки информации

ПСК-2.4- способен организовывать разработку программного обеспечения для систем цифровой обработки сигналов

|  |  |  |  |
| --- | --- | --- | --- |
| **Номер задания** | **Содержание вопроса** | **Компетенция** | **Время ответа, мин.** |
|  | Определить количество информации в комбинаторной мере для двоичной системы счисления при условии, что передается два сообщения величиной 2 бит и 7 бит  512  132  9  128 | ОПК - 7 | 3 |
|  | Сообщения передаются 6-разрядным и 8-разрядным двоичным кодом. Определить количество информации статистической мерой при передаче двух сообщений разрядности 6 и 8, при условии равенства вероятности появления всех элементов алфавита  320  14  8  256 | ОПК - 7 | 3 |
|  | Энтропия равна 0, когда вероятность наступления события pi=  0  1  0.5  1/e | ОПК - 7 | 1 |
|  | Что принято называть электронной подписью?  присоединяемое к тексту его криптографическое преобразование текст зашифрованный текст  скан подписи | ОПК - 7 | 1 |
|  | Требования, предъявляемые к современным криптографическим системам защиты информации: знание алгоритма шифрования не должно влиять на надежность защиты  структурные элементы алгоритма шифрования должны быть неизменными не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования | ОПК - 7 | 1 |
|  | Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 542кГц  542  542000  293764  1084  1084000 | ОПК - 7 | 5 |
|  | Определить ширину спектра в передаваемом сообщении, если пропускная способность канала составляет 822963 бит/с. Ответ представить в Гц | ОПК - 7 | 8 |
|  | Определить требуемое минимальное расстояние по Хеммингу для исправления 1-кратной ошибки | ОПК - 7 | 3 |
|  | Избыточность кода с 77 информационными  и 8 проверочными битами равна | ОПК - 7 | 4 |
|  | Вычислить разрешенную кодовую комбинацию циклического кода для информационной последовательности 1111 и образующего полинома 1011 | ОПК - 7 | 8 |
|  | Является ли следующая последовательность кодов префиксным кодом?  00  01  11  010  011 | ОПК - 7 | 5 |
|  | Найти пропущенную в номере банковской карты цифру:  Х475201128118025 | ОПК - 7 | 7 |
|  | Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности? алгоритмом гаммирования алгоритмом перестановки алгоритмом аналитических преобразований  Шифром Люцифера | ОПК - 7 | 1 |
|  | Не является свойством или характеристикой односторонней функции хэширования: Она преобразует сообщение произвольной длины в значение фиксированной длины Имея значение дайджеста сообщения, невозможно получить само сообщение Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко Она преобразует сообщение фиксированной длины в значение переменной длины | ОПК - 7 | 1 |
|  | Выберите то, что указывает на изменение сообщения: Изменился открытый ключ Изменился закрытый ключ Изменился хэш сообщения Сообщение было правильно зашифровано | ОПК - 7 | 1 |
|  | Разработчик первого алгоритма квантовой криптографии:  Хеллман  Шнайер  Фейстель  Брассар  Шамир | ОПК - 7 | 1 |
|  | Определите преимущество RSA над AES? Он может обеспечить функциональность цифровой подписи и шифрования Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи Это блочный шифр и он лучше поточного Он использует одноразовые шифровальные блокноты | ОПК - 7 | 1 |
|  | Определить значение функции Эйлера для числа 8 | ОПК - 7 | 5 |
|  | На алгоритме Люцифер базируется:  AES  DES  RSA  Диффи-Хеллмана | ОПК - 7 | 1 |
|  | Если при использовании хеширования разных сообщений получается один и тот же хеш, то это:  кластеризация  хэширование  коллизия  MAC | ОПК - 7 | 1 |
|  | Определить количество информации в комбинаторной мере для двоичной системы счисления при условии, что передается два сообщения величиной 9 бит и 1 бит  512  10  1024  2048 | ОПК-5 | 3 |
|  | Энтропия равна 0, когда вероятность наступления события pi=  0  1  0.5  1/е | ОПК-5 | 1 |
|  | Энтропия максимальна, когда вероятность наступления события pi=  1  0  0.5  1/i | ОПК-5 | 1 |
|  | Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 797кГц | ОПК-5 | 5 |
|  | Преобразование давления в электрический сигнал присуще следующему эффекту:  фотогальваническому пьезоэлектрическому  Зеебека  электромагнитной индукции  пироэлектрическому | ОПК-5 | 1 |
|  | Определить максимальную скорость передачи двоичных данных в реальном канале, если полоса пропускания канала 532 Гц, отношение сигнал/шум 56 Дб | ОПК-5 | 10 |
|  | Определить ширину спектра в передаваемом сообщении, если пропускная способность канала составляет 227089 бит/с. Ответ представить в Гц | ОПК-5 | 8 |
|  | Определить требуемое минимальное расстояние по Хеммингу для исправления 4-кратной ошибки | ОПК-5 | 3 |
|  | Определить вероятность пропуска ошибки при передаче четырех информационных разрядов кода с контролем четности, если вероятность безошибочной передачи равна 0,9.  !!!Учесть суммарное количество разрядов кода! | ОПК-5 | 8 |
|  | Вычислить степень сжатия, если длина исходного сообщения  равна 888, длина сжатого - 542 | ОПК-5 | 4 |
|  | Минимальное количество ключей, необходимое для приватного общения группы из 34 пользователей равно | ОПК-5 | 5 |
|  | Найти пропущенную в номере банковской карты цифру:  4460Х84553390931 | ОПК-5 | 7 |
|  | Определить значение функции Эйлера для числа 13 | ОПК-5 | 5 |
|  | К симметричным методам относятся:  Эллиптических кривых  BB84  RSA  Эль-Гамаля  DES  Диффи-Хеллмана  AES | ОПК-5 | 2 |
|  | Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:  2  1  4  2^n | ОПК-5 | 1 |
|  | Разработчик первого алгоритма с открытыми ключами:  Хеллман  Шнайер  Фейстель  Брассар  Шамир | ОПК-5 | 1 |
|  | Невозможность несанкционированного изменения информации - это  идентификация  обеспечение криптостойкости  аутентификация  обеспечение конфиденциальности  обеспечение целостности | ОПК-5 | 1 |
|  | Зашифровать с помощью афинного шифра (2,1) букву Б русского алфавита (позиции алфавита 0:32) | ОПК-5 | 7 |
|  | Если буквы меняют свои позиции, но сохраняют свои роли, то это:  шифр подстановки  шифр Цезаря  шифр Полибия  перестановочное шифрование | ОПК-5 | 1 |
|  | Является ли следующая последовательность кодов префиксным кодом?  00  01  10  110  101 | ОПК-5 | 5 |
|  | Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 542кГц  542  542000  293764  1084  1084000 | ПСК-2.3 | 5 |
|  | Определить максимальную скорость передачи двоичных данных в реальном канале, если полоса пропускания канала 346 Гц, отношение сигнал/шум 24 Дб | ПСК-2.3 | 10 |
|  | Определить ширину спектра в передаваемом сообщении, если пропускная способность канала составляет 812703 бит/с. Ответ представить в Гц  AMI (Alternate mark inversion) код | ПСК-2.3 | 8 |
|  | Определить требуемое минимальное расстояние по Хеммингу для обнаружения 11-кратной ошибки | ПСК-2.3 | 3 |
|  | Определить требуемое минимальное расстояние по Хеммингу для обнаружения 12-кратной ошибки и исправления 7-кратной | ПСК-2.3 | 3 |
|  | Избыточность кода с 112 информационными  и 13 проверочными битами равна | ПСК-2.3 | 4 |
|  | Вычислить разрешенную кодовую комбинацию циклического кода для информационной последовательности 1001 и образующего полинома 1011 | ПСК-2.3 | 8 |
|  | Вычислить степень сжатия, если длина исходного сообщения  равна 888, длина сжатого - 542 | ПСК-2.3 | 4 |
|  | Определить нижнюю границу частот в передаваемом сообщении, если пропускная способность канала составляет 22436 бит/с. Ответ представить в Гц | ПСК-2.3 | 5 |
|  | Самая помехозащищенная линия связи на основе:  коаксиальный кабель  радиолиния  витая пара  волоконно-оптический кабель  беспроводная оптическая линия | ПСК-2.3 | 1 |
|  | Какова цель использования генераторов псевдослучайных чисел при поточном шифровании?  формирование открытых ключей  защита информации от всех случайных или преднамеренных изменений  получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа  защита информации от случайных помех при передаче и хранении  сжатие информации | ПСК-2.3 | 1 |
|  | Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии:  функцией Диффи-Хеллмана  односторонней функцией  функцией Эйлера  криптографической функцией | ПСК-2.3 | 1 |
|  | Что является особенностью использования режима CBС блочного шифра? одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст  сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке  одинаковые блоки исходного текста преобразуются в одинаковый шифротекст  этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений  сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока | ПСК-2.3 | 1 |
|  | Какой язык обладает минимальной избыточностью сообщений?  Язык, в котором только два символа  Язык, в котором некоторые символы гораздо вероятнее других  Язык, в котором как можно больше символов  Язык, в котором все символы равновероятны и могут встречаться в сообщениях независимо друг от друга в любом порядке | ПСК-2.3 | 1 |
|  | Определить вес кодовой комбинации: 11110000000011 | ПСК-2.3 | 1 |
|  | Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)?  для генерации псевдослучайных чисел  для сжатия информации  для формирования открытых ключей  для формирования хеш-кода | ПСК-2.3 | 1 |
|  | Кто предложил реализацию совершенно секретной системы, называемую в настоящее время одноразовой лентой или одноразовым блокнотом?  Шеннон  Вернам  Альберти  Виженер | ПСК-2.3 | 1 |
|  | Определить значение функции Эйлера для числа 7 | ПСК-2.3 | 5 |
|  | Какой алгоритм не используется для шифрования?  AES  DES  RSA  Диффи-Хеллмана | ПСК-2.3 | 1 |
|  | Выберите вариант ответа, содержащий только взаимно простые числа:  7, 27, 77, 147  5, 9, 27, 54  3, 7, 25, 38  4, 7, 16, 59 | ПСК-2.3 | 3 |
|  | Каким преимуществом не обладает цифровая система обработки по сравнению с аналоговой:  Отсутствие проблемы согласования нагрузок  Малые габариты и потребление  Высокая точность преобразования  Высокая стабильность характеристик | ПСК-2.4 | 1 |
|  | Какая процедура называется дискретизацией:  Прореживание отсчетов по времени  Прореживание отсчетов по частоте  Преобразование аналоговых отсчетов сигнала в цифровые  Взятие мгновенных значений сигнала с заданным периодом | ПСК-2.4 | 1 |
|  | Какая процедура называется квантованием:  Прореживание отсчетов по времени  Преобразование аналоговых отсчетов сигнала в цифровые  Взятие мгновенных значений сигнала с заданным периодом  Переход из временной области в частотную | ПСК-2.4 | 1 |
|  | **Максимальное значение энтропии источника, который порождает 16 различных символов равно:**  **1**  **4**  **16**  **216** | ПСК-2.4 | 1 |
|  | **Как соотносятся коды Фано и Хаффмана для источника с равномерным распределением вероятностей?**  **Равны**  **В Хаффмана больше символов**  **В Фано больше символов** | ПСК-2.4 | 1 |
|  | Сообщения передаются 8-разрядным и 7-разрядным двоичным кодом. Определить количество информации по Хартли, передаваемое двумя сообщениями  15  576  32  256 | ПСК-2.4 | 3 |
|  | Преобразование давления в электрический сигнал присуще следующему эффекту:  фотогальваническому пьезоэлектрическому  Зеебека  электромагнитной индукции  пироэлектрическому | ПСК-2.4 | 1 |
|  | Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 614кГц | ПСК-2.4 | 5 |
|  | Одномодовые или многомодовые - это параметр:  акустической линии связи витой пары  радиоволн  оптоволокна | ПСК-2.4 | 1 |
|  | Определить кодовое расстояние по Хеммингу двух кодовых комбинаций: 111000111 и 111110111 | ПСК-2.4 | 2 |
|  | Определить вероятность пропуска ошибки при передаче четырех информационных разрядов кода с контролем четности, если вероятность безошибочной передачи равна 0,9.  !!!Учесть суммарное количество разрядов кода! | ПСК-2.4 | 8 |
|  | Вычислить коэффициент сжатия, если длина исходного сообщения  равна 356, длина сжатого - 60 | ПСК-2.4 | 4 |
|  | Стеганография:  способ передачи или хранения зашифрованной информации  техника сокрытия информации  раздел криптографии  метод подстановочного шифрования  метод перестановочного шифрования | ПСК-2.4 | 1 |
|  | К симметричным методам относятся:  Эллиптических кривых  BB84  RSA  Эль-Гамаля  DES  Диффи-Хеллмана  AES | ПСК-2.4 | 2 |
|  | Как связаны ключи друг с другом в системе с открытым ключом:  экзистенциально  логически  алгоритмически  математически | ПСК-2.4 | 1 |
|  | Выберите то, что используют для создания цифровой подписи:  Открытый ключ получателя  Открытый ключ отправителя   Закрытый ключ получателя  Закрытый ключ отправителя | ПСК-2.4 | 1 |
|  | **Основными видами словарных методов типа LZ являются:**  адаптивные коды  коды со скользящим окном и коды с использованием адаптивного словаря  адаптивный код Хаффмана и коды с использованием адаптивного словаря  оптимальные коды | ПСК-2.4 | 1 |
|  | Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя: ECC RSA DES Диффи-Хеллман | ПСК-2.4 | 1 |
|  | Для чего используются в криптографии сдвиговые регистры с обратной связью?  для сжатия информации  для формирования открытых ключей  для формирования хеш-кода  для генерации псевдослучайных чисел | ПСК-2.4 | 1 |
|  | Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?  сложение по модулю 2  нахождение остатка от деления на большое простое число  замена бит по таблице замен  перестановка бит  возведение в степень | ПСК-2.4 | 1 |