Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
Начальник УРОПСП

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 01ff058c007bae2c8149e7712c28ce8469
Владелец: Мельникова Виктория Александровна
Действителен: с 18.04.2022 по 18.04.2023

Фонд оценочных средств
(приложение к рабочей программе модуля)

«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Специализация
«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ цифровых технологии
РАЗРАБОТЧИК кафедра информационной безопасности

1. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными индикаторами достижения компетенций

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ОПК-10: Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ОПК-10.1: Знает основные задачи и понятия криптографии, модели шифров и математические методы их исследования, типовые криптографические алгоритмы. ОПК-10.2: Владеет методами и средствами криптографической защиты информации при решении задач профессиональной деятельности.	Методы и средства криптографической защиты информации	*Знать:* основные задачи и понятия криптографии; типовые криптографические алгоритмы; требования к шифрам и основные характеристики шифров; принципы разработки современных блочных и поточных криптосистем. *Уметь*: анализировать результаты исследований; анализировать проекты средств защиты информации. *Владеть:* навыками использования типовых криптографических алгоритмов.

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПОЭТАПНОГО ФОРМИРОВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ (ТЕКУЩИЙ КОНТРОЛЬ) И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2.1 Для оценки результатов освоения дисциплины используются:

- оценочные средства текущего контроля успеваемости;

- оценочные средства для промежуточной аттестации по дисциплине.

2.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания;

- задания и контрольные вопросы по лабораторным работам.

2.3 К оценочным средствам для промежуточной аттестации по дисциплине, проводимой в форме дифференцированного зачета и экзамена, относятся:

- промежуточная аттестация в форме дифференцированного зачета проходит по результатам прохождения всех видов текущего контроля успеваемости;

- экзаменационные вопросы.

3. ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

3.1 Тестовые задания предназначены для оценки в рамках текущего контроля успеваемости знаний, приобретенных студентами на лекционных и лабораторных занятиях и для измерения соответствующих индикаторов достижения компетенции.

Содержание теста определяется в соответствии с содержанием дисциплины пропорционально учебному времени, отведенному на изучение разделов, перечисленных в рабочей программе модуля.

Время выполнения теста 70 мин.

Тестовые задания приведены в Приложении № 1, а ключи к ним – в приложении № 5.

Таблица 5 - Шкала оценок уровня освоения дисциплины по тесту.

Оценка	Неудовлетворительный «2» (неудовлетворительно)	Пороговый «3» (удовлетворительно)	Углубленный «4» (хорошо)	Продвинутый «5» (отлично)
	Менее 50% правильных ответов.	50-70% правильных ответов.	71-90% правильных ответов.	91-100% правильных ответов.

3.2. Задания и контрольные вопросы по лабораторным работам приведены в приложении № 2. В приложении № 3 приведены примеры для защиты лабораторных работ.

4. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1 Промежуточная аттестация по дисциплине проводится в форме дифференцированного зачета, экзамена.

Промежуточная аттестация проходит по результатам прохождения всех видов текущего контроля успеваемости.

Типовые экзаменационные вопросы приведены в Приложении № 4.

Дисциплина рассчитана на два семестра (7 и 8 семестр), в 7 семестре проводится дифференцированный зачет, в 8 семестре – экзамен.

Таблица 2 - Шкала оценок уровня освоения дисциплины по дифференцированному зачету

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Правильно выполнены менее чем 50% заданий. Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи.	Правильные выполнены 51-64% заданий. Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.	Правильные выполнены 65-94% заданий. Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.	Правильные выполнены 95-100% заданий. Ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания предмета. Соблюдаются нормы литературной речи.

Таблица 3 - Шкала оценок уровня освоения дисциплины по экзамену.

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания, задачи.	Усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в	Твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и	Глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его изложил, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые реше-

	выполнении практических заданий.	навыками при выполнении практических заданий.	ния, умеет самостоятельно обобщать и излагать материал, не допуская ошибок.

5. СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «**Методы и средства криптографической защиты информации**» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация «Безопасность открытых информационных систем»).

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности 20.04.2022 г. (протокол № 7).

Заведующий кафедрой  Н.Я. Великите

Приложение № 1

ТИПОВЫЕ ВАРИАНТЫ ТЕСТОВЫХ ЗАДАНИЙ (семестр 7)

	ВАРИАНТ 1
1.	Криптография – это наука о защите информации: 1. от несанкционированного доступа посторонними лицами 2. от прочтения ее посторонними лицами, достигаемая путем шифрования, которое делает защищенные данные труднораскрываемыми без знания специальной (ключевой) информации 3. с помощью математических преобразований, которые являются симметричными
2.	Если число *x* является простым относительно *y*, то справедливы следующие утверждения: 1. его можно разложить на сомножители, на которые число *y* не делится без остатка 2. его нельзя разложить на сомножители, на которые число ***y*** делится без остатка 3. *НОД (x,y)=1*
3.	Замена смысловых конструкций исходной информации (слов, предложений) кодами называется: 1. шифрованием 2. кодированием 3. дешифрованием
4.	Если противник ничего не знает об источнике сообщений, кроме того, что он создает текст на русском языке, то для сокращения полного перебора он может воспользоваться: 1 относительными частотами букв в русском языке 2. абсолютными частотами букв в русском языке 3. методом обратных преобразований
5.	По характеру использования ключа все криптосистемы можно разделить на: 1. блоковые и потоковые 2. синхронные и асинхронные 3. симметричные и асимметричные
6.	Шифры перестановки являются частным случаем: 1. блоковых шифров 2. шифров перестановки 3. скремблеров
7.	Элементы матричной алгебры применяются для шифрования в методах: 1. перестановок 2. аналитического шифрования 3. замены по таблице
8.	В идеальной криптосистеме один и тот же ключ может использоваться: 1. только один раз 2. многократно 3. два раза
9.	Наименьшее число, взаимно простое с 756: 1. 565 2. 5 3. 113
10.	Количество простых чисел в диапазоне от 20 до 40 равно: 1. 4 2. 3 3. 2

	4. 5
11.	Наименьшее число, взаимно простое с 9100: 1. 3 2. 2 3. 1
12.	Расширенный алгоритм Евклида вычисляет: 1. аддитивную инверсию числа 2. остаток от деления двух чисел 3. мультипликативную инверсию числа
13.	Любой элемент из Z_n*: 1. является простым числом 2. имеет мультипликативную инверсию 3. является делителем n
14.	Число a имеет мультипликативную инверсию в Z_n, если: 1. НОД(a,n)$=0$ 2. НОД(a,n)$\neq 1$ 3. НОД(a,n)$=1$
15.	Значение выражения $(a + b) \bmod n$ равно: 1. $[(a \bmod n) + (b \bmod n)] \bmod n$ 2. $[(a \bmod n) + (b \bmod n)]$ 3. $(a + b)$
16.	Аффинный шифр определен: 1. на кольце 2. в группе 3. в поле
17.	Согласно принципу Керкгоффса предполагается, что: 1. ключ может быть общеизвестен, а алгоритм шифрования должен быть строго засекречен 2. ключ должен быть настолько труден, что скрывать алгоритм кодирования/дешифрования нет необходимости 3. и ключ, и алгоритм шифрования должны быть строго засекречены
18.	При статистической атаке противник: 1. пробует все возможные ключи 2. анализирует некоторые свойственные языку исходного текста характеристики 3. в дополнение к перехваченному зашифрованному тексту, получил доступ к некоторым парам исходный/зашифрованный текст»
19.	При шифровании методом Плейфера фиктивный символ ставится между: 1. словами 2. слогами 3. стоящими рядом одинаковыми буквами
20.	Соотношение, описывающее процесс образования зашифрованных данных из открытых называется: 1. способом шифрования 2. функцией шифрования 3. программой шифрования
	ВАРИАНТ 2
1.	Шифр – это: 1. совокупность преобразований, с помощью которых осуществляется кодирование информации

	2. алгоритм преобразования, в котором используется ключ 3. совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования
2.	Общей задачей дешифрования называется задача вычисления: 1. апостериорных вероятностей 2. алгоритма дешифрования 3. априорных вероятностей
3.	Методы, позволяющие скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации относятся к методам: 1. шифрования 2. сжатия 3. стеганографии
4.	Шифр Цезаря является частным случаем шифра: 1. моноалфавитной подстановки 2. полиалфавитной подстановки 3. мультиалфавитной подстановки
5.	Блоковые шифры являются частным случаем: 1. симметричного шифрования 2. асимметричного шифрования 3. шифров перестановки
6.	В симметричных криптосистемах: 1. для шифрования и дешифрования всегда используется один и тот же алгоритм 2. ключ может быть доступным для всех пользователей 3. как для шифрования, так и для дешифрования применяется один и тот же ключ
7.	Режимы использования блочных шифров применяются с целью: 1. повысить криптостойкость системы 2. сокрытия структуры закодированного сообщения 3. увеличения скорости шифрования 4. уменьшения объема зашифрованного сообщения
8.	Наибольший общий делитель чисел 574, 273 равен: 1. 7 2. 1 3. 6
9.	Из перечисленных пар чисел взаимно простыми являются: 1. 18, 21 2. 22, 25 3. 24, 27
10.	Наибольший общий делитель чисел 115, 253 равен: 1. 23 2. 3 3. 1
11.	Потоковый шифр можно применять для: 1. генерирования случайных чисел 2. блокового шифрования 3. построения электронной подписи
12.	Операция по модулю в криптографии – это: 1. вычисление остатка от деления двух чисел 2. нахождение модуля числа

	3. вычисление наибольшего общего делителя двух чисел
13.	Числа a и b мультипликативно инверсны в Z_n, если: 1. $(a \times b) mod\ n=0$ 2. $(a \times b) mod\ n \neq 1$ 3. $(a \times b) mod\ n=1$
14.	Число 4 имеет мультипликативную инверсию: 1. в Z_{12} 2. в Z_{13} 3. в Z_{14}
15.	В Z_{10} ноль аддитивен: 1. единице 2. десяти 3. самому себе
16.	В Z_{10} число 9: 1. не имеет мультипликативной инверсии 2. мультипликативно единице 3. мультипликативно самому себе
17.	Криптоанализ – это наука и искусство: 1. создания секретных шифров 2. создания и взламывания секретных шифров 3. взламывания шифров
18.	В моноалфавитных шифрах символ исходного текста: 1. всегда заменяется на один и тот же символ зашифрованного текста, независимо от его позиции в тексте 2. при шифровании зависит от его позиции в тексте 3. при шифровании всегда заменяется на символ, стоящий справа
19.	В шифре Хилла размерность ключевой матрицы зависит от: 1. величины блоков, на которые разбит исходный текст 2. количества строк в исходном тексте 3. количества символов в строке исходного текста
20.	Из перечисленных пар чисел взаимно простыми являются: 1. 18, 21 2. 18, 23 3. 10, 15
	ВАРИАНТ 3
1.	Соотношение, описывающее процесс образования зашифрованных данных из открытых называется: 1. алгоритмом шифрования 2. методом шифрования 3. программой шифрования
2.	Апостериорная вероятность – это вероятность: 1. получения ключа с помощью перехвата 2. того, что шифрограмма будет расшифрована без знания ключа 3. использования системы криптографической защиты в условиях постоянных атак
3.	Процесс дешифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования называется: 1. повторным шифрованием 2. криптоанализом 3. обратным шифрованием

4.	Зашифрованное сообщение ЗАЩИТА с помощью шифра Цезаря с ключом 4 (для шифрования используется алфавит «А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я ») : 1. ИТАЗАЩ 2. ЩИЗАТА 3. МДЭНЦД
5.	Потоковое шифрование является частным случаем: 1. симметричного шифрования 2. асимметричного шифрования 3. шифров гаммирования
6.	В потоковых шифрах основной операцией кодирования являются: 1. матричные преобразования 2. преобразования, основанные на вычислениях с плавающей точкой 3. операции сложения по модулю два (xor)
7.	Пары чисел, которые не являются взаимно простыми: 1. 8 и 3 2. 8 и 6 3. 12 и 7
8.	В Z_{23} значение 3^{-1} равно: 1. 4 2. 12 3. 8
9.	Количество операций умножения, которых достаточно для вычисления выражения 7^8: 1. 3 2. 5 3. 7 4. 4
10.	Условие, при которых простейший шифр Цезаря становится невскрываемым: 1. сообщение представлено двоичным кодом 2. буквы сообщения перемешаны между собой 3. буквы сообщения равновероятны и независимы
11.	Простой алгоритм Евклида вычисляет: 1. аддитивную инверсию числа 2. наибольший общий делитель двух чисел 3. мультипликативную инверсию числа
12.	Число -17 в системе вычетов Z_{26} равно: 1. 9 2. 1 3. 0
13.	Числа *a* и *b* аддитивно инверсны в Z_n, если: 1. $(a+b) mod\ n=0$ 2. $(a+b) mod\ n\neq 1$ 3. $(a+b) mod\ n=1$
14.	Значение выражения $(12 – 43)\ mod\ 13 = (–31)\ mod\ 13$ равно: 1. 8 2. -5 3. 5
15.	Число *8* в Z_{10} не имеет мультипликативную инверсию, потому что: 1. *8* не принадлежит Z_{10}

	2. *НОД(10,8)=2* 3. четные числа не могут иметь мультипликативную инверсию в любой системе вычетов
16.	Согласно принципу Керкгоффса, нужно всегда предполагать, что противник: 1. знает алгоритм кодирования/дешифрования 2. не знает алгоритм кодирования/дешифрования 3. всегда прослушивает канал передачи данных
17.	При методе грубой силы противник: 1. пробует все возможные ключи 2. анализирует некоторые свойственные языку исходного текста характеристики 3. в дополнение к перехваченному зашифрованному тексту, получил доступ к некоторым парам исходный/зашифрованный текст»
18.	Слову *"crypt"* соответствует числовая последовательность: *x=(2,17,24,15),* которая зашифрована аффинным шифром с ключами (3,5); в результате шифрования получилось сообщение: 1. *LEZY* 2. *LEAH* 3. *LEYG*
19.	Систематически перемешанный алфавит – это буквы алфавита, записанные: 1. в обратном порядке их следования в алфавите 2. по порядку их следования в алфавите, исключая буквы, использованные в ключевом слове 3. по порядку их следования в алфавите, причем буквы, использованные в ключевом слове, повторяются дважды
20.	Если противник ничего не знает об источнике сообщений, кроме того, что он создает текст на английском языке, то для сокращения полного перебора он может воспользоваться: 1. абсолютными частотами букв в английском языке 2. методом обратных преобразований 3. словарем наиболее часто используемых в английском языке слов

ТИПОВЫЕ ВАРИАНТЫ ТЕСТОВЫХ ЗАДАНИЙ (семестр 8)

	ВАРИАНТ 1
1.	В российском стандарте электронная подпись к сообщению состоит из чисел *r, s*; число *r* не должно быть равно нулю, т.к. в этом случае: 1. проверка подписи не будет правильной 2. сформировать подпись будет невозможно 3. автор сообщения может отказаться от своей подписи
2.	Наиболее известными представителями асимметричных систем шифрования является алгоритм: 1. RSA 2. Рабина-Миллера 3. Хаффмана
3.	Для потоковых шифров справедливо утверждение: 1. для получения гаммы чаще всего используются генераторы псевдослучайных чисел 2. имея пару *открытый текст-зашифрованный текст* вычислить гамму невозможно

	3. чем меньше разница длин ключа и исходной информации, тем выше вероятность успешной атаки на шифротекст
4.	В современной криптографии используются режим: 1. ECB 2. CBB 3. AFB
5.	В современной криптографии с открытыми ключами используются следующие виды необратимых преобразований: 1. разложение произведения больших простых чисел на сомножители 2. матричные преобразования 3. разложение на сомножители больших простых чисел
6.	Алгоритм Эль-Гамаля базируется на основе необратимых преобразований: 1. матричные преобразования 2. разложение произведения больших простых чисел на сомножители 3. вычисление логарифма в конечном поле
7.	Для оптимизации вычислений при кодировании по алгоритму RSA используется прием, называемый цепочкой: 1. возведения в степень 2. сложений 3. умножений
8.	Электронной цифровой подписью называется: 1. присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения 2. зашифрованное сообщение, которое содержит информацию об алгоритме шифрования и ключе 3. сообщение, посылаемое в открытом виде получателю сообщения, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения
9.	Атака на подпись RSA по выбранному шифротексту базируется на свойстве: 1. коммутативности при вычислении логарифма в конечном поле 2. мультипликативности при возведении в степень 3. коммутативности при возведении в степень
10.	В идеальной системе шифрования найти сообщение без знания ключа: 1. невозможно 2. возможно при наличии компьютера и неограниченного времени вычислений 3. возможно при полном переборе ключей
11.	Секретные параметры пользователя в протоколе Шамира 1. взаимно простые 2. четные 3. нечетные
12.	Хэш-функция в криптографии должна обладать свойством трудности нахождения: 1. аргументов с равными значениями функции 2. участков монотонности 3. значений функции для некоторых (секретных) аргументов
13.	В российском стандарте электронная подпись к сообщению состоит из чисел *r, s*; число *r* не должно быть равно нулю, т.к. в этом случае: 1. подпись не будет зависеть от сообщения 2. проверка подписи не будет правильной

	3. сообщение будет пустым
14.	Шифр Вернама применили для шифрования неизвестного сообщения с ключом 1100 и получили зашифрованное сообщение 1000; неизвестное сообщение среди приведенных: 1. 1110 2. 1010 3. 0000 4. 0100
15.	В системе Диффи-Хеллмана используется большое число P, по модулю которого ведется вычисление ключа; это число должно быть: 1. любыми целым 2. простым 3. любым нечетным
16.	Шифр RSA базируется на сложности задачи: 1. дискретного логарифмирования 2. извлечения квадратного корня 3. разложения числа на простые множители
17.	В протоколе шифра Эль-Гамаля сообщение пересылается: 1. один раз 2. два раза 3. три раза
18.	Пусть x – некоторое сообщение, $h\,(x)$ – хэш-функция, тогда: 1. вычисление хэш-функции $h\,(x)$ должно выполняться относительно быстро 2. вычисление хэш-функции $h\,(x)$ должно быть практически невозможным 3. можно легко найти другое сообщение $x' \neq x$, такое, что $h\,(x') = h\,(x)$
19.	Для асимметричных криптосистем справедливо утверждение: 1. между открытым и закрытым ключом существует математическая зависимость 2. зная открытый ключ можно шифровать и дешифровать сообщения 3. имея пару открытый текст-зашифрованный текст можно вычислить открытый ключ
20.	В современной криптографии используются режим: 1. CBB 2. CBC 3. AFB
	ВАРИАНТ 2
1.	При использовании криптографических систем защиты могут возникать побочные эффекты: 1. ошибки шифрования для больших объемов информации 2. перегрузка трафика 3. сбой в работе центрального процессора
2.	Одним из наиболее распространенных способов задания блочных шифров является: 1. сеть Фейстела 2. матрица Виженера 3. квадрат Полибия
3.	Маршруты Гамильтона применяются в методах: 1. аналитического шифрования 2. перестановки 3. замены 4. гаммирования
4.	Сеть Фейстеля используется в основе:

	1. стандарта шифрования DES 2. алгоритма BlowFish 3. алгоритма Rijndael
5.	Российский стандарт шифрования ГОСТ 28147-89 предусматривает следующие режимы работы: 1. простая замена 2. простая подстановка 3. гаммирование со сцеплением блоков
6.	Алгоритм RSA базируется на основе необратимых преобразований: 1. вычисление логарифма в конечном поле 2. разложение произведения больших простых чисел на сомножители 3. вычисление корней алгебраических уравнений
7.	Для алгоритма Эль-Гамаля справедливы следующие утверждения: 1. получаемый шифротекст в два раза длиннее открытого текста 2. открытый и закрытый ключ можно менять местами 3. в алгоритме Эль-Гамаля не используются простые числа
8.	Криптографическим называется протокол, в котором: 1. обмен информацией шифруется с помощью некоторого криптографического алгоритма 2. используется криптография, применяемая для предотвращения или обнаружения вредительства и мошенничества 3. обмен информацией не шифруется
9.	При построении электронной подписи используется: 1. хэш-функция 2. блоковый шифр 3. генератор случайных чисел
10.	В Российском стандарте для электронной подписи используется: 1. международный стандарт 2. Российский стандарт 3. стандарт Европейского сообщества
11.	В шифре RSA сообщение шифруется путем: 1. умножения на секретное число 2. возведения в степень 3. сложения с секретным числом
12.	При построении электронной подписи используется: 1. генератор случайных чисел 2. хэш-функция 3. блоковый шифр
13.	Режим OFB блокового шифра допускает: 1. получение произвольного элемента последовательности 2. параллельное получение элементов псевдослучайной последовательности 3. с. только последовательное получение элементов последовательности
14.	RC4 является: 1. совершенным шифром 2. потоковым шифром 3. блоковым шифром
15.	В Российском стандарте электронной подписи используется большое число P, по модулю которого ведутся вычисления; это число должно быть: 1. любыми целым

	2. простым 3. любым нечетным
16.	В шифре Эль-Гамаля сообщение шифруется путем: 1. возведения в степень 2. сложения с секретным числом 3. умножения на секретное число
17.	В системе Диффи-Хеллмана ключ: 1. доставляется по защищенным каналам связи 2. вычисляется 3. доставляется курьером
18.	Пусть x – некоторое сообщение, $h(x)$ – хэш-функция, тогда: 1. вычисление хэш-функции $h\,(x)$ должно практически невозможным 2. при известном y должно быть практически невозможно найти x, для которого $y = h\,(x)$; 3. при известном сообщении x легко найти другое сообщение $x' \neq x$, такое, что $h(x') = h\,(x)$
19.	В асимметричных криптосистемах: 1. все ключи являются доступными для всех пользователей 2. один из ключей является доступным для всех пользователей 3. зная закрытый ключ можно вычислить открытый ключ
20.	Сеть Фейстеля используется в основе: 1. алгоритма BlowFish 2. алгоритм Rijndael 3. Российского стандарта шифрования ГОСТ 28147-89
	ВАРИАНТ 3
1.	В асимметричных криптосистемах: 1. для шифрования и дешифрования используются разные ключи, связанные между собой некоторой математической зависимостью 2. все ключи являются доступными для всех пользователей 3. и открытый, и закрытый ключ является секретным
2.	Для ассиметричных криптосистем справедливо утверждение: 1. в асимметричных криптосистемах используется пара ключей – открытый ключ и закрытый ключ 2. зная закрытый ключ можно шифровать и дешифровать сообщения 3. имея пару *открытый текст-зашифрованный текст* легко можно вычислить открытый ключ
3.	Проблема неполных последних блоков при использовании методов блокового шифрования решается с помощью следующих способов: 1. изменение длины блока таким образом, чтобы длина исходного текста оказалась кратной длине блока 2. отказ от шифрования неполного последнего блока 3. использовании адаптивных алгоритмов шифрования
4.	На функцию стойкого блочного шифра Z=EnCrypt(X,Key) накладываются следующие условия: 1. функция EnCrypt должна быть симметричной 2. функция EnCrypt должна быть обратимой 3. длина ключа Key должна быть не меньше, чем размер шифруемого блока
5.	Системы с открытым ключом могут использоваться как: 1. общий способ задания блочных шифров

	2. средства идентификации пользователей 3. самостоятельные средства защиты передаваемых и хранимых данных
6.	Если число *x* является простым относительно *y*, то его: 1. можно разложить на сомножители, на которые число *y* не делится без остатка 2. нельзя разложить на сомножители, на которые число *y* не делится без остатка 3. нельзя разложить на сомножители, на которые число ***y*** делится без остатка
7.	Для алгоритма RSA справедливы следующие утверждения: 1. получаемый шифротекст в два раза длиннее открытого текста 2. открытый и закрытый ключ можно менять местами 3. в алгоритме RSA не используются простые числа
8.	Хэш-функция должна: 1. иметь бесконечную область значений 2. иметь конечную область определения 3. быть необратимой
9.	Система Диффи-Хеллмана базируется на сложности задачи 1. дискретного логарифмирования 2. извлечения корня 3. разложения на простые множители
10.	В Российском стандарте на блоковый шифр Магма длина блока равна: 1. 256 бит 2. 64 бита 3. 128 бит
11.	Для алгоритма Эль-Гамаля справедливы следующие утверждения: 1. открытый и закрытый ключ можно менять местами 2. в алгоритме Эль-Гамаля не используются простые числа 3. при равном значении ключа алгоритмы RSA и Эль-Гамаля имеют одинаковую криптостойкость
12.	Модуль, по которому ведутся вычисления в системе RSA – это: 1. нечетное число 2. четное число 3. простое число
13.	В Российском стандарте на электронную подпись используется: 1. шифр с открытым ключом 2. потоковый шифр 3. блоковый шифр
14.	В шифре RSA сообщение шифруется с использованием: 1. секретного ключа отправителя 2. открытого ключа получателя 3. открытого ключа отправителя 4. секретного ключа получателя
15.	Идеальный шифр: 1. может быть взломан при помощи полного перебора ключей 2. не может быть взломан 3. может быть взломан при помощи разложения на простые множители
16.	Для алгоритма RSA справедливы следующие утверждения: 1. получаемый шифротекст в два раза длиннее открытого текста 2. в алгоритме RSA не используются простые числа 3. при равном значении ключа алгоритмы RSA и Эль-Гамаля имеют одинаковую криптостойкость.

17.	При использовании криптографических систем защиты могут возникать побочные эффекты: 1. ошибки шифрования для больших объемов информации 2. замедление работы операционной системы 3. захват системных ресурсов
18.	Пусть x – некоторое сообщение, $h(x)$ – хэш-функция, тогда: 1. вычисление хэш-функции $h\ (x)$ должно практически невозможным 2. при известном y должно быть легко найти x, для которого $y = h\ (x)$; 3. при известном сообщении x практически невозможно найти другое сообщение $x' \neq x$, такое, что $h\ (x') = h\ (x)$
19.	Если при использовании методов блокового шифрования последних блок неполон, то проблема решается с помощью следующих способов: 1. изменение длины блока таким образом, чтобы длина исходного текста оказалась кратной длине блока 2. замена недостающих символов последнего блока служебными символами 3. применение других алгоритмов шифрования
20.	Российский стандарт шифрования ГОСТ 28147-89 предусматривает следующие режимы работы: 1. простая подстановка 2. гаммирование с обратной связью 3. гаммирование со сцеплением блоков

Приложение № 2

ТЕМЫ И ОБРАЗЦЫ ЗАДАНИЙ ДЛЯ ЛАБОРАТОРНЫХ ЗАНЯТИЙ (семестр 7)

Тема 1. Простой и расширенный алгоритм Евклида. Модульная арифметика. Операции в системе вычетов Zn. Аддитивная и мультипликативная инверсии.

Пример 1.1

Используя алгоритм Евклида, Найти *НОД (2740, 1760), НОД (25, 60).*

Пример 1.2

Используя расширенный алгоритм Евклида, найти мультипликативную инверсию 23 в Z_{100}.

Пример 1.3

Выполните следующие операции:
а. сложить *7* и *14* в Z_{15}
б. вычесть *11* из *7* в Z_{13}
в. умножить *11* на *7* в Z_{20}

Тема 2. Алгебраические структуры.

Пример 2.1

Дана группа $G = <Z_6, +>$, из нее сгенерировать циклические подгруппы.

Пример 2.2

Дана группа $G=<Z_{10^*}, \times>$, найти для нее циклические подгруппы.

Тема 3. Аффинный шифр. Шифр Плейфера. Шифр Виженера. Шифр Хилла

Пример 3.1

С помощью аффинного шифра зашифровать сообщение *cryptography* с ключевой парой *(3,5)* в Z_{26}.

Пример 3.2

С помощью шифра Плейфера зашифровать текст *happy;* ключ шифрования:

Секретный ключ =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

С помощью шифра Виженера зашифровать сообщение *She is listening*, используя ключевое слово *PASCAL*.

Пример 3.4

С помощью шифра Хилла зашифровать фразу: *без труда не вынешь рыбку из пруда,* записанную в 30-буквенном русском алфавите. Ключевую матрицу выбрать самостоятельно.

Тема 4. Шифр вертикальной перестановки.

Пример 4.1

Зашифровать фразу *вот пример шифра вертикальной перестановки,* используя матрицу *6×7* и числовой ключ *(5,1,4,7,2,6,3).*

Тема 5. Шифрование с помощью симметричного алгоритма DES

Пример 5.1

Зашифровать *64*-битовую последовательность *123456ABCD132536* ключом *AABB09182736CCDD.* Сделать только первый раунд.

Пример 5.2

В примере 5.1 используя ключ шифрования первого раунда сгенерировать ключ шифрования для второго раунда

Тема 6. Усовершенствованный шифр Цезаря

Пример 6.1

Зашифровать усовершенствованным шифром Цезаря (два раунда) слово ЛУНА. Ключ $k1 = 6$, $k2 = 11$. В алфавите 32 буквы (исключить букву Ё)
Таблица замены:
А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Р Т М Ф Ы Щ Ъ З Й Ю У Я Г С Э П Ц Н Б К Д Х А Ч Ш В Ь Е Ж О И Л

ТЕМЫ И ОБРАЗЦЫ ЗАДАНИЙ ДЛЯ ЛАБОРАТОНЫХ ЗАНЯТИЙ (семестр 8)

Тема 7. Криптосистемы с открытым ключом: RSA, Шамира, Эль-Гамаля.

Пример 7.1

Для шифра Шамира с параметрами $p = 30803$, $cA = 501$, $cB = 601$ и сообщения $m = 11111$ вычислить dA, dB, $x1$, $x2$, $x3$, $x4$.

Пример 7.2

Для шифра Эль-Гамаля с параметрами $p = 30803$, $g = 2$, $c = 500$, $k = 600$ и сообщения $m = 11111$ вычислить зашифрованное сообщение.

Тема 8. Алгоритм рюкзака.

Пример 8.1

Зашифровать сообщение *АБРАМОВ*, символы которого представить в бинарном виде в соответствии с таблицей кодов символов *Windows 1251*. Сверхвозрастающая последовательность равна *{2, 3, 6, 13, 27, 52, 105, 210}, n=31, m=420.*

Тема 9. Электронная подпись

Пример 9.1

Для системы RSA с параметрами пользователя P = 131, Q = 227, d = 3 и
секретного ключа c, найденного в первой лабораторной работе, вычислить подпись для сообщения m = «Happy New Year». Осуществить проверку подписи.

Пример 9.2

В подписанный документ (пример 9.1) внести ошибку (искажение). Еще раз сделать проверку подписи.

Тема 10. Алгоритм Диффи-Хеллмана

Пример 10.1

Сгенерировать секретный ключ. Исходные данные: $p = 23$ – открытое простое число, $g = 5$ – первообразный корень по модулю p (тоже открытое число), $a = 6$ – секретный ключ Алисы, $b = 15$ – секретный ключ Боба.

Пример 10.2

Найти все точки эллиптической кривой $E_7(2,6)$.

Пример 10.3

Найти порядок точки $P(9,4)$ в группе эллиптической кривой $E_{11}(6,3)$.

Пример 10.4

Найти общий ключ для шифрования $K=(x,y)$, используя алгоритм Диффи-Хеллмана на основе эллиптических кривых, если кривая имеет вид $y^2 = x^3 + 2x + 2 \; mod 17$. Примитивный элемент равен $P=(5,1)$. Секретный ключ Алисы $c=3$, секретный ключ Боба $d=10$.

Приложение № 3

ПРИМЕРЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

1. Используя расширенный алгоритм Евклида, найти мультипликативную инверсию числа 11 в Z_{26}.

2. *a = 161* и *b = 28*, найти *НОД (a, b).*

3. Выполните следующие операции:
   а. сложить *17* и *27* в Z_{14}
   б. вычесть *43* из *12* в Z_{13}
   в. умножить *123* на *–10* в Z_{19}

4. Используя свойства mod, вычислить:

(1723345+2124945) mod 11 =(8+9) mod 11 =6
(1723345–2124945) mod 11 =(8–9) mod 11 =10
(1723345×2124945) mod 11 =(8×9) mod 11 =6

5. Дана группа $G = <Z_6, \times>$, из нее получить циклические подгруппы.

6. Пусть существуют группы $H=<Z_{10},+>$ и $G=<Z_{12},+>$. Можно ли утверждать, что группа *H* подгруппа группы *G*?

7. Зашифровать сообщение *"happy"* в Z_{26} аддитивным шифром с ключом = *114.*

8. Дана группа $G=<Z_{10^*}, \times>$, получить для нее циклические подгруппы.

9. Злоумышленнику удалось получить зашифрованный текст *"NGVVEHOXZNJGEZUEUA*". Применяя атаку грубой силы, взломать шифр.

10. Используя вертикальную перестановку, зашифровать свою фамилию, используя числовой ключ *(5,1,4,7,2,6,3).*

11. Используя вертикальную перестановку, зашифровать сообщение *Enemy attacks tonight.* Ключ шифрования *(3,1,4,5,2).*

12. Используя шифр изгороди, зашифровать сообщение *Meet me at the park.*

13. Зашифровать слово *HELP* по алгоритму Хилла. Кодирующая матрица

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

14. С помощью таблицы Виженера зашифровать свою фамилию, используя в качестве ключевого слова свое имя.

15. С помощью шифра Плейфера зашифровать фразу *автором метода является Уитстон.* Ключевое слово – *командир.*

16. С помощью автоключевого шифра с начальным ключевым значением $k_1 = 12$ зашифровать сообщение *"Attack is today"*.

17. С помощью аффинного шифра расшифровать сообщение *"XCVVW"* в Z_{26} с ключевой парой *(α=3, β=2).*

18. Пусть удалось перехватить зашифрованный текст *XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW.* Найти исходный текст, применив статистическую атаку. Таблицу частоты символов взять у преподавателя.

19. Найти порядок точки *P(0,1)* в группе эллиптической кривой $y^2=x^3+1$ над полем *GF(5).*

20. Определить ключи шифра Цезаря, если известны следующие пары открытый текст – шифротекст: а. АПЕЛЬСИН – САЦЬНВЩЮ,

Приложение № 4

ВОПРОСЫ К ЭКЗАМЕНУ (семестр 8)

1. Модульная арифметика. Система вычетов Z_n.
2. Основные понятия теории чисел, применяемые в криптографии (основная теорема арифметики, функция Эйлера, теорема Ферма, теорема Эйлера).
3. Простой и расширенный алгоритм Евклида. Вычисление наибольшего общего делителя.
4. Аддитивная и мультипликативная инверсии.
5. Алгебраические структуры. Группы, кольца, поля.
6. Циклические группы. Циклические подгруппы.
7. Поля $GF(p^n)$.
8. Понятие шифрования. Шифры подстановки. Криптоанализ.
9. Моноалфавитные шифры. Аддитивный, мультипликативные, аффинный шифры.
10. Многоалфавитные шифры. Автоключевой шифр.
11. Бесключевые шифры перестановки и ключевые шифры перестановки.
12. Блочный шифр и его компоненты.
13. Рассеивание и перемешивание. Раунды.
14. Структура DES.
15. Функция DES. Генерация ключей.
16. Шифр Плейфера.
17. Шифр Хилла.
18. Шифр Вернама.
19. Энтропия Шеннона.
20. Модифицированный шифр Цезаря.
21. Шифр Магма.
22. Применение хеш-функций для проверки истинности сообщений.
23. Шифр Шамира.
24. Электронная цифровая подпись. Компоненты ЭЦП.
25. Электронная цифровая подпись. Формирование цифровой подписи.
26. Электронная цифровая подпись. Проверка цифровой подписи.
27. Схема цифровой подписи RSA.
28. Схема электронной подписи Эль-Гамаля (EGSA).
29. Алгоритмы с открытыми ключами RSA. Общие положения криптосистем с открытым ключом.
30. Алгоритмы рюкзака.
31. Алгоритм Диффи-Хеллмана.
32. Выбор эллиптической кривой и базовой точки.
33. Алгоритм Диффи-Хеллмана на эллиптических кривых ECDH.
34. Сложение точек на эллиптических кривых.
35. Генерация ключа в ECDH.

ПРИМЕРЫ К ЭКЗАМЕНУ (семестр 8)

1. Зашифровать и расшифровать слово *Криптография* с помощью алгоритма рюкзака. Закрытый ключ подобрать самостоятельно.

2. Зашифровать с помощью алгоритма *RSA* сообщение *CAB*. Исходные данные*: p=3, q=11, d=3, e=7*; ключ *{7,33}*. Сообщение представить в виде последовательности цифр, соответствующих положению букв в алфавите *(A=1, B=2, C=3)*.
3. Сгенерировать общий секретный ключ по алгоритму Диффи-Хеллмана. Исходные данные: *p=23, q=5*, у абонента А секретный ключ *a=6,* у абонента В секретный ключ *b=15*.
4. С помощью алгоритма рюкзака зашифровать свою фамилию. Открытый ключ – (62,93,186, 403, 417, 352, 315, 210).
5. Алгоритм Фейстеля. Шифруемая последовательность – последовательность *123456ABCD132536*. Получить L_0 *и* R_0.
6. Алгоритм Фейстеля. Имеется исходный ключ *AABB09182736CCDD*. Сгенерировать ключи 1-го и 2-го раундов и представить их в 16-чном виде.
7. Найти порядок точки *P(0,1)* в группе эллиптической кривой $y^2=x^3+1$ над полем *GF(5)*.
8. Вычислить в группе $E_{11}(1,6)$: *а) (8,3)+(3,6); б) 2(1,8)*.
9. Найти порядок точки *P(9,4)* в группе эллиптической кривой $E_{11}(6,3)$.
10. Для алгоритма ЭЦП ГОСТ Р34.10-94 выбраны следующие общие параметры: p = 22921, q = 191, a = 9281. Секретный ключ пользователя – автора документа x = 100. Найти открытый ключ, вычислить и проверить подпись длясообщения m = «Happy New Year»