Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление подготовки / специальность: Прикладная математика и информатика
Профиль / специализация: Математическое моделирование и вычислительная математика
Дисциплина: Эллиптические системы в криптографии

Формируемые компетенции: ОПК-4

ПК-3

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения не ниже порогового

Шкалы оценивания компетенций при сдаче зачета

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Пороговый уровень	Обучающийся: - обнаружил на зачете всесторонние, систематические и глубокие знания учебно-программного материала; - допустил небольшие упущения в ответах на вопросы, существенным образом не снижающие их качество; - допустил существенное упущение в ответе на один из вопросов, которое за тем было устранено студентом с помощью уточняющих вопросов; - допустил существенное упущение в ответах на вопросы, часть из которых была устранена студентом с помощью уточняющих вопросов	Зачтено
Низкий уровень	Обучающийся: - допустил существенные упущения при ответах на все вопросы преподавателя; - обнаружил пробелы более чем 50% в знаниях основного учебно-программного материала	Не зачтено

Описание шкал оценивания
Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения		
	Не зачтено		Зачтено

Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Владеть	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей

2. Перечень вопросов и задач к экзаменам, зачетам, курсовому проектированию, лабораторным занятиям.

Примерный перечень вопросов к зачету

Компетенция ПК-3, ОПК-4:

1. Является ли линейное представление НОД двух чисел единственных и почему?
2. Каков геометрический смысл сложения точек на кривой?
3. В чем заключается процедура композиции точек на кривой?
4. Перечислите основные параметры эллиптической кривой? На что влияет их качественный выбор?
5. В чем заключается операция дискретного логарифмирования на кривой?
6. Перечислите правила сложения точек на эллиптической кривой.
7. Что такое порядок эллиптической кривой? Каким должен быть порядок кривой для обеспечения стойкости алгоритмов шифрования?
8. Что такое квадратичный вычет? Как применяются квадратичные вычеты для вычисления порядка кривой?
9. Что показывает символ Лежандра? Как он используется для вычисления порядка кривой?
10. Сформулируйте теорему Хассе. Доказательство теоремы Хассе.
11. Что такое след Фробениуса? Как его можно применить для вычисления порядка кривой?
12. Сформулируйте китайскую теорему об остатках и ее применении для вычисления порядка кривой.

13. К какому классу шифров относится шифр Эль-Гамаля на ЭК?
14. Каким ключом шифруется сообщение в системе Эль-Гамаля?
15. Какую проблему нужно решить криптоаналитику для вскрытия схемы Эль-Гамаля на ЭК?
16. Почему для шифрования в схеме Эль-Гамаля каждый раз должно использоваться новое значение k?
17. В чем разница между классической схемой Эль-Гамаля и той же схемой, основанной на эллиптических кривых?
18. Что служит ключом в системе Диффи-Хеллмана?
19. Какова цель обмена ключами?
20. Что знают абоненты о ключах друг друга и что остается в секрете?
21. Какие параметры криптосистемы выбираются абонентами открыто?
22. Что получают абоненты в результате обмена ключами?
23. В чем разница между классическим протоколом Диффи-Хэллмана и его аналогом на эллиптических кривых?
24. Какие задачи решает ЭЦП?
25. Имеет ли смысл ставить ЭЦП на незашифрованные данные?
26. Сколько ключей используется в механизме ЭЦП?
27. Каким ключом ставится ЭЦП на сообщение?
28. Каким ключом проверяется подлинность ЭЦП?
29. В чём заключается процедура проверки подлинности ЭЦП?
30. Что такое коллизия хэш-образа? Методы борьбы с коллизиями.
31. Для чего используется хэш-функции на практике?
32. Как называется хэш-образ, полученный с применением закрытого ключа шифрования?
33. Что такое хэширование?
34. В чем заключается стандартная схема генерации хэш-образа?
35. Схема алгоритма ρ-Поларда проверки чисел на простоту.
36. Схема алгоритма Голдвассер—Килиана.
37. Аналогом какого алгоритма является алгоритм факторизации Ленстры на ЭК. Объясните суть этого алгоритма. В чем различие?
38. Суть алгоритма факторизации Ленстры? В чем преимущество метода?
39. Как используется понятие гладкости целого числа в алгоритме Ленстры?
40. Какие существуют алгоритмы факторизации, основанные на эллиптических кривых? Объяснить основную идею одного из них.
41. Приведите оценку сложности и трудоемкости алгоритма Ленстры на ЭК. От чего она зависит?
42. Какие усовершенствования известны для классического алгоритма Ленстры на ЭК? В чем они заключаются?
43. Применение алгоритмов шифрования, основанных на эллиптических кривых, и вычисления электронно-цифровой подписи, выполненной по стандартам ГОСТ 34.10-2001 и ГОСТ 34.10-2012, для решения задач построения криптосистем

3. Тестовые задания. Оценка по результатам тестирования.

3.1. Примерные задания теста

Задание 1 (ПК-3, ОПК-4)
Выберите правильный вариант ответа.
Условие задания: Выбрать правильный ответ
Цель атаки на криптосистему

- ☑ нарушение целостности передачи информации абоненту
- ☐ вскрытие ключа шифрования
- ☐ фальсификация сообщения
- ☐ вскрытие передаваемых зашифрованных сообщений

Задание 2 (ПК-3, ОПК-4)
Приведите в возрастающей последовательности последовательность действий при авторизации пользователя в системе

1: регистрация пользователя и идентифицирующей его информации
2: получение информации о пользователе при его входе в систему
3: сравнение характеристик введенной пользователем информации при входе в систему с зарегистрированной
4: предоставление доступа к системе или отказ в доступе

Задание 3 (ПК-3, ОПК-4)
Приведите соответствие между видами атак и информацией, которой обладает злоумышленник

атака с использованием только шифротекста	у криптоаналитика есть шифротексты нескольких сообщений, зашифрованных одним и тем же алгоритмом шифрования;
атака с использованием открытого текста	криптоаналитик имеет доступ ко всем или некоторым зашифрованным сообщениям и соответствующим им исходным текстам;
атака с использованием выбранного открытого текста	у криптоаналитика есть временный доступ не только к шифротекстам и открытым текстам, но и возможность выбирать исходный текст и получать для него шифрованный текст;
атака с использованием выбранного шифротекста	криптоаналитик имеет временный доступ к процессу расшифровки и может выбирать зашифрованные сообщения и получать для них исходные тексты с целью определить ключ шифрования;

Задание 4 (ПК-3, ОПК-4)
Вставить число
Разрядность 3DES равна ____ бит.
Правильные варианты ответа: 112;

Полный комплект тестовых заданий в корпоративной тестовой оболочке АСТ размещен на сервере УИТ ДВГУПС, а также на сайте Университета в разделе СДО ДВГУПС (образовательная среда в личном кабинете преподавателя).
Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета, курсового проектирования.

Оценка ответа обучающегося на вопросы зачета

Элементы оценивания	Содержание шкалы оценивания			
	Не зачтено	Зачтено	Зачтено	Зачтено
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	1. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.