**Программа учебной дисциплины «Теоретическая криптография»**

Утверждена

Академическим советом ООП

Протокол № \_\_\_\_\_от «\_\_»\_\_\_\_\_\_\_20\_\_ г.

|  |  |
| --- | --- |
| Автор | С. Н. Федоров |
| Число кредитов |  |
| Контактная работа (час.) | 64 |
| Самостоятельная работа (час.) | 126 |
| Курс |  |
| Формат изучения дисциплины | Без использования онлайн курса |

1. **ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ**

Целями освоения дисциплины «Теоретическая криптография» является освоение студентами основных положений математической теории криптографии.

В результате освоения дисциплины студент должен:

**знать:**

- определения основных понятий теоретической криптографии;

- формулировки основных результатов теоретической криптографии;

- примеры криптографических протоколов (криптографических схем) и задач, которые они решают;

**уметь:**

- анализировать корректность обоснований стойкости криптографических протоколов;

- математически строго формулировать требования к стойкости криптографических протоколов (схем);

- строить математические модели криптографических средств защиты информации;

**владеть:**

-навыками оперирования основными криптографическими понятиями;

- техниками вывода утверждений о возможности/невозможности криптографической защиты информации в тех или иных условиях.

Изучение дисциплины «Теоретическая криптография» базируется на следующих дисциплинах:

- информатика (computer science) и дискретная математика;

- теория вероятностей;

- алгебра и теория чисел.

Для освоения учебной дисциплины студенты должны владеть следующими знаниями и компетенциями:

- умение строить строгие математические определения и рассуждения;

- знание содержания курсов информатики (computer science) и дискретной математики;

- владение основными понятиями таких разделов математики, как теория вероятностей, общая алгебра, теория чисел.

1. **СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Тема 1. Из истории криптографии.**

Примеры систем шифрования с античности до начала XX века. Шифр Вернама. Начало криптографии как науки. «Новые направления криптографии» (1970-е гг.), примеры криптографических протоколов (протокол Диффи—Хеллмана, криптосистема Эль-Гамаля, криптосистема RSA, схема подписи RSA, схема разделения секрета Блэкли, протокол Блюма подбрасывания монеты по телефону).

**Тема 2. Предмет теоретической криптографии.**

Три задачи криптографии. Криптографические протоколы. Криптографические примитивы. Модель противника. Понятие стойкости. Криптосинтез и криптоанализ.

**Тема 3. Основные положения теории Шеннона.**

Системы связи с секретностью. Критерии оценки таких систем. Априорные и апостериорные вероятности. Совершенная секретность и ее необходимое условие. Энтропия как мера неопределенности. Расстояние единственности. Идеальные системы.

**Тема 4. Элементы теории сложности вычислений.**

Вычислительная задача: распознавательный и поисковый варианты (язык и отношение). Однородная и неоднородная модели вычислений: машина Тьюринга (детерминированная, недетерминированная, вероятностная, с оракулом) и семейство булевых схем. Тезисы Тьюринга—Чёрча и Эдмондса. Классы сложностей DTIME, P, EXP, NP, BPP, RP, PSPACE, P/poly и их соотношения. Теоремы о распознаваемости языков из P/poly семейством схем полиномиального размера и о соотношении классов BPP и P/poly.

**Тема 5. Односторонняя функция и трудный предикат.**

Сильно и слабо односторонние функции. Теорема Яо. Односторонние семейства функций. Дискретная экспонента как кандидат в односторонние функции. Трудный предикат для функции. Теорема Гольдрайха—Левина.

**Тема 6. Генераторы псевдослучайных последовательностей.**

Два определения криптографически стойкого генератора псевдослучайных последовательностей. Теорема Яо об эквивалентности этих определений. Теорема о «растягивании» выхода псевдослучайного генератора. Теорема Хостада—Импальяццо—Левина—Луби.

**Тема 7. Криптосистемы с секретным ключом.**

Определение. Блоковые и потоковые криптосистемы. Модель противника (варианты атак и угроз). Пример определения стойкости и (гипотетический) пример стойкой криптосистемы. Необходимое и достаточное условие существования стойких криптосистем.

**Тема 8. Криптографические хэш-функции.**

Определения семейства хэш-функций с трудно обнаружимыми коллизиями и одностороннего семейства хэш-функций. Лемма об *l*-композиции. Теорема об *l*(*n*)-композиции. Теорема Наора—Юнга. Теорема Ромпеля для хэш-функций.

**Тема 9. Схемы электронной подписи.**

Определение и пример. Модель противника (варианты атак и угроз). Пример определения стойкости. Одноразовая схема Лэмпорта, преобразование её в многоразовую. Теорема Ромпеля о стойкой схеме электронной подписи.

**Тема 10. Доказательства с нулевым разглашением.**

Интерактивное доказательство. Свойство нулевого разглашения (три варианта определения). Классы сложностей IP, ZK, SZK, PZK. Теорема Гольдрайха—Микали—Вигдерсона. Интерактивное доказательство с нулевым разглашением для языка ИЗОМОРФИЗМ ГРАФОВ. Протокол привязки к биту.

**Тема 11. Криптосистемы с открытым ключом.**

Определение, пример. Атаки и угрозы. Семейства функций с секретом. Достаточное и необходимое условия существования стойких криптосистем с открытым ключом. Семейство функций Рабина как гипотетический пример семейства функций с секретом. Полиномиальная стойкость. Криптосистема Гольдвассер—Микали.

**Тема 12. Системы электронных платежей.**

Общая схема. Задача неотслеживаемости. Схема подписи вслепую.

1. **ОЦЕНИВАНИЕ**

В целях текущего контроля в рамках курса слушателям предлагается выполнить контрольную работу и домашние задания. Контрольная работа оценивается по 10-балльной шкале (*ОКР*). Каждое домашнее задание оценивается по 10-балльной шкале, общая оценка за домашние задания (*ОДЗ*) является средним арифметическим оценок за каждое отдельное домашнее задание.

Итоговый устный экзамен оценивается по 10-балльной шкале (*ОЭ*).

Результирующая оценка по учебной дисциплине вычисляется округлением значения

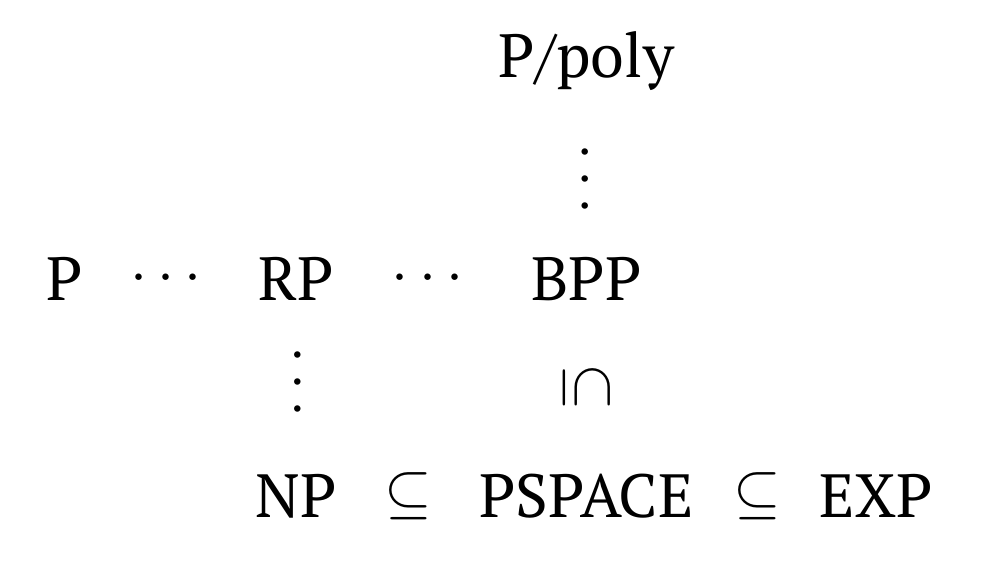
0,8·*ОЭ* + 0,1·*ОДЗ* + 0,1·*ОКР*,

то есть *Орезульт* = ⌊0,8·*ОЭ* + 0,1·*ОДЗ* + 0,1·*ОКР* + 0,5⌋ (целая часть числа в скобках).

1. **ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ**

Промежуточный контроль проводится с помощью письменной контрольной работы и домашних заданий. В конце учебного периода проводится устный экзамен.

**Варианты заданий для письменной контрольной работы**

* Дополните диаграмму недостающими знаками ⊆ нестрогого вложения между сложностными классами (вместо многоточий). Выбор знака обоснуйте.
* Докажите, что если односторонняя функция существует, то классы P и NP не совпадают. (Постройте язык, зависящий от односторонней функции, который принадлежит NP, но не P.)
* Пусть *f* — перестановка. Докажите, что если для *f* существует трудный предикат, то *f* — односторонняя.

**Примерные варианты домашних заданий**

* Придумайте пороговую схему разделения секрета (так чтобы любые t участников вместе могли вычислить секрет, а t – 1 уже нет). (Например, воспользуйтесь интерполяционным многочленом Лагранжа.)
* В определении (сильно) односторонней функции не будем подавать на вход машине *A* строку 1*n*. Приведите пример функции, удовлетворяющей такому «испорченному» определению, но не являющуюся трудно инвертируемой в интуитивном понимании этого термина.
* Пусть *f* — односторонняя перестановка. Постройте криптографически стойкий генератор псевдослучайных последовательностей (воспользуйтесь теоремой Гольдрайха—Левина). Обоснуйте конструкцию.
* Докажите, что класс IP содержит NP и сам содержится в PSPACE.

**Вопросы к устному экзамену**

1. Сильно и слабо односторонние функции. Теорема Яо об эквивалентности предположений о существовании сильно и слабо односторонних функций. Дискретная экспонента как кандидат в односторонние функции.
2. Трудный предикат для функции. Теорема Гольдрайха—Левина о существовании у односторонней функции трудного предиката.
3. Два определения генератора псевдослучайных последовательностей — через неотличимость от равномерно распределенных последовательностей и через непредсказуемость следующего бита. Теорема Яо об эквивалентности этих определений.
4. Построение генератора псевдослучайных последовательностей с помощью произвольной односторонней перестановки. Теорема Хостада—Импальяццо—Левина—Луби о существовании генераторов псевдослучайных последовательностей (доказательство достаточного условия — только для случая односторонней перестановки).
5. Криптосистемы с секретным ключом. Блоковые и потоковые криптосистемы. Атаки на криптосистемы и угрозы безопасности криптосистем. Определение стойкости криптосистемы.
6. Доказательство существования стойкой потоковой криптосистемы с секретным ключом в предположении существования генератора псевдослучайных последовательностей.
7. Определения семейства односторонних хэш-функций и семейства функций с трудно обнаружимыми коллизиями. Теорема Наора—Юнга о существовании семейства односторонних хэш-функций при условии существования односторонней перестановки.
8. Определение схемы электронной подписи. Атаки на схемы электронной подписи и угрозы их безопасности. Определение стойкости схемы электронной подписи. Схема Лэмпорта. Теорема Ромпеля о существовании стойких схем электронной подписи (без доказательства).
9. Определение протокола интерактивного доказательства для языка. Свойство нулевого разглашения: вычислительное, статистическое, абсолютное. Теорема Гольдрайха—Микали—Вигдерсона о существовании протоколов доказательства с нулевым разглашением для всех языков из класса NP (без доказательства).
10. Определение криптосистемы с открытым ключом. Атаки и угрозы для криптосистем с открытым ключом. Семейства функций с секретом. Условия существования стойких криптосистем с открытым ключом.
11. Семейство функций Рабина как гипотетический пример семейства функций с секретом.
12. Полиномиальная стойкость систем вероятностного шифрования. Конструкция Гольдвассер—Микали как гипотетический пример стойкой в этом смысле криптосистемы.
13. Системы электронных платежей. Понятие неотслеживаемости и другие требования к системе.

**Дополнительные вопросы на устном экзамене**

1. Классы сложностей P, NP, RP, BPP, EXP, P/poly, IP, ZK и их соотношения.
2. Протокол Диффи—Хеллмана.
3. Криптосистема Эль-Гамаля.
4. Криптосистема RSA.
5. Схема электронной подписи RSA.
6. Протокол доказательства с абсолютно нулевым разглашением (например, для языка ИЗОМОРФИЗМ ГРАФОВ).
7. Протокол привязки к биту (bit commitment).
8. Протокол неведомой передачи (oblivious transfer).
9. Схема электронной подписи вслепую (blind signature).

**Задачи на устном экзамене** аналогичны заданиям на контрольной работе и домашним заданиям.

1. **РЕСУРСЫ**
   1. **Основная литература**
2. O. Goldreich. Foundations of cryptography: Volume 1 (Basic tools). — Cambridge, UK: Cambridge University Press, 2001. —   
   URL: http://www.wisdom.weizmann.ac.il/~oded/foc-vol1.html
3. O. Goldreich. Foundations of cryptography: Volume 2 (Basic applications). — Cambridge, UK: Cambridge University Press, 2004. —   
   URL: http://www.wisdom.weizmann.ac.il/~oded/foc-vol2.html
4. S. Goldwasser, M. Bellare. Lecture notes on cryptography. —   
   URL: http://cseweb.ucsd.edu/users/mihir/papers/gb.pdf
5. M. Luby. Pseudorandomness and cryptographic applications. — Princeton, New Jersey: Princeton University Press, 1996. —   
   URL: https://books.google.ru/books?hl=en&lr=&id=1eI9DwAAQBAJ — Google Books
6. М. И. Анохин. Введение в математическую криптографию. Математическая криптография: Конспект лекций. — 2017. —   
   URL: http://cryptography.ru/info/курс\_лекций\_м-\_и-\_анохина
7. Н. П. Варновский. Курс лекций по математической криптографии: (Предварительная версия). — 2009. —   
   URL: http://cryptography.ru/wp-content/uploads/2014/11/varn\_lectures\_long.pdf
   1. **Дополнительная литература**
8. Ященко, В. В. Введение в криптографию / В. В. Ященко, Н. П. Варновский, Ю. В. Нестеренко и др.; Под ред. В. В. Ященко . – Изд. 4-е, доп. – М.: МЦНМО, 2012. – 347 с. - ISBN 978-5-443-90026-1.
9. Гэри, М. Вычислительные машины и труднорешаемые задачи / М. Гэри, Д. Джонсон; Пер. с англ. Е. В. Левнера, М. А. Фрумкина; Под ред. А. А. Фридмана. – М.: Мир, 1982. – 416 с.
10. Н. Н. Писарук. Сложность вычислений и криптография: (Предварительная версия). — Минск, 1999. — URL: http://pisaruk.narod.ru/books/complexity.pdf
    1. **Программное обеспечение**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Условия доступа** |
| 1. |  |  |

* 1. **Профессиональные базы данных, информационные справочные системы,   
     интернет-ресурсы (электронные образовательные ресурсы)**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Условия доступа** |
|  | ***Профессиональные базы данных, информационно-справочные системы*** | |
| 1. |  |  |
| 2. |  |  |
|  | ***Интернет-ресурсы (электронные образовательные ресурсы)*** | |
| 1. |  |  |

* 1. **Материально-техническое обеспечение дисциплины**

Учебные аудитории для лекционных занятий по дисциплине обеспечивают представление материала, соответствующего программе дисциплины в составе:

белая маркерная доска;

маркеры для белых досок;

губка-стиратель для маркерных досок.