Федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В.ЛОМОНОСОВА»

ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

УТВЕРЖДАЮ

Декан факультета ВМК МГУ
академик РАН

/*И.А. Соколов*/

«20» июня 2022 г.

ПРОГРАММА-МИНИМУМ

кандидатского экзамена по специальности

2.3.6. Методы и системы защиты информации, информационная безопасность

Область науки: 1. Естественные науки

Группа научных специальностей: 1.1. Математика и механика

Отрасль науки: физико-математические науки

Москва 2022

I. Описание программы

Настоящая программа разработана на основе паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» и охватывает основополагающие разделы в области методов и систем защиты информации, информационной безопасности и криптографии, а также в области применения аппарата математических методов и алгоритмов при решении задач информационной безопасности, защиты информации и криптографии.

II. Основные разделы и вопросы к экзамену

1. **Математические основы защиты информации:**
   - 1.1. Группы. Кольца и поля. Многочлены. Расширения полей.
   - 1.2. Конечные поля: характеризация конечных полей, корни неприводимых многочленов. Следы, нормы и базисы. Корни из единицы и круговые многочлены. Представления элементов конечных полей.
   - 1.3. Многочлены над конечными полями. Порядки многочленов и примитивные многочлены, неприводимые многочлены. Построение неприводимых многочленов. Линеаризованные многочлены.
   - 1.4. Линейные рекуррентные последовательности. Регистры сдвига с обратной связью. Периодичность. Характеристический многочлен. Производящие функции. Характеризация линейных рекуррентных последовательностей. Распределение элементов в линейных рекуррентных последовательностях. Алгоритм Берлекемпа—Месси.
   - 1.5. Целочисленные решётки. Фундаментальный параллелепипед. Базисы решётки. Короткие векторы решётки. LLL-приведённый базис решётки. LLL-алгоритм, обоснование его корректности, его вычислительная сложность.
   - 1.6. Коды, исправляющие ошибки. Сложные задачи в теории кодов, исправляющих ошибки: задача синдромного декодирования и её NP-полнота, задача о спектре весов и её NP-полнота, задача об эквивалентности линейных кодов и её связь с задачей об изоморфизме графов.

2. **Криптография с секретным ключом: блочные и поточные шифры, хеш-функции:**
   - 2.1. Общие принципы построения криптосистем с секретным ключом. Совершенная секретность, энтропия.

2.2. Псевдослучайные функции и псевдослучайные перестановки. IND-CPA стойкая криптосистема с секретным ключом.

2.3. Сеть Фейстеля и её свойства. Шифры, построенные на основе сетей Фейстеля: DES и Магма.

2.4. Булевы функции и отображения. Преобразование Уолша—Адамара булевой функции. Быстрое преобразование Уолша—Адамара. Спектральные характеристики булевых функций и их основные свойства. Основные криптографические свойства булевых функций: максимальная нелинейность, корреляционная иммунность и устойчивость, совершенная уравновешенность, алгебраическая иммунность. Дифференциальный криптоанализ и линейный криптоанализ. Устойчивость узлов замены блочных шифров к дифференциальному и линейному криптоанализу в терминах свойств булевых отображений.

2.5. Синтез и анализ поточных шифров. Поточные шифры, построенные на основе регистров сдвига с линейными обратными связями. Линейная сложность. Нелинейные фильтрующие генераторы. Нелинейные комбинирующие генераторы.

2.6. Криптографические хеш-функции и их приложения. Основные методы криптоанализа хеш-функций, применения парадокса о днях рождения. Построение итерационных хеш-функций на основе блочных шифров, криптоанализ общей схемы.

3. **Криптография с открытым ключом: криптосистемы с открытым ключом и протоколы электронной подписи:**

3.1. Односторонние функции с секретом. Понятие криптосистемы с открытым ключом. IND-CPA стойкая криптосистема с открытым ключом, LR-CPA стойкая криптосистема с открытым ключом и многократное шифрование сообщений, IND-CCA стойкая криптосистема с открытым ключом.

3.2. Криптосистема Рабина и её стойкость в предположении сложности задачи целочисленной факторизации

3.3. Криптосистема RSA: обоснование корректности алгоритма расшифрования, полиномиальная эквивалентность задачи восстановления секретного ключа по открытому и задачи целочисленной факторизации, атака на основе связанных сообщений, эквивалентные секретные ключи, атака на повторное шифрование сообщений, теорема Винера и атака на малый показать расшифрования.

3.4. Задача целочисленной факторизации: ро-метод Полларда, факторизация Ферма и факторные базы, метод квадратичного решета.

3.5. Криптосистема Эль-Гамаля и её IND-CPA стойкость в предположении сложности распознавательной проблемы Диффи-Хеллмана.

3.6. Задача дискретного логарифмирования. Основные алгоритмы дискретного логарифмирования: большой шаг – малый шаг, ро-метод Полларда, метод Полига—Хеллмана.

3.7. Криптосистема Меркла—Хеллмана, атака на неё с использованием LLL-алгоритма.

3.8. Криптосистема Мак-Элиса. Классическая криптосистема Мак-Элиса на основе кодов Гоппы. Коды Гоппы, определение, основные параметры, декодирование неприводимых кодов Гоппы, декодирование сепарабельных кодов Гоппы на основе алгоритма Берлекемпа—Месси. Атака на повторное шифрование одного сообщения. Алгоритм Штерна поиска слов небольшого веса Хемминга в коде, его сложность. Приложение алгоритма Штерна в криптографическом анализе криптосистемы Мак-Элиса.

3.9. Эллиптические кривые: основные понятия. Протокол Диффи—Хеллмана на эллиптических кривых.

3.10. Протоколы электронной-цифровой подписи. Угрозы схемам электронной подписи.

3.11. Основные протоколы электронной подписи: RSA, протокол Меркла—Лемпорта, протокол Эль-Гамаля на эллиптических кривых.

4. **Компьютерная безопасность**

4.1. Определение политики безопасности. Дискреционная политика. Политика MLS. Математические методы анализа политики безопасности. Модель «take-grant», модель Белла-Лападула, модель LWM, модель невлияния и автоматный подход

4.2. Защита компьютерных систем от удаленных атак через сеть Internet. Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

III. Основная литература

1. Лидл Л., Нидеррайтер Г. Конечные поля. Том 1 / Л. Лидл, Г. Нидеррайтер, Москва: Мир, 1988. 430 с.

2. Лидл Л., Нидеррайтер Г. Конечные поля. Том 2 / Л. Лидл, Г. Нидеррайтер, Москва: Мир, 1988. 430 с.

3. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography. CRC Press, 1996

4. D. Stinson, Cryptography: Theory and Practice. 4th Edition, CRC Press, 2019.

5. Rainer A.Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986

6. Смарт Н. Криптография / Н. Смарт, Москва: Техносфера, 2005. 528 с.

7. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц, Москва: Научное изд-во ТВП, 2001. 254 с.

8. Berson T. A. Failure of the McEliece public-key cryptosystem under message-resend and related-message attack Lecture Notes in Computer Science / под ред. B. S. Kaliski, Berlin, Heidelberg: Springer, 1997.С. 213–220.

9. Болотов А. А. [и др.]. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основны / А. А. Болотов, С. Б. Гашков, А. Б. Фролов, А. А. Часовских, Москва: КомКнига, 2006. 328 с.

10. Болотов А. А. [и др.]. Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов, А. А. Часовских, Москва: КомКнига, 2006. 280 с.

11. Goldreich O. Foundations of Cryptography Basic Tools / O. Goldreich, Cambridge University Press, 2004.

12. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник / Тилборг ван Х.К.А., Москва: Мир, 2006. 471 с.

13. Katz J., Lindell Y. Introduction to Modern Cryptography, Second Edition / J. Katz, Y. Lindell, 2nd-е изд., Chapman & Hall/CRC, 2014.

14. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. Изд. центр «Академия», 2009.

15. Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. Москва: ЛЕНАНД, 2015, 576 страниц.

16. Ф. Дж. Мак-Вильямс, Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн, под ред. Л. А. Бассалыго, перевод И. И. Грушко, В. А. Зиновьев, Москва: Связь, 1979. 744 с.

17. Stern J. A method for finding codewords of small weight под ред. G. Cohen, J. Wolfmann, Springer Berlin Heidelberg, 1989.С. 106–113.

18. Preneel B. Analysis and Design of Cryptographic Hash Functions, PhD Thesis, 1993, http://www.esat.kuleuven.ac.be/~pretieel/phd_preneel_febl993.pdf

19. Столлингс В. Криптография и защита сетей. Принципы и практика.

Москва, Санкт- Петербург, Киев: Издательский дом «Вильямс», 2-е издание, 2001.

20. Berlekamp E., McEliece R. J., Tilborg H. C. van On the Inherent Intractability of Certain Coding Problems // Information Theory, IEEE Transactions on. 1978. No 3 (24). С. 384–386.

21. Repka M., Zajac P. Overview of the Mceliece Cryptosystem and its Security // Tatra Mountains Mathematical Publications. 2014. No 1 (60). С. 57–83.

22. Черепнёв, М. А. Криптографические протоколы: учебное пособие, Москва: МАКС Пресс, 2018, 125 с.

IV. Дополнительная литература

1. N. Koblitz: Algebraic Aspects of Cryptography, Vol.3, Algorithms and Computation in Mathematics, Springer-Verlag, 1998.

2. W. Patterson, Mathematical Cryptology for Computer Scientists and Mathematicians Rowman and Littlefield Publishers, 1987

3. Применко Э.А. Алгебраические основы криптографии. М: Либроком, 2013, 288 с

4. M.Grötschel, L. Lovasz, and A. Schrijver, Geometric Algorithms and Combinatorial Optimization, 2nd edition, Springer-Verlag, 1993.

5. J. Buchmann, Introduction to Cryptography, Springer-Verlag, New York, 2000.

6. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. Москва : МЦНМО, 2014, 334 с.

7. Введение в теоретико-числовые методы криптографии: учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090101 "Криптография" / М. М. Глухов, И. А. Круглов, А. В. Пичкур, А. В. Черемушкин. - Санкт-Петербург ; Москва : Лань, 2011. - 394 с.

8. Основы криптографии: учебное пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. - Москва : Гелиос АРВ, 2001. – 478 с.

9. Аверченков В. И. Криптографические методы защиты информации: учебное пособие. - 2-е издание, стереотипное. - Москва: «ФЛИНТА», 2017. - 214 с.

V. Автор программы

– Доцент кафедры информационной безопасности, к.ф.-м.н. Чижов Иван Владимирович

VI. Критерии оценивания

Критерии и показатели оценивания ответа на экзамене			
2	3	4	5
Неудовлетворительно	**Удовлетворительно**	**Хорошо**	**Отлично**
Фрагментарные знания актуальных проблем и тенденций в области методов и систем защиты информации, информационной безопасности и криптографии, а также в применении аппарата математических методов и алгоритмов при решении задач информационной безопасности, защиты информации и криптографии.	Неполные знания актуальных проблем и тенденций в области методов и систем защиты информации, информационной безопасности и криптографии, а также в применении аппарата математических методов и алгоритмов при решении задач информационной безопасности, защиты информации и криптографии.	Сформированные, но содержащие отдельные пробелы знания актуальных проблем и тенденций в области методов и систем защиты информации, информационной безопасности и криптографии, а также в применении аппарата математических методов и алгоритмов при решении задач информационной безопасности, защиты информации и криптографии.	Сформированные и систематические знания актуальных проблем и тенденций в области методов и систем защиты информации, информационной безопасности и криптографии, а также в применении аппарата математических методов и алгоритмов при решении задач информационной безопасности, защиты информации и криптографии.