Кафедра ИБ

Вопросы к государственному экзамену
Магистерская программа
«Информационная безопасность компьютерных систем» (гр. 619/1)

1. Односторонние функции. Сильно и слабо односторонние функции, теорема Яо о связи между ними. Дискретная экспонента как пример гипотетической односторонней функции.
2. Криптографически стойкий генератор псевдослучайных последовательностей. Два определения стойкости псевдослучайных генераторов и их эквивалентность. Трудный предикат функции. Теорема Гольдрайха–Левина (без доказательства). Построение псевдослучайного генератора из односторонней перестановки.
3. Доказательства с нулевым разглашением. Интерактивная пара машин Тьюринга. Протокол интерактивного доказательства. Три типа нулевого разглашения. Теорема о существовании доказательств с нулевым разглашением для всех языков из класса NP (идея доказательства).
4. Методы анализа блочных шифров. Понятия линейного и дифференциального анализа. 5. T-функции. Определение, основные свойства. T-функции как детерминированные функции автоматов с бинарным входом/выходом (с доказательством). T-функции как 1-липшицевы функции на пространстве целых 2-адических чисел (с доказательством).
5. T-функции, сохраняющие меру: критерии и достаточные условия для T-функций, в том числе и многих переменных (для равномерно дифференцируемых функций — с доказательством; в терминах рядов Малера и координатных функций — только формулировки). Латинские квадраты на основе T-функций (с доказательством) и их применение в псевдослучайных генераторах.
6. Эргодические T-функции: критерии и признаки эргодичности T-функций (для равномерно–дифференцируемых по модулю функций — формулировка, в терминах рядов Малера — формулировка и доказательство достаточности, в терминах координатных функций — с доказательством).
7. Криптосистема Рабина: алгоритм генерации ключей, функция шифрования и функция расшифрования. Обоснование корректности алгоритма расшифрования. Связь криптосистемы Рабина и задачи факторизации целых чисел.
8. Криптосистема RSA. Односторонняя функция RSA и односторонняя функция RSA с секретом. Теорема о связи односторонней функции RSA и задачи факторизации целых чисел. Проблема RSA.
9. Анализ криптосистемы RSA. Эквивалентные ключи. Теорема об описании класса эквивалентности секретного ключа. Итерация процесса шифрования. Оценка сложности.
10. Понятие криптосистемы с открытым ключом. Понятие криптосистемы с открытым ключом с неразличимым шифрованием. Понятие CPA-стойкой криптосистемы с открытым ключом. Теорема о том, что любая CPA–стойкая криптосистема с открытым ключом является CPA–стойкой в модели с возможностью многократного шифрования сообщений на одном ключе.
11. Доказательство CPA-стойкости криптосистемы Эль-Гамаля в предположениях сложности распознавательной задачи Диффи–Хеллмана.
12. Основные понятия теории линейных кодов: линейный код, порождающая и проверочная матрица, длина, размерность, кодовое расстояние. Граница Варшамова-Гильберта. Граница Синглтона.
13. Граница Хэмминга. Код Хэмминга. Утверждение о том, что только коды Хэмминга являются совершенными двоичными линейными кодами с кодовым расстоянием 3.
14. Задача кодирования источника информации. Граница энтропии как фундаментальная нижняя граница длины однозначно декодируемого кода. Рост вероятности ошибки кодирования при выборе скорости кода меньше величины энтропии.
15. Дискретный канал без памяти. Вероятность ошибки декодирования двоичного симметричного канала, интерпретация его функции ёмкости. Код с повторением.
16. NP-полнота задачи декодирования кода общего положения и задачи о спектре весов кода.
17. Постановка задачи о перестановочной эквивалентности двоичных линейных кодов. Доказательство того, что эта задача не может быть NP-полной, а также того, что она не проще, чем задача об изоморфизме графов.

18. Решение задачи декодирования кода общего положения на основе информационных множеств: описание алгоритма, оценка его сложности.
19. Понятие кодовой криптосистемы Мак-Элиса. Пример криптосистемы Мак-Элиса на кодах Хемминга, оценка сложности восстановления секретного сообщения с помощью алгоритма декодирования на основе информационных множеств.
20. Понятие кодовой криптосистемы Нидеррайтера. Теоремы об эквивалентности криптосистем Мак-Элиса и Нидеррайтера.
21. Архитектурные особенности современных микропроцессоров. Последовательная и параллельная сложность алгоритмов, информационный граф и ресурс параллелизма алгоритм.
22. Интерфейсы передачи данных (SPI, JTAG, UART) и особенности их работы. Практическая реализация передачи данных с помощью интерфейса UART. Снятие дампа с ИМС с помощью интерфейса UART.
23. Определение перечня дефектов безопасности с описаниями. Базовые метрики уязвимостей. Специализированные механизмы защиты.

Список рекомендованной литературы

[1] Введение в криптографию. Под общей редакцией В. В. Ященко. Издание 4-е, дополненное. МЦНМО, М. , 2012.

[2] O.Goldreich. Foundations of cryptography. Volume 1 (Basictools). Volume 2 (Basicapplications). Cambridge University Press, 2001 (v.1), 2004 (v. 2).

[3] M. Luby.Pseudorandomness and cryptographic applications. Princeton University Press, 1996. [4] S. Arora, B. Barak. Computational Complexity: A Modern Approach. Cambridge UniversityPress,USA 2009.

[4] Брюс Шнайер Прикладная криптография, «Издательство ТРИУМФ», 2002. [6] Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.Основы криптографии, 2004. [7] Х.К.А. ван Тилборг. Основы криптологии, МИР, 2006.

[5] Э.А. Применко. Алгебраические основы криптографии «Либроком» 2013. [9] О.А. Логачев, А.А. Сальников, В.В. Ященко. Булевы функции в теории кодирования и криптологии, МЦНМО, 2004.

[6] А.Чмора. Современная прикладная криптография, Гелиос АРВ, 2001.

[7] Р.Лидл, Г.Нидеррайтер. Конечные поля, т.1, т.2, МИР 1988.

[8] V.Anashin, A.Khrennikov. Applied Algebraic Dynamics. DeGruyter, Berlin, 2009 [13] V.Anashin. The Non-Archimedean Theory of Discrete Systems. Math. Comp. Sci. 2012,vol. 6, No 4, pp. 375–393

[9] Мак-Вильямс Ф. Д., Слоэн Д. Н. Теория кодов, исправляющих ошибки. Москва: Связь, 1979.

[10] Handbook of Coding Theory, volume I, chapter 7, pages 649–754. North-Holland(1998). [16] Виноградов И.М. Основы теории чисел. М.:Наука, 1990.-167с.

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

[12] Petrank E., Roth R. M. Is code equivalence easy to decide? // IEEE Transactions on Information Theory. 1997. № 5 (43). С. 1602–1604.

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

[14] Dhanjani, N., Chow, A., Ho, K., Leong, B., & Reyes, G. (2021). Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things. No Starch Press.

[15] OWASP Foundation. (2014). OWASP Testing Guide v4.