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).
6. 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.
7. 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).
8. Криптосистема Рабина: алгоритм генерации ключей, функция шифрования и функция расшифрования. Обоснование корректности алгоритма расшифрования. Связь криптосистемы Рабина и задачи факторизации целых чисел.
9. Криптосистема RSA. Односторонняя функция RSA и односторонняя функция RSA ссекретом. Теорема о связи односторонней функции RSA и задачи факторизации целых чисел. Проблема RSA.
10. Анализ криптосистемы RSA. Эквивалентные ключи. Теорема об описании класса эквивалентности секретного ключа. Итерация процесса шифрования. Оценка сложности.
11. Понятие криптосистемы с открытым ключом. Понятие CPA-стойкой криптосистемы с открытым ключом. Понятие LR-CPA–стойкой криптосистемы с открытым ключом. Теорема о том, что любая CPA–стойкая криптосистема с открытым ключом является LR-CPA–стойкой.
12. Доказательство CPA-стойкости криптосистемы Эль-Гамаля в предположениях сложности распознавательной задачи Диффи–Хеллмана.
13. Основные понятия теории линейных кодов: линейный код, порождающая и проверочная матрица, длина, размерность, кодовое расстояние. Граница Хэмминга. Граница Варшамова-Гильберта. Граница Синглтона.
14. Циклические коды. Цикличность кодов Хэмминга. Коды БЧХ. Граница БЧХ.
15. Коды БЧХ. Декодирование кодов БЧХ с помощью алгоритма Берлекемпа-Мэсси.
16. Задача кодирования дискретного источника без памяти равномерными кодами. Прямая теорема для равномерного кодирования дискретного источника без памяти. Обратная теорема для равномерного кодирования дискретного источника без памяти.
17. Неравномерное кодирование дискретных стационарных источников: постановка задачи,скорость создания, формулировка прямой и обратной теорем кодирования, оптимальный код, теорема о существовании оптимального D-ичного кода для одноместного ансамбля, метод Хаффмена с обоснованием.

18. Постановка задачи о трёхмерном сочетании и доказательство её NP-полноты.
19. NP-полнота задачи декодирования кода общего положения и задачи о спектре весов кода.
20. Кодовая криптосистема Мак-Элиса, построенная на кодах Хэмминга, её криптографический анализ.
21. Постановка задачи о перестановочной эквивалентности линейных кодов. Доказательство того, что эта задача не может быть NP-полной, а также того, что она не проще, чем задача об изоморфизме графов.
22. Криптосистема Мак–Элиса на основе кодов Рида–Маллера первого порядка, быстрый алгоритм декодирования кодов Рида–Маллера первого порядка.
23. Группа автоморфизмов кодов. Группа автоморфизмов кодов Рида–Маллера первого порядка. Криптосистема Мак–Элиса, построенная на кодах Рида–Маллера первого порядка, и её анализ.
24. Архитектурные особенности современных микропроцессоров. Последовательная и параллельная сложность алгоритмов, информационный граф и ресурс параллелизма алгоритм

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.

[5] 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.

[8] 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.

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

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

[12] 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

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

[15] 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.

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

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

[19] 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.