Екзамен. Крипта

Nikita Isachenko

June 2024

Зміст

1. **Цілі, напрямки, методи і аспекти захисту інформації. Криптологія. Задачі криптографії та криптоаналізу. Початкові поняття криптології та етапи розвитку. Класифікація криптосистем.**

Тут має бути якийсь текст

2. **Класична криптографія: терміни, поняття, позначення, типи шифрів. Визначення шифру підстановки (заміни). Моноалфавітні підстановки: визначення, загальний шифр простої підстановки. Моноалфавітні шифри класичної криптографії: Цезаря, афінної заміни, шифр Полібія та інші. Частотний аналіз шифру Цезаря та афінної підстановки.**

Тут має бути якийсь текст

3. **Блокові (табличні) підстановки: шифр Плейфера, афінна n-грамна заміна, шифр Хілла. Можливості частотного аналізу цих шифрів.**

Тут має бути якийсь текст

4. **Визначення поліалфавітної підстановки. Модульне шифрування. Класичні поліалфавітні шифри: Віженера, багатоконтурний шифр Віженера, шифр з автоключем, аперіодичні поліалфавітні шифри, книжковий шифр з бігучим рядком, шифр Вернама (одноразовий блокнот). Частотний аналіз шифру Віженера. Поняття адитивних або шифрів модульного гамування.**

Тут має бути якийсь текст

5. **Класична криптографія. Визначення шифру загальної блокової перестановки. Класичні шифри перестановки: Скітала, частоколу, табличні перестановки, маршрути Гамільтона, грати Кардано, магічні квадрати, n-кратні перестановки. Класифікація класичних шифрів.**

Тут має бути якийсь текст

6. **Поняття ентропії, властивості ентропії імовірнісних ансамблів, сумісна та умовна ентропія, взаємна інформація.**

Тут має бути якийсь текст

7. **Джерела дискретних сигналів, ентропія на символ джерела, надлишковість. Моделі джерел відкритого тексту.**

Тут має бути якийсь текст

8. **Поняття стійкості, теоретична і практична стійкість. Правило Керкгоффса. Ієрархія типів атак на криптосистему за рівнем доступної криптоаналітику інформації. Відмінність в криптоаналізі на основі шифрованих текстів та на основі відкритих текстів для класичних шифрів. Загальна схема секретного зв'язку.**

Тут має бути якийсь текст

9. Поняття криптосистеми. Математична модель Шеннона симетричного шифру. Припущення Шеннона. Формули для розрахунку сумісних і умовних розподілів в математичній моделі шифру.

Тут має бути якийсь текст

10. Цілком таємна криптосистема. Необхідні і достатні умови цілковита таємності. Межа Шеннона. Цілковита таємність шифру Вернама.

Тут має бути якийсь текст

11. Ненадійність ключа і відкритого тексту. Теореми про ентропією ключів за умовою криптограми та про середнє число хибних ключів (із доведенням).

Тут має бути якийсь текст

12. Функція ненадійності ключа. Відстань однозначності: визначення, доведення формули, інтерпретація, застосування. Принципи Шеннона: розсіювання і перемішування. Підхід до побудови стійких криптосистем, запропонований Шенноном. Класифікація сучасних криптосистем.

Тут має бути якийсь текст

13. Випадкові та псевдовипадкові послідовності в криптографії. Вимоги до випадкових послідовностей в криптографії.

Тут має бути якийсь текст

14. Формальні підходи до визначення поняття випадкової послідовності

Тут має бути якийсь текст

15. Первинні джерела випадкових шумів. Способи перетворення первинного шуму в випадкові дискретні послідовності. Математичні перетворення для покращення якості випадкових послідовностей.

Тут має бути якийсь текст

16. Одновимірні та багатовимірні булеві функції. Способи представлення булевих функцій: таблиці істинності, формули, ДДНФ, розклад Шеннона.

Тут має бути якийсь текст

17. Поліном Жегалкіна (АНФ), алгебраїчний степінь булевої функції. Швидке перетворення Мебіуса.

Тут має бути якийсь текст

18. Спектральні представлення булевих функцій. Ряд та коефіцієнти Фур'є, перетворення та коефіцієнти Уолша.

Тут має бути якийсь текст

19. Швидке перетворення Фур'є. Властивості коефіцієнтів Фур'є та Уолша, рівність Парсеваля.

Тут має бути якийсь текст

20. Криптографічні властивості булевих функцій. Невиродженість, відсутність заборон, збалансованість, згладжування.

Тут має бути якийсь текст

21. Статистичні аналоги булевих функцій. Нелінійність як відстань до класу афінних функцій, вивід формули, оцінка. Поняття бент-функції.

Тут має бути якийсь текст

22. Кореляційний імунітет булевих функцій: різні визначення, зв'язок із коефіцієнтами Уолша (із доведенням).

Тут має бути якийсь текст

23. Лавинні ефекти булевих функцій. Строгі лавинні критерії та критерії поширення. Похідні булевих функцій, функція автокореляції та її зв'язок із критеріями поширення.

Тут має бути якийсь текст

24. Симетричні блокові шифри: визначення, загальні властивості. Принципи побудови сучасних блокових шифрів. Модель ітеративного шифру.

Тут має бути якийсь текст

25. Схеми блокового шифрування: SP-мережа, схема Фейстеля, їх властивості.

Тут має бути якийсь текст

26. Стандарт шифрування DES: схема роботи, характеристики, недоліки. Модифікації алгоритму DES.

Тут має бути якийсь текст

27. Стандарт шифрування ДСТУ ГОСТ 28147:2009: схема роботи, характеристики.

Тут має бути якийсь текст

28. Стандарт шифрування AES: схема роботи, структура, характеристики. Швидка реалізація AES.

Тут має бути якийсь текст

29. Стандарти шифрування ДСТУ 7624:2014 «Калина» та ГОСТ Р 34.12-2015 «Кузнєчік»: схема роботи, основні характеристики.

Тут має бути якийсь текст

30. Режими роботи блокових шифрів, основні характеристики. Вплив спотворень у шифротекстах на відкриті тексти у різних режимах роботи.

Тут має бути якийсь текст

31. Потокові шифри: визначення, загальна модель. Типи генераторів гами. Внесення нелінійності у схеми на основі регістрів зсуву із лінійним зворотним зв'язком.

Тут має бути якийсь текст

32. Типи атак на потокові шифри. Кореляційна атака на схему нелінійної комбінації (на прикладі генератору Джиффі).

Тут має бути якийсь текст

33. Потокові шифри A5/1, A5/2. Потоковий шифр RC4. Конкурс eSTREAM.

Тут має бути якийсь текст