2022

Вопросы на ЗАЧЕТ

«Криптографические алгоритмы защиты информации»

ТЕОРЕТИЧЕСКИЕ ВОПРОСЫ

Тема 1. Дисциплина Криптографические методы защиты информации. Основные понятия.

1. Предмет КМЗИ, цели и задачи дисциплины.
2. Понятие криптография
3. Понятие криптоанализ
4. Понятие стеганография
5. Шифрование
6. Дешифрование
7. Кодирование
8. Основные методы шифрования и дешифрования
9. Основные методы методов кодирования
10. Основные методы криптоанализа
11. Основные методы стеганографии

Тема 2. История криптографии

12. Криптография в Древнем мире
13. Криптография в древнем Египте
14. Криптография в Атбаше
15. Криптография в Скитале
16. Тайнописи
17. Криптография от Средних веков до Нового времени
18. Криптография в британских колониях и США
19. Криптография на Руси и в России
20. Криптография в литературе
21. Криптография Первой мировой войны
22. Криптография Второй мировой войны
23. Германия: «Энигма», «Fish»
24. Математическая криптография
25. Открытая криптография и государство
26. Современный этап криптографии

Тема 3. Правовые основы защиты информации.

27. Правовые основы защиты информации в компьютерных системах;
28. Атаки и угрозы безопасности, каналы утечки информации.
29. Основные способы защиты информации.
30. Закон об охране программ для ЭВМ и баз данных.
31. Закон о защите личных данных.

Тема 4. Симметричные системы шифрования

32. Симметричные системы шифрования с одним ключом.
33. Достоинства и недостатки шифров с одним ключом.
34. Создание шифров на основе блочных алгоритмом перестановки.
35. Стандарты шифрования DES, 3DES и ГОСТ.
36. Стандарт шифрования AES

Тема 5. Асимметричные системы шифрования (с открытым ключом)

37. Асимметричные системы шифрования с открытым ключом.

38. Достоинства и недостатки шифров с открытым ключом.
39. Способы передачи секретного ключа.
40. Создание ключа на основе псевдослучайных последовательностей.
41. Примеры шифров на основе алгоритма Эль-Гамаля и алгоритма RSA.

Тема 6. Использование шифров для защиты информации

42. Аутентификация (подмена данных, хэш-функция, защита от подмены данных).
43. Цифровая подпись (создание цифровой подписи, атаки и защита цифровой подписи).
44. Стандарты на электронно-цифровую подпись: DSS и ГОСТ Р 34.10-94.
45. Цифровая подпись на базе шифра RSA и шифра Эль-Гамаля.

Тема 7. Хэш-функции

46. Определение хэш-функция
47. Назначение хэш-функций
48. Основные принципы построений хэш-функций
49. Принцип работы «Итеративная последовательная схема»
50. Принцип работы «Сжимающая функция на основе симметричного блочного алгоритма»
51. Применение хэш-функций в цифровой подписи
52. Проверка паролей с помощью хэш-функции
53. Сравнительная характеристика наиболее известных функций

Тема 8. Криптографические протоколы.

54. Основные понятия, классификация протоколов.
55. Протоколы аутентификации (разделение доступа к информации – пароли).
56. Протоколы цифровой подписи (связь аутентификации и цифровой подписи).

Тема 9. Средства идентификации и аутентификации в компьютерных системах

57. Классификация средств идентификации и аутентификации в КС
58. Аутентификация по многоразовым паролям.
59. Протокол аутентификации Kerberos.
60. Протокол аутентификации RADIUS.
61. Аутентификация по предъявлению цифрового сертификата.
62. Использование смарт-карт и USB-ключей с шифрованием.
63. Генерация ключевой пары вне устройства.
64. Генерация ключевой пары с помощью устройства.

2022

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

(приветствуется использование ПК для построения алгоритма и решения задачи, Python)

ЗАДАНИЕ 1. Сообщение, зашифрованное в пункте А шифром простой замены в алфавите из букв русского языка и знака пробела (-) между словами, передается в пункт Б отрезками по 12 символов. При передаче очередного отрезка сначала передаются символы, стоящие на четных местах в порядке возрастания их номеров, начиная со второго, а затем - символы, стоящие на нечетных местах (также в порядке возрастания их номеров), начиная с первого. В пункте В полученное шифрованное сообщение дополнительно шифруется с помощью некоторого другого шифра простой замены в том же алфавите, а затем таким же образом, как и из пункта А, передается в пункт В. По перехваченным в пункте В

отрезкам:

С О - Г Ж Т П Н Б Л Ж О

Р С Т К Д К С П Х Е У Б

- Е - П Ф П У Б - Ю О Б

С П - Е О К Ж У У Л Ж Л

С М Ц Х Б Э К Г О Щ П Ы

У Л К Л - И К Н Т Л Ж Г

восстановите исходное сообщение, зная, что в одном из переданных отрезков зашифровано слово

КРИПТОГРАФИЯ.

ЗАДАНИЕ 2. Расшифруйте исходное изречение, зашифрованное методом перестановки:

Изречение французского философа Жана-Поля Сартра:

ИНККО ОТСОЧ ЯЧПОТ ЕАРЕЯ ОЛНЕА АЕМТК ОНСТШ

ЗАДАНИЕ 3. Расшифруйте исходное изречение, зашифрованное методом перестановки:

Изречение немецкого ученого-гуманиста Эразма Роттердамского:

ЙЫТЫР КСТНА ЛАТЕН ТЕАДЗ ОСИИЦ АТУПЕ РОООО

ЗАДАНИЕ 4. Вам пришло зашифрованное сообщение:

ЫЛЧУЩЗКГУВ

Найдите исходное сообщение, если известно, что шифрпреобразование заключалось в следующем. Пусть x1, x2 - корни трехчлена x2+3x+1. К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавлялось значение многочлена f(x)=x6+3x5+x4+x3+4x2+4x+4, вычисленное либо при x=x1, либо при x=x2 (в неизвестном нам порядке), а затем полученное число заменялось соответствующей ему буквой.

ЗАДАНИЕ 5.

Текст

ЦЗЩИОНФЛЦЩРИОПЖЩЭЩХЖНФЛТЪЙ

ЗНЛУФ_АЩЛЗПИАЗНЭПЬОИВЛОПАЛ

АПАЛТЪЙЗЛЖФЛЦЗВХФОЛХПИОЩОН

ЛЪИЦЩУДЁЩЭПЖЪВЛЗПЁУЪХЖНШЛИ

ЪЮЭЩУЩЭЛЭЛЩОАЗНОЩЮЛОФАИОФ.

получен из исходного текста шифром простой замены. А текст

ЯАЧЕЕТВТВРАКНОО_ЛТКЛЛОРСТА

РИФШЫ_ПС_ЫЗХО_ЫКЫК_ОВОТЕНЕ

ЛСЯДЫП_ЧРВПСАК_ЕЗ_СГРМАОТН
СВ_ЕПР_Н_КТСЫОРААИТОООТИК_
ТРИ_НО_ТЧЧЬЫШВЮ_ФАИ_МЕИСЯ.
получен из исходного простым перестановочным шифром. Найти исходное сообщение.

ЗАДАНИЕ 6.

Расшифруйте исходное изречение, зашифрованное методом перестановки:
Изречение польского писателя-фантаста Станислава Лема:
ТОУМА МЕЖЕЧ ЫАООО ОММГЗ ЕСНМЕ ДЕООО ЧЫАОД НЛОТМ УМООО ТДЕРО ЕОЧОМ МОООО

ЗАДАНИЕ 7.

Расшифруйте исходное изречение, зашифрованное методом перестановки:
Изречение датского ученого-физика Нильса Бора:
ТПРРО УСЕБД ООДИН ОБЖВЛ ООЕЕУ ИОЧОЕ НАДЮ ЩНЬЕУ ОТДБУ

ЗАДАНИЕ 8.

Расшифруйте исходное изречение, зашифрованное методом перестановки:
Изречение американского писателя Джона Стейнбека:
АРЕНО ЫЕТМО ЕЖОИБ ЕДДЖЙ ЯПТВС ОДОКМ ПСИОЖ ОЙЛГО ОИЕНТ

ЗАДАНИЕ 9

Зашифруйте число 2, используя алгоритм RSA.

ЗАДАНИЕ 10

Шифрование методом блочной перестановки. Зашифруйте фразу «Чтобы пройти Путь воина, ты должен укрепить свое сердце» с помощью блочного алгоритма перестановки. Напишите программу для шифрования текста.

Описание алгоритма блочной перестановки. Исходный текст записывается в строки таблицы (например, по 15 символов в строке). Затем буквы текста переставляются по определенным правилам внутри шифруемого блока символов. Пустые ячейки таблицы можно заполнить любыми символами. Для получения шифротекста надо считать буквы по столбцам и записать их в виде строки с разбивкой на пятерки букв.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
К	Р	И	П	Т	О	А	Н	А	Л	И	З	Ш	И	Ф
Р	О	В	А	Н	Н	О	Г	О	Т	Е	К	С	Т	А

Например: задан открытый текст «КРИПТОАНАЛИЗ ШИФРОВАННОГО ТЕКСТА».
разбивка текста на блоки по 5 букв «КРИПТ ОАНАЛ ИЗШИФ РОВАН НОГОТ ЕКСТА».
шифротекст будет иметь вид «АТСКЕ ТОГОН НАВОР ФИШЗИ ЛОНАО ТПИРК».

ЗАДАНИЕ 11

Шифрование методом блочной перестановки с ключом. Зашифровать фразу «Чтобы пройти Путь воина, ты должен укрепить свое сердце» с помощью блочного алгоритма перестановки с ключом.Напишите программу для шифрования и дешифрования. Выполните криптоанализ шифрованного текста.

Описание алгоритма блочной перестановки с ключом. Символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. В качестве ключа выбирается любое слово и записывается в верхнюю строку таблицы. Например, в качестве ключа возьмем слово «информация». Буквы ключа нумеруются в алфавитном порядке (А=1, И=2, вторая И=3; М=4) и записываются в следующую строку таблицы. В следующих строках записывается исходный текст. Пустые ячейки можно заполнить любым символом (например, «ь»).

И	Н	Ф	О	Р	М	А	Ц	И	Я
2	5	8	6	7	4	1	9	3	10
М	Е	Т	О	Д	Б	Л	О	Ч	Н
О	Й	Ц	Е	Р	Е	С	Т	А	Н
О	В	К	И	И	К	Л	Ю	Ч	Ь

Для получения шифротекста надо выписать буквы по столбцам (с учетом нумерации столбцов, заданной ключевым словом). Для расшифровки надо записать шифротекст в таблицу по столбцам (учитывая номера столбцов).

Например: задан открытый текст «МЕТОД БЛОЧНОЙ ПЕРЕСТАНОВКИ и КЛЮЧ». Получаем шифротекст вида «ЛСЛМООЧАЧБЕКЕЙВОЕИДРИТПКОТЮННЬ».

Список использованных источников

1. Коржик В.И., Яковлев В.А. Основы криптографии, 2017 http://www.iprbookshop.ru/66798.html
2. Фороузан Бехроуз А. Криптография и безопасность сетей Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017
3. Торстейнсон П. Ганеш Г.А. Криптография и безопасность в технологии .NET БИНОМ. Лаборатория знаний, 2015