МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.45 Методы и средства криптографической защиты информации

1. **Код и наименование направления подготовки/специальности:**

10.05.01 Компьютерная безопасность

2. **Профиль подготовки/специализация:**

Математические методы защиты информации

Безопасность компьютерных систем и сетей

3. **Квалификация (степень) выпускника:** Специалист

4. **Форма обучения:** очная

5. **Кафедра, отвечающая за реализацию дисциплины:**

кибербезопасности информационных систем

6. **Составители программы:**

Степанец Юлия Александровна к.т.н., доцент кафедры кибербезопасности информационных систем

7. **Рекомендована:**

Научно-методическим советом факультета ПММ, протокол № 5 от 22.03.2024 г

8. **Учебный год:** 2027/2028 **Семестр(ы):** 7

9. Цели и задачи учебной дисциплины

Целью изучения дисциплины «Методы и средства криптографической защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и средств, а также примеров реализации этих методов на практике.

Задачи дисциплины - дать основы: системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов разработки шифров; математических методов, используемых в криптографии.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к обязательной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ОПК-10.1	Знает основные задачи, решаемые криптографическими методами.	Знание: основных задач, решаемых криптографическими методами; математических моделей шифров, подходов к оценке их стойкости; зарубежных и российских криптографических стандартов; принципов оценки защищённости информации в компьютерных системах. Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Знание методов анализа безопасности компьютерных систем. Умение корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик
		ОПК-10.2	Знает математические модели шифров, подходы к оценке их стойкости.	
		ОПК-10.3	Знает зарубежные и российские криптографические стандарты.	
		ОПК-10.4	Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами.	
		ОПК-10.5	Умеет применять математические методы при исследовании криптографических алгоритмов.	

		ОПК-10.6	Владеет навыками использования типовых криптографических алгоритмов.	безопасности в компьютерных системах. Владение: навыками использования типовых криптографических алгоритмов; методами анализа безопасности компьютерных систем; методиками оценки эффективности реализации систем защиты информации навыками работы с программными средствами общего и специального назначения; методами оценки защищённости информации в компьютерных системах

12. Объем дисциплины в зачетных единицах/час— 3/108.

Форма промежуточной аттестации - зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			7			
Аудиторные занятия	64		64			
в том числе: лекции	34		34			
Практические						
Лабораторные	34		34			
Самостоятельная работа	40		40			
Итого:	108		108			
Форма промежуточной аттестации	Зачет с оценкой		Зачет с оценкой			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Основные понятия. Терминология.	Информация, сообщения, сигналы, криптосистемы.	Криптографические методы защиты информации (10.05.01)
1.2	Математические основы криптографии	Теоремы о простых числах. Алгоритм Евклида. Функция Эйлера. Свойства модулярной арифметики. Теорема Эйлера. Вычисление обратных величин. Расширенный алгоритм Евклида	

1.3	Общие вопросы информационной безопасности	Основы классической криптографии. Классификация криптографических методов. Угрозы информации. Атаки на криптосистемы.	
1.4	Особенные системы криптографии.	Классы стойкости. Идеальные криптосистемы.	
1.5	Системы шифрования	Шифр RSA. Шифр Эль Гамаля. Цифровая подпись	
2. Лабораторные работы			
2.1	Работа с криптографическими средствами защиты	ГОСТ Р 34.12-2015, «Магма». ГОСТ Р 34.12-2015, «Кузнечик». Криптосистема Эль Гамаля.	Криптографические методы защиты информации (10.05.01)

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоя-тельная работа	Всего
1.1	Основные понятия. Терминология.	6	0	4	10
1.2	Математические основы криптографии	8	0	12	20
1.3	Общие вопросы информационной безопасности	8	10	8	26
1.4	Особенные системы криптографии	8		4	12
1.5	Системы шифрования	4	4	4	12
2.1	Работа с криптографическими средствами защиты	0	20	8	28
	Итого:	34	34	40	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-99120286-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111097 (дата обращения: 5.04.2019). — Режим доступа: для авториз. пользователей.
2	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, [б. г.]. — Часть 1 — 2017. — 64 с. — ISBN 978-5-7641-1053-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111765 (дата обращения: 5.02.2022). — Режим доступа: для авториз. пользователей.
3	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2018 — Часть 2 — 2018. — 63 с. — ISBN 978-5-7641-1215-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/138103 (дата обращения: 5.02.2022). — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
4	Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. — Самара : ПГУТИ, 2019. — 68 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223319 (дата обращения: 20.01.2020). — Режим доступа: для авториз. пользователей.
5	Салий В. Н. Криптографические методы и средства защиты информации / В. Н. Салий. – 2010. (URL: http://www.sgu.ru/files/nodes/11017/V.N._Saliy._Kriptograficheskie_metody_i_sredstva_zashchity_informacii.doc) (дата обращения: 12.05.2019)

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
6	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
7	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
8	Криптографические методы защиты информации (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебнометодической литературой, подготовка отчётов по лабораторным работам.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению проекта. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Криптографические методы защиты информации», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины: см. файл «МТО»

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.

Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение: ОС Windows v.7, 8, 10, набор утилит (архиваторы, файлменеджеры), LibreOffice v.5-7, Foxit PDF Reader.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.1	Основные понятия. Терминология.	ОПК-10	ОПК-10.1-3	Контрольная работа
1.2	Математические основы криптографии	ОПК-10	ОПК-10.1-3	Контрольная работа
1.3	Общие вопросы информационной безопасности	ОПК-10	ОПК-10.1-3	Контрольная работа
1.4	Особенные системы криптографии	ОПК-10	ОПК-10.1-3	Контрольная работа
1.5	Системы шифрования	ОПК-10	ОПК-10.2, 5	Контрольная работа
2.1	Работа с криптографическими средствами защиты	ОПК-10	ОПК-10.4-6	Лабораторные работы
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

 контрольная работа, лабораторные работы.

Перечень контрольных работ

1. Протоколы и их классификация.
2. Обмен ключами средствами симметричной криптографии.
3. Протоколы открытого распределения ключей.
4. Протоколы передачи секретного ключа по открытому каналу.
5. Аутентификация при входе в систему.
6. Вручение битов на хранение.
7. Бросание монеты по телефону.
8. Доказательство с нулевым разглашением.
9. Схемы аутентификации.
10. Методы разделения секрета.
11. Скрытый канал связи.
12. Мысленный покер.
13. Мысленный покер с тремя игроками.

Технология проведения

Студент выбирает вариант задания, ориентируясь на номер зачетки. Студент выполняет предложенное преподавателем задание, представляет его в письменном виде, при необходимости, комментирует выполненные действия, анализирует и интерпретирует результаты. В курсе предусмотрена одна контрольная работа (одна тема из списка).

Критерии оценивания

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Все задания контрольной работы выполнены, арифметических и логических ошибок нет, показано владение терминологией.	Повышенный уровень	Отлично
Все задания контрольной работы выполнены, но имеют место быть незначительные ошибки (арифметические, логические, в терминологии).	Базовый уровень	Хорошо
Не все задания контрольной работы выполнены и имеют место быть несущественные ошибки (арифметические, логические, в терминологии).	Пороговый уровень	Удовлетворительно
Задания контрольной работы не выполнены или имеют место быть существенные ошибки (арифметические, логические, в терминологии).	–	Неудовлетворительно

Перечень лабораторных работ

Лабораторная работа №1 Тема: ГОСТ Р 34.12-2015, «Магма»

Теоретические сведения 1.
Схема Фейстеля.
2. Операции по модулю.
3. Нелинейное преобразование.
4. Преобразование ключа.
Практическая часть
Обучение на основе компьютерной программы

Лабораторная работа №2 Тема: ГОСТ Р 34.12-2015, «Кузнечик».
Теоретические сведения
1. Простые и расширенные поля Галуа.
2. Преобразование ключа..
3. SP-сети.
Практическая часть
1. Реализация и исследование стандарта.
2. Подготовка и защита отчёта по лабораторной работе.

Лабораторная работа №3 Тема: Криптосистема Эль Гамаля.
Теоретические сведения
1. Понятие дискретного алгоритма.
2. Криптостойкость.
3. Сравнение с RSA.
Практическая часть
1. Обучение на основе компьютерной программы.
2. Подготовка и защита отчёта по лабораторной работе.

Технология проведения
Все лабораторные работы обязательны для выполнения. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания и они правильные, даны пояснения);
- оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к зачету.

Перечень вопросов к зачету (КИМ №1)

1. Что такое информационная безопасность?
2. В чем заключаются постулаты информационной безопасности?

3. Чем достигается обеспечение безопасности?
4. Что такое способы защиты информации?
5. В чем проявляются угрозы информации?
6. Что такое инженерно-техническая защита информации?
7. Что такое цена и ценность информации?
8. В чем состоят цели защиты информации?
9. Что подразумевается под эффективностью защиты информации?
10. Что такое система безопасности?
11. Охарактеризуйте физические системы защиты информации.
12. На какие классы разделяются инженерно-технические средства защиты информации?
13. Что такое криптология, криптограмма, криптография, криптоанализ?
14. Дайте определение криптосистемы (шифра).
15. В чем состоит основная идея шифрования данных?
16. В чем различие и в чем сходство шифрования и кодирования?
17. В чем различие терминов "дешифрование" и "расшифрование"?
18. Для решения каких задач используется кодирование информации?
19. Охарактеризуйте методы симметричного шифрования данных.
20. Опишите схему симметричного шифрования информации.
21. Приведите упрощённую схему алгоритма шифрования/расшифрования DES?
22. Что такое криптостойкость?
23. Каковы количественные характеристики криптостойкости?
24. Каким образом классифицируется инженерно-техническая защита информации?
25. Перечислите возможные виды утечек информации.
26. Сформулируйте основные законы модулярной арифметики.
27. Что представляет собой функция Эйлера?
28. В чем состоит теорема Эйлера?
29. Охарактеризуйте основные способы нахождения обратных по модулю величин.
30. Что такое криптосистема Эль Гамаля?

Критерии оценки ответов на вопросы зачета

Для оценивания результатов обучения на зачете используется – 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.

Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.

Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.

Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле:

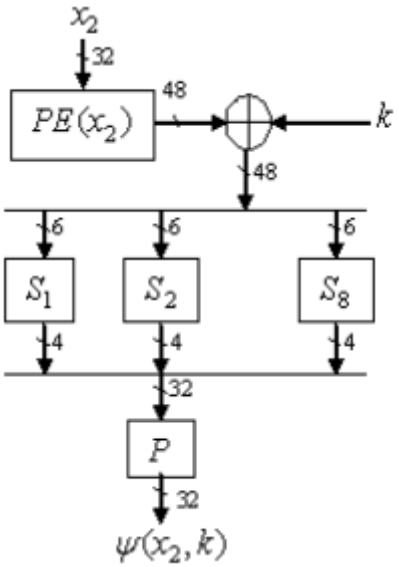
$$Q_{пром\_ат} = 0{,}4Q_{КР} + 0{,}6Q_{зач}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1) <u>закрытые задания (тестовые, средний уровень сложности):</u>

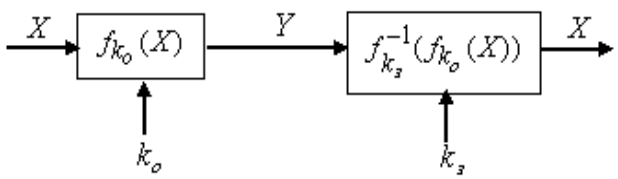
1. Какие шифры основаны на действиях с полиномами в поле Галуа:
   a) DES
   b) AES
   c) ГОСТ 28147-89
   d) KASTL
2. Определите правильную последовательность действий для шифра DES:
   a) ОТ(64 б) → Начальная перестановка → Схема Фейстеля (16 раундов с 48 битным ключом) → Конечная перестановка → Шифртекст (64 б)
   b) ОТ(64 б) → Начальная перестановка → Конечная перестановка → Схема Фейстеля (16 раундов с 64 битным ключом) → Шифртекст (64 б)
   c) ОТ(64 б) → Начальная перестановка → Конечная перестановка → Схема Фейстеля (12 раундов с 64 битным ключом) → Шифртекст (64 б)
   d) ОТ(64 б) → Начальная перестановка → Схема Фейстеля (16 раундов с 64 битным ключом) → Конечная перестановка → Шифртекст (64 б)
3. Дифференциальный криптоанализ относится к атакам:
   a) На основе шифртекста
   b) На основе открытых текстов
   c) На основе подобранного открытого текста
   d) На основе адаптивно подобранного открытого текста
4. Схема на рисунке представляет:



a) Общий вид схемы Фейстеля
b) Функцию усложнения DES
c) Схему расширения ключа AES
d) Функцию усложнения AES

5. Какие шифры не являются шифрами замены:
   a) Гаммирование
   b) Шифр Порта
   c) Решетка Кардано
   d) Шифр Вернама
   e) Метод Ришелье
6. Какие из режимов шифрования не требуют синхропосылки:
   a) Режим электронной кодировочной книги
   b) Режим сцепления блоков шифротекста
   c) Режим обратной связи по шифротексту
   d) Режим обратной связи по выходу
7. Какие из криптографических методов не являются шифрами в полном смысле этого слова:
   a) Скитала
   b) Метод магических квадратов
   c) Атбаш
   d) Линейка Энея
8. Алгебраическая модель шифра имеет вид:
   a) $f: X \times Y \to K$, где f инъективна и сюръективна
   b) $f: X \times K \to Y$, где f инъективна и сюръективна
   c) $f: X \times K \to Y$, где f инъективна
   d) $f: X \times Y \to K$, где f сюръективна
   e) $f: X \times K \to Y$, где f инъективна, сюръективна и транзитивна
9. Шифр, для которого верно $\forall\, x \in X\ y \in Y\ p(x|y) = p(x)$ является:
   a) Шифром гаммирования с равновероятной гаммой
   b) Шифром с марковским источником открытых текстов
   c) Совершенным
   d) Идемпотентным
10. При генерация раундового ключа в AES производится:
    a) Отбрасывание битов четности, используемых для помехоустойчивости
    b) Расширение ключа на основе закрытого ключа
    c) Расширение ключа на основе предыдущего раундового ключа
    d) Построение ключа на основе образующего полинома поля Галуа

11. Наличие слабых и полуслабых ключей является характерным недостатком алгоритмов:
    a) AES
    b) DES
    c) Любой схемы Фейстеля
    d) Полиалфавитных шифров
12. К методам взлома полиалфавитных шифров относятся:
    a) Частотный метод
    b) Метод бумеранга
    c) Метод чтения в колонках
    d) Линейный криптоанализ
    e) Метод Касински
13. Теоретическую стойкость шифра не определяют:
    a) То, что знание шифртекста не влечет перераспределение вероятностей на множестве шифруемых текстов
    b) Априорное допущение об информированности противника о криптосистеме с точностью до ключевой информации
    c) Стремление к нулю средней вероятности правильной дешифровки открытого текста с ростом длины сообщения
    d) Возможность подбора эффективного метода взлома по принципу оптимального соотношения минимальной трудоемкости и максимальной вероятности верной дешифровки
14. Расстояние единственности шифра это:
    a) минимальное натуральное L, при котором по известному шифротексту e_L однозначно восстанавливается открытый текст m_L
    b) количество букв открытого текста, которое можно убрать до наступления нечитаемости открытого текста.
    c) мера ненадежности открытого текста и ключа
    d) среднее расстояние между периодическими m-граммами в шифротексте полиалфавитных шифров
15. Метод криптоанализа, основанный на замене функции криптопреобразования ее статистическим аналогом называется:
    a) Дискретный криптоанализ
    b) Метод встречи посередине
    c) Линейный криптоанализ
    d) Метод Симпсона
16. Криптология включат в себя следующие дисциплины:
    a) Критографию и стеганографию
    b) Криптографию и криптоанализ
    c) Криптографию, криптоанализ и стеганографию
    d) Стеганографию и криптоанализ
17. На рисунке представлена

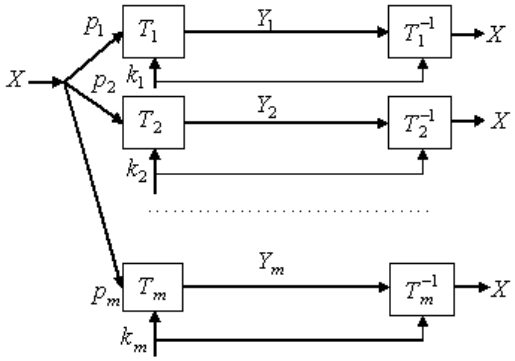


    a) Общая схема симметричной киптосистемы
    b) Общая схема ассиметричной криптосистемы
    c) Общая схема электронной цифровой подписи
    d) Общая схема поточной криптосистемы
18. К вероятностным моделям источников открытых сообщений не относятся:

a) Источники независимых символов
b) Источники марковски зависимых букв
c) Нестационарные источники
d) Самосинхронизирующиеся источники

19. К видам криптопреобразований не относятся:
a) Шифры замены
b) Шифры престановки
c) Композиционные шифры
d) Поточные шифры

20. На рисунке изображена



a) Сумма криптосистем
b) Произведение криптосистем
c) Транзитивная криптосистема
d) Идемпотентная криптосистема

21. Разделение криптосистем по конструктивным принципам происходит на:
a) Шифры замены и перестановки
b) Симметричные и ассиметричные системы
c) Блочные и поточные системы
d) Сумму и произведение криптосистем

22. Формула $f_{k3}^{-1}\left(f_{ko}(X)\right) = X$ определяет:
a) Шифрование в симметричной криптосистеме
b) Дешифрование в симметричной криптосистеме
c) Шифрование в асимметричной криптосистеме
d) Дешифрование в асимметричной криптосистеме

23. К свойствам шифров относятся:
a) Имитостойкость
b) Помехоустойчивость
c) Разрядность
d) Необратимость преобразования

24. Выполнение свойства шифра $\forall\, k \in K\ (f(x_1) = f(x_2) => x_1 = x_2)$
a) Является необходимым и определяет инъективность криптопреобразования
b) Является необходимым и определяет обратимость криптопреобразования
c) Является достаточным условием совершенности шифра
d) Не является необходимым для криптопреобразования

25. Криптосистема с преобразованием $f: X \times K \to Y$ является минимальной, если выполняется:
a) $|X| = |K|$
b) V=TT=T, где T – оператор криптопреобразования, а V – произведение криптоситем
c) $\forall\, x \in X\ y \in Y\ p(x|y) = p(x)$
d) $\forall y \in Y\ \exists\, x \in X: y = f(x)$

26. Аффиный шифр описывается криптопреобразованием:

a) $y_i = (x_i + k)\ mod\ m, i = \overline{1,n}$
b) $x_i = (y_i - k)\ mod\ m, i = \overline{1,n}$
c) $y_i = (ax_i + k)\ mod\ m,\ i = \overline{1,n}$
d) $f\ = (f_0 \dots f_{n-1})$

27. Криптопреобразование $y_i = \left(x_i + \tilde{k}i + \tilde{\mu}i + \cdots + \tilde{\sigma}i\right)\ mod\ m,\ i = \overline{1,n}$, где $\tilde{k}i, \tilde{\mu}i, \tilde{\sigma}i$ – ключевые последовательности разных периодов, является:
    a) Шифром Виженера
    b) Шифром Вернама
    c) Перешифровкой для шифра Виженера
    d) Шифром Белазо
28. Перестановка по гамильтоновым путям является частным случаем:
    a) Простой перестановки
    b) Вертикальной перестановки
    c) Маршрутной перестановки
    d) Диагональной перестановки
29. Частью синхронной поточной криптосистемы не являются:
    a) Зашумляющий блок
    b) Управляющий блок
    c) Генератор гаммы
    d) Регистр внутреннего состояния генератора
30. К недостаткам синхронной криптосистемы относятся:
    a) Размножение ошибок
    b) Рассинхронизация
    c) Уязвимость к вставкам фрагментов
    d) Уязвимость к замене символа
31. Криптопреобразование вида $\varphi((L_0, R_0), k) = R_0 || F(R_0, K) \oplus L_0$, где || - конкатенация, F – функция усложнения, описывает:
    a) Цикловую функцию ячейки Фейстеля
    b) Общий вид итеративной блочной криптосистемы
    c) Общий вид ассиметричной криптосистемы
    d) Цикловую функцию KASTL-сети
32. Какие криптопреобразования являются частью цикловой функции алгоритма AES?
    a) Нелинейная замена
    b) Предварительная перестановка
    c) Перемешивание в столбцах
    d) Выбор сеансового ключа
33. Глобальная дедукция – это:
    a) Извлечение секретного ключа
    b) Метод криптоанализа блочных шифров
    c) Статистический метод криптоанализа
    d) Работка эквивалента алгоритма для дешифровки без знания ключа
34. К криптоатакам по сторонним каналам относятся:
    a) Зондирование
    b) Дифференциальный анализ
    c) Метод встречи посередине
    d) Имитовставка
35. Метод максимального правдоподобия позволяет получить:
    a) Эффективный линейный аналог для нелинейных криптопреобразований
    b) Оценку ключа при наличии шифротекста с известным распределением вероятностей в открытом тексте
    c) Гамму и открытый текст при повторном использовании гаммы
    d) Период для периодической шифрующей последовательности
36. Для шифрующего автомата начальное состояние будет представлять собой:

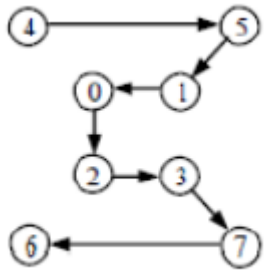
a) Открытый текст
b) Криптопреобразование
c) Базовый алфавит
d) Ключ

37. Правило постоянного процента позволяет учесть:
    a) Избыточность языка
    b) Старение дешифруемой информации
    c) Ненадежность ключа
    d) Равнораспределенность вероятностной схемы
38. Для эргодической модели открытого текста справедливо:
    a) для любых двух отрезков открытого теста найдется сообщение, содержащие в себе оба этих отрезка
    b) Длина ключа не может быть меньше длины открытого теста, следовательно число ключей растет с длиной открытого текста
    c) Вероятности появления *k* -грамм в тексте зависят от их места в тексте
    d) открытый текст является реализацией цепи Маркова
39. Вероятностная модель шифра с распределениями $P(X) = P(p(x), x \in X)\ P(K) = P(p(k), k \in K)$ индуцирует:
    a) Матрицу переходных вероятностей шифра $\|p(y|x)\|$, $|X| \times |Y|$
    b) Совместные распределения $P(X, K)$, $P(X, Y)$, $P(Y, K)$
    c) Старение дешифруемой информации
    d) Сложность задачи факторизации для шифра
40. Метод встречи посередине используется для:
    a) Решения задачи дискретного логарифмирования
    b) Подбора адаптивного открытого текста
    c) Получения эффективного линейного аналога
    d) Уменьшения времени полного перебора
41. Использование эквивалентных ключей относится к:
    a) Алгоритмам поиска
    b) Методам апробирования
    c) Итерационным методам
    d) Ни одному из перечисленных
42. Расширение ключа в алгоритме ГОСТ 28147-89 производится посредствам:
    a) отбрасывания служебных битов, реализующих проверку четности для помехоустойчивости хранения ключа
    b) циклического сдвига на количество разрядов, заданное в таблице для каждой итерации
    c) разбиением ключа на машинные слова подключи
    d) рекуррентных вычислений на основе ключа предыдущего раунда

2) <u>открытые задания (тестовые, средний уровень сложности):</u>

1. Зашифруйте при помощи блочной криптосистемы с размером блока в один байт и синхропосылкой (начальным вектором) y_0=0x02 открытый текст из шестнадцатеричных чисел «0x4C 0x4F 0x4C» шифром простого гаммирования (XOR) с гаммой γ=0xB2 в режиме обратной связи по шифротексту (ответ 0x4E 0xB3 0x4D)

2. Как называется блок шифротекста, формирующийся из всего объема открытого текста при помощи суммирования по модулю 2 шифрованных блоков? Ответ: имитовставка
3. Зашифруйте открытый текст «Юстас Алексу» шифром Виженера с ключом «жираф» (ответ дщваежухкещ)
4. Зашифруйте открытый текст «Юстас Алексу» маршрутной перестановкой по указанному гамильтонову пути с заполнителем *



Ответ саютлсеас*ку****

5. Как называется подход, при котором криптопреобразования производятся над прямоугольными массивами данных, называемыми состояниями? Ответ KASTL-сеть
6. Для какого источника открытых текстов вероятности появления *k* -грамм в тексте зависят от их места в тексте? Ответ Нестационарный
7. Какая криптоатака основана на знании открытого текста для случайных фрагментов шифротекста? Ответ: на основе открытых текстов
8. Какой шифр описывает криптопреобразование $f = (f_0 \dots f_{n-1})$ для открытого текста $X = x_0 \dots x_{n-1}$ дающее шифротекст $Y = y_0 \dots y_{n-1} = x_{f(0)} \dots x_{f(n-1)}$? Ответ шифр перестановки
9. Какой метод криптоанализа заключается в анализе изменения несходства между парой открытых текстов в процессе прохождения через циклы шифрования с одним и тем же ключом Ответ Дифференциальный
10. Над какими структурами производится криптопреобразования в KASTL-сетях? Ответ: состояния
11. Какой параметр криптосистемы перебирается при использовании алгоритмов поиска? Ответ: Ключ
12. Какой структурный элемент алгоритма проверяется на несходства входа и выхода при дифференциальном анализе DES? Ответ : S-блок
13. Как называют совокупность раундовых ключей в итеративных криптосистемах? Ответ: ключевое расписание
14. Какой размер имеет закрытый ключ в алгоритме ГОСТ 28147-89? Ответ 256
15. Какое криптопреобразование осуществляется на первом этапе реализации шифрования алгоритмом DES? Ответ: начальная перестановка
16. Какое свойство асинхронных поточных криптосистем гарантирует совпадение гаммы на разных концах информационного обмена? Ответ: самосинхронизация
17. При каком режиме шифрования каждый блок открытого текста складывается по модулю 2(XOR) с предыдущем блоком шифротекста, затем шифруется? Ответ: режим сцепления блоков шифротекста
18. Какое разбиение производится на множестве ключей K, если верно $\forall\, x\, \chi,\ \chi' \in K\ f(x,\chi) = f(x,\chi')$, при использовании методов апробирования? Ответ: классы эквивалентности

К какому классу криптоатак по сторонним каналам относятся атаки с прямым доступом к внутренним компонентам? Ответ: агрессивные

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).