МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий
/Д. Г. Демидов/
"30" августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптоанализ»

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2021

Москва 2021 г.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01«Информационная безопасность»**.

Программу составил: доцент, к.ф.-м.н. Н.Г.Бутакова

Программа утверждена на заседании кафедры "Информационная безопасность" «30» августа 2021 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Криптоанализ» следует отнести:

- изучение современных методов и средств анализа криптографической защиты информации для решения проблем защиты информации.

К **основным задачам** освоения дисциплины «Криптоанализ» следует отнести:

- овладение основными криптографическими инструментами, необходимыми для построения защищенных информационных систем.

2. Место дисциплины в структуре ООП бакалавриата.

Дисциплина «Криптоанализ» относится к числу элективных учебных дисциплин (Б.1.2) основной образовательной программы (Б.1.ДВ.3).

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Математический анализ», «Дискретная математика», «Теория вероятностей и математическая статистика», «Теория информации», «Основы информационной безопасности».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать	Перечень планируемых результатов обучения по дисциплине
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	**знать:** принципы построения криптографических алгоритмов, типовые криптографические алгоритмы; алгоритмы криптографических стандартов и их использование в информационных системах. **уметь:** пользоваться научно-технической литературой в области криптографии. **владеть:** криптографической терминологией; навыками использования типовых криптографических алгоритмов

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет **4** зачетных единицы, т.е. **144** академических часов (лабораторные занятия- 72 час, самостоятельная работа – 72 часов, форма контроля - экзамен) в 4 семестре.

Структура и содержание дисциплины «Программирование криптографических алгоритмов» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. Разработка, отладка и тестирование программ криптоанализа шифров замены:

Частотный анализ.

Поиск вероятного слова.

Шифры замены.

Криптоанализ шифров простой замены.

Тема 2. Разработка, отладка и тестирование программ криптоанализа поточных шифров:

Шифры многозначной замены.

Криптоанализ шифров гаммирования Белазо и Виженера.

Регистры сдвига с обратной связью.

Скремблеры.

Криптоанализ шифрующей гаммы.

Криптоанализ начального заполнения – ключевой инициализации.

Тема 3. Разработка, отладка и тестирование программ криптоанализа блочных системы шифрования:

Шифры блочной замены.

Криптоанализ шифров вертикальной перестановки.

Конструкции Фейстеля. Алгоритмы блочного шифрования.

Алгоритмы шифрования ГОСТ 28147-89, ГОСТ 34.12-2015.

ГОСТ 34.13-2015. Режим простой замены.

Анализ рассеивания знака открытого текста по шифртексту.

Атака полным перебором.

Тема 4. Разработка, отладка и тестирование программ криптоанализа криптосистем с открытыми ключами:

Асимметричные системы шифрования.

Открытое распределение ключей. Схема Диффи-Хеллмана.

Алгоритм RSA. Метод факторизации Ферма.

Система шифрования El Gamal. Дискретное логарифмирование.

5. Образовательные технологии.

Методика преподавания дисциплины «Криптоанализ» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

подготовка к выполнению практических работ с использованием видео уроков;

- проведение интерактивных лекционных и практических занятий в форме видео уроков;
- проведение групповых упражнений;
- обсуждение и защита домашних заданий по дисциплине;
- подготовка, представление и обсуждение презентаций на семинарских занятиях.

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 60 % аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- подготовка к решению прикладных задач, групповых упражнений;
- подготовка к выполнению лабораторных работ и их защита;
- контрольные работы;
- экзамен.

Образцы тестовых заданий, заданий курсовых проектов, контрольных вопросов и заданий для проведения текущего контроля, экзаменационных билетов, приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.
В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю)

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**

знать: принципы построения криптографических алгоритмов, типовые криптографические алгоритмы; алгоритмы криптографических стандартов и их использование в информационных системах.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: принципы построения криптографических алгоритмов, типовые криптографические алгоритмы; алгоритмы криптографических стандартов и их использование в информационных системах.	Обучающийся демонстрирует неполное соответствие следующих знаний: принципы построения криптографических алгоритмов, типовые криптографические алгоритмы; алгоритмы криптографических стандартов и их использование в информационных системах. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: принципы построения криптографических алгоритмов, типовые криптографические алгоритмы; алгоритмы криптографических стандартов и их использование в информационных системах. но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: принципы построения криптографических алгоритмов, типовые криптографические алгоритмы; алгоритмы криптографических стандартов и их использование в информационных системах. свободно оперирует приобретенными знаниями.
уметь: пользоваться научно-технической литературой в области криптографии.	Обучающийся не умеет или в недостаточной степени умеет пользоваться научно-технической литературой в области криптографии	Обучающийся демонстрирует неполное соответствие следующих умений: пользоваться научно-технической литературой в области криптографии Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих умений: пользоваться научно-технической литературой в области криптографии Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие следующих умений: пользоваться научно-технической литературой в области криптографии Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.

владеть: криптографической терминологией; навыками использования типовых криптографических алгоритмов	Обучающийся не владеет или в недостаточной степени владеет криптографической терминологией; навыками использования типовых криптографических алгоритмов	Обучающийся владеет криптографической терминологией; навыками использования типовых криптографических алгоритмов; в неполном объеме, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет криптографической терминологией, навыками использования типовых криптографических алгоритмов; навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет криптографической терминологией; навыками использования типовых криптографических алгоритмов, свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации*: экзамен.*

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.

Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

1. Бутакова Н.Г. Криптографические методы защиты информации. Электронный образовательный ресурс. Московский Политех, 2020 - https://lms.mospolytech.ru/course/view.php?id=2518.
2. Бутакова Н.Г., Федоров В.Н. Криптографические методы и средства защиты информации: учебное пособие. Издание 2-е, исправленное и дополненное. – СПб: ИЦ «Интермедиа», 2020. – 380с. – ISBN 978-5-4383-0210-0.
3. Бутакова Н.Г., Семененко В.А., Федоров Н.В. Криптографическая защита информации: учебное пособие для вузов. – М.: Изд-во МГИУ, 2011 . – 316 с. - ISBN 978-5-2760-1503-3
4. Бутакова Н.Г., Федоров В.Н. Криптографические методы и средства защиты информации: учебное пособие. – СПб: ИЦ «Интермедиа», 2016. – 384с. – ISBN 978-5-4383-0135-6. Доступ к электронной версии книги открыт на сайте https://elibrary.ru/item.asp?id=28331738.

б) дополнительная литература:

1. Рябко Б.Я. Криптографические методы защиты информации [Текст] : Учеб. пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М. : Горячая линия-Телеком, 2013. - 229 с. - Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 978-5-9912-086-2.
2. Баричев. С.Г. Основы современной криптографии [Текст] : Учеб. курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - 2-е изд., перераб. и доп. - М. : Горячая линия-Телеком, 2002. - 176 с. - ISBN 5-93517-075-2: 57-29.
3. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с. - ISBN 5-93517-292-5 : 204-33. Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 5-93517-292-5.
4. Бернет С. Криптография. Официальное руководство RSA Security [Текст] : Пер. с англ. / С. Бернет, С. Пейн. - М. : Бином, 2002. - 382 с. - ISBN 5-9518-0003-X. - ISBN 0-07-213139-X: 168-00.
5. Введение в информационную безопасность [Электронный ресурс]: Учеб. пособие для вузов / А. А. Малюк [и др.] ; Под ред. В.С. Горбатова. - М. : Горячая линия-Телеком, 2011. - 288 с. - Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 978-5-9912-0160-5.
6. Криптография. Скоростные шифры [Текст] / А. А. Молдовян [и др.]. - СПб. : BHV, 2002. - 493 с. - ISBN 5-94157-214-X : 280-00.
7. Основы криптографии [Текст] : Учеб. пособие / А. П. Алферов [и др.]. - 3-е изд., испр. и доп. - М. : Гелиос АРВ, 2005. - 480 с. - ISBN 5-85438-137-0.
8. Столлингс, В. Криптография и защита сетей: Принципы и практика [Текст] : Пер. с англ. / В. Столлингс. - 2-е изд. - М. : Вильямс, 2001. - 672 с. - ISBN 5-8459-0185-5. - ISBN 0-13-869017-0 : 408-00.

в) программное обеспечение и интернет-ресурсы:

1. Журнал «Специальная техника и связь» (ВАК). Сайт журнала – http://www.st-s.su/index.htm.
2. Журнал «Защита информации. Инсайд». Сайт журнала – http://www.inside-zi.ru/
3. Журнал «Безопасность информационных технологий». Сайт журнала – сайт журнала http://www.pvti.ru/articles_14.htm.
4. Журнал «Информация и безопасность». Сайт журнала – http://kafedrasib.ru/?page_id=119.

5. Журнал «Information Security/Информационная безопасность». Издатель: компания «Гротек». Сайт журнала – http://www.itsec.ru.
6. ЭБС издательства Лань – http://e.lanbook.com/.
7. Научная электронная библиотека eLIBRARY.RU – http://elibrary.ru/.
8. Библиографическая и реферативная база данных научной периодики «Scopus» - www.scopus.com.
9. Сайт Федеральной службы безопасности России (ФСБ России). -http://www.fsb.ru.
10. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). - http://www.fstec.ru.
11. Портал технического комитета по стандартизации «Защита информации». – http://tk.gost.ru/wps/portal/tk362
12. Информационно-аналитический Интернет-портал ISO27000.ru. – http://www.iso27000.ru/
13. Портал по безопасности. – http://www.sec.ru/.
14. http://82.179.184.119/MegaPro/Web
15. http://e.lanbook.com/view/book/5171/
16. http://82.179.184.119/MegaPro/Download/MObject/420/34251.pdf
17. http://e.lanbook.com/

8. Материально-техническое обеспечение дисциплины.

Интерактивный класс или аудитория с интерактивной доской.

Класс ПЭВМ с установленным программным обеспечением. Из расчета одна ПЭВМ на одного человека.

Практические занятия и исследовательские лабораторные занятия проводятся в компьютерных классах корпуса 4 на Автозаводской.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *лекции.*

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. *Практические занятия* проводятся по теоретическим и проблемным вопросам ИБ. Практическое занятие предполагает творческие дискуссии, активный обмен мнениями по поставленным *вопросам,* заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении практического занятия преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В

случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на зачете.

Самостоятельная работа по дисциплине предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др..

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

10. Методические рекомендации для преподавателя

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

Приложение 1
к рабочей программе

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОГМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.03.01 «Информационная безопасность»
ОП (профиль): «Безопасность компьютерных систем (кибербезопасность новой информационной среды)»

Форма обучения: очная
Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; организационно-управленческая

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ «Криптоанализ»

Состав: 1. Паспорт фонда оценочных средств
2. Описание оценочных средств:
Контрольные работы
Тест
Зачет

Составители: доцент, к.ф.-м.н. Бутакова Н.Г.

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Криптоанализ					
ФГОС ВО **10.03.01 «Информационная безопасность»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочных средств**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	знать: принципы построения криптографических алгоритмов, типовые криптографические алгоритмы; алгоритмы криптографических стандартов и их использование в информационных системах. уметь: пользоваться научно-технической литературой в области криптографии. владеть: криптографической терминологией; навыками использования типовых криптографических алгоритмов	самостоятельная работа, лабораторные работы	КР тест экзамен	Базовый уровень: способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач. Повышенный уровень: демонстрирует полное соответствие следующих навыков: использования типовых криптографических алгоритмов, свободно оперирует приобретенными знаниями .

Приложение 2
к рабочей программе

Оценочные средства для текущей аттестации

Вопросы к контрольным работам

1. Дайте общее понятие криптографии. В чем состоит сущность шифрования и дешифрования информации?
2. Соотнесите между собой понятия «криптография», «криптоанализ» и «криптология».
3. Чем определяется криптостойкость шифрования? Какие другие требования предъявляются к шифрованию?
4. В чем состоит правило Керкгоффса? Почему это правило является общепринятым в криптографии?
5. Когда появилась криптография с открытыми ключами и первая реальная система шифрования?
6. Чем отличаются подходы к обеспечению безопасности информации в криптографии и в стеганографии?
7. Что общего и в чем отличие криптографического преобразования информации от кодирования ее при защите от случайных угроз безопасности?
8. Какими методами обеспечивается конфиденциальность информации?
9. Что такое целостность информации?
10. Дайте определение имитостойкости шифра.
11. Что такое имитовставка? Для каких целей она используется?
12. Для каких аспектов информационного взаимодействия необходима аутентификация?
13. Два основных требования к хэш-функциям. Против каких атак они направлены?
14. Какие средства используются для обеспечения невозможности отказа от авторства?
15. Что означает свойство односторонности криптографической хэш-функции?
16. В чем суть предварительного распределения ключей?
17. Что такое сертификат открытого ключа?
18. Для чего используется схема разделения секрета?
19. Что такое шифрвеличина, шифробозначение и как эти понятия соотносятся?
20. Какие особенности характерны для методов шифрования с симметричным ключом и несимметричным (открытым) ключом?
21. Чем отличаются симметричные шифрсистемы от асимметричных?
22. Поясните на примере сущность шифрования методом замены.
23. Приведите примеры шифрования методами перестановки. Что означает маршрутная перестановка?
24. Поясните сущность гаммирования как способа криптографического преобразования информации. Что является при этом ключом шифрования?
25. Почему аддитивные методы шифрования относятся к шифрам гаммирования?
26. К какому классу шифров относятся аналитические способы шифрования?
27. Приведите пример шифра перестановки, который может рассматриваться и как блочный шифр замены?
28. С какими целями в криптографии вводятся модели открытых текстов?
29. Какие подходы используются для распознавания открытых текстов
30. Какое правило лежит в основе всех шифров перестановки?
31. Что является ключом шифра перестановки?
32. Назовите основной недостаток шифров перестановки.
33. Приведите пример шифра перестановки, который может рассматриваться и как блочный шифр замены?

34. Как определить по криптограмме, полученной с помощью шифра вертикальной перестановки, число коротких столбцов заполненного открытым текстом основного прямоугольника?
35. Какие свойства открытого текста используются при вскрытии шифра перестановки?
36. Какие шифры называются шифрами простой замены?
37. Что является ключом шифра простой замены? Каково максимально возможное число ключей шифра простой замены?
38. Что более целесообразно для надежной защиты информации: архивация открытого текста с последующим шифрованием или шифрование открытого текста с последующей архивацией?
39. Имеет ли шифр Плейфера эквивалентные ключи, то есть такие ключи, на которых любые открытые тексты шифруются одинаково?
40. Какие шифры называются омофонами? Приведите пример.
41. Какие шифры называются шифрами многозначной замены? Приведите примеры.
42. Является ли шифр пропорциональной замены омофоном?
43. Поясните, что вы понимаете под совершенным шифром. Приведите примеры.
44. Почему шифр Тритемия, лежащий в основе шифра Виженера не является шифром гаммирования?
45. Почему наложение на открытый текст гаммы, представляющей собой периодическую последовательность небольшого периода, не дает надежной защиты?
46. Почему недопустимо использовать дважды одну и ту же гамму (даже случайную и равновероятностную!) для зашифрования разных открытых текстов?
47. Перечислите основные требования к гамме.
48. Каковы с точки зрения криптографии преимущества и недостатки перехода к блочному шифрованию?
49. Как реализуется предложенный К.Шенноном принцип «перемешивания» при практической реализации алгоритмов блочного шифрования?
50. Каковы основные недостатки алгоритма DES, и каковы пути их устранения?
51. В каких случаях можно рекомендовать использовать блочный шифр в режиме простой замены?
52. От каких потенциальных слабостей позволяет избавиться использование блочных шифров в режимах шифрования с обратной связью?
53. В чем заключаются достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами?
54. Почему возникает проблема синхронизации поточных шифров?
55. Какие причины обусловили широкое использование линейных регистров сдвига в качестве управляющих блоков поточных шифрсистем?
56. Проведите сравнительный анализ алгоритмов шифрования RC4 и RC5.
57. Перечислите основные режимы работы, предусмотренные в российском стандарте шифрования данных
58. В чем состоят преимущества систем с открытыми ключами перед симметричными шифрсистемами?
59. Сложностью какой математической задачи определяется стойкость системы RSA?
60. Какие требования предъявляются к ключам в шифре RSA?
61. К какому типу шифров принадлежит схема шифрования, используемая в системе Эль-Гамаля? В чем ее преимущества?
62. Сложностью какой математической задачи определяется стойкость шифрсистемы Эль-Гамаля?
63. Назовите недостатки схемы Эль-Гамаля.
64. Какие проблемы информационной безопасности можно решить с помощью асимметричных шифров.

65. Изложите принципиальную схему организации секретной связи с использованием шифрсистемы с открытым ключом.
66. Каким образом с помощью криптосистемы RSA можно организовать передачу сообщений, подлинность которых мог бы проверить любой получатель?
67. Каким образом с помощью криптосистемы RSA можно организовать передачу сообщений, подлинность авторства которых можно при необходимости доказать?
68. Что общего между обычной и цифровой подписью? Чем они различаются?
69. Какие задачи позволяет решить цифровая подпись?
70. В чем заключается принципиальная сложность в практическом применении систем цифровой подписи?
71. Почему в криптографических системах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования и цифровой подписи?

ТЕСТ-ВОПРОСЫ

1. Что является предметом науки КРИПТОРГАФИЯ?
А) способы шифрования и дешифрования;
Б) методы сокрытия факта передачи секретной информации;
В) способы преобразования информации с целью ее защиты от несанкционированных пользователей.

2. Криптосистема называется криптосистемой общего использования, если ее стойкость основывается на секретности
А) алгоритмов шифрования и расшифрования;
Б) ключа;
В) режима шифрования.

3. На какие две группы можно разделить симметричные криптосистемы?
А) блочные и поточные;
Б) синхронные и асинхронные;
В) аналоговые и цифровые.

4. Какие события способствовали развитию криптографии?
А) рост грамотности среди населения;
Б) раздел территорий, образование государств, войны;
В) переход к фонетическому письму, сокращение мощности алфавита.

5. Почему поточные шифры в общем случае по скорости намного превосходят блочные шифры?
А) посимвольное шифрование менее трудоемко, чем шифрование большими блоками;
Б) поточное шифрование не требует схем синхронизации;
В) шифрующая последовательность часто генерируется независимо от открытого текста или шифртекста.

6. Назовите основную проблему при организации секретной связи в случае поточных шифров?
А) проблема передачи ключей между абонентами;
Б) проблема устранения ошибок в потоке шифруемых данных;
В) проблема синхронизации потока шифруемых данных.

7. Кем была предложена первая практическая реализация криптографии с открытым ключом?

А) Уитфилдом Диффи (Whitfield Diffie) и Мартином Хеллманом (Martin Hellman) и Ральфом Мерклем (Ralf Merkle);
Б) Рональдом Райвистом (Ronald Rivest), Ади Шамиром (Adi Shamir) и Леонардом Адлеманом (Leonard Adleman);
В) Шафи Гольдвассером (Shafi Goldwasser) и Сильвио Микэли (Silvio Micali).

8. К какой группе шифров относится шифр СЦИТАЛА?
А) шифр замены;
Б) шифр перестановки;
В) комбинированный шифр.

9. Слово КРИПТОГРАФИЯ зашифровано классическим шифром Цезаря. Выберите соответствующий шифртекст.
А) УБТОИГСБИЪТЬ;
Б) ФСЖВЛЫКСПЭЖЮ;
В) НУЛГХСЖУГЧЛБ.

10. При шифровании открытого текста его буквы заменяются парой чисел, соответствующих номерам столбцов и строк данной буквы в таблице. Как называется этот шифр?
А) решетка Кардано;
Б) квадрат Полибия;
В) таблица Порто.

11. Как назывался шифр, на основе которого был создан один из наиболее стойких военно-морских шифров Великобритании во время Второй мировой войны?
А) решетка Кардано;
Б) квадрат Полибия;
В) таблица Порто.

12. При каких условиях восстановить текст по криптограмме криптоаналитику становится принципиально невозможно?
А) если шифрование «стирает» избыточность;
Б) если используется длинный ключ;
В) если алгоритм шифрования неизвестен.

13. Как называются используемые в криптографии модели открытого текста, учитывающие зависимость букв текста от предыдущих букв?
А) позначные модели открытого текста;
Б) вероятностные модели k -го приближения;
В) Марковские модели открытых текстов.

14. Кто в России руководил разработкой телефонного шифратора?
А) В.А.Котельников;
Б) А.Н.Колмогоров;
В) Б.Б.Пиотровский.

15. В чем состоит основной принцип Керкгоффса?
А) компрометация системы не должна причинять неудобств корреспондентам;
Б) необходимо, чтобы криптосистема была простой в использовании, и её применение не требовало соблюдения длинного списка правил;
В) у корреспондентов должна быть возможность по собственной воле менять ключ.

16. Что понимается под криптографическим протоколом?
А) алгоритм шифрования данных перед передачей по общедоступному каналу связи;
Б) распределенный алгоритм решения двумя или более участниками некоторой криптографической задачи;
В) набор правил шифрования и расшифрования криптосистемы.

17. В чем состоит криптографическая задача обеспечения целостности?
А) гарантирование невозможности внесения случайных ошибок в процессе передачи по каналам связи;
Б) гарантирование невозможности несанкционированного изменения информации;
В) оба ответа верны.

18. Какие методы разрабатываются с целью обеспечения аутентификации?
А) методы подтверждения подлинности сторон и самой информации в процессе информационного взаимодействия;
Б) методы присвоения уникального идентификатора взаимодействующим сторонам и самой информации в процессе информационного взаимодействия;
В) оба ответа верны.

19. Какой механизм используется для обеспечения невозможности отказа от авторства или приписывания авторства?
А) механизм симметричного шифрования с привлечением арбитра;
Б) механизм цифровой подписи;
В) оба ответа верны.

20. С чем связана активная атака на зашифрованную информацию?
А) с прослушиванием, анализом трафика, перехватом, записью передаваемых шифрованных сообщений;
Б) с дешифрованием, т. е. попытками "взломать" защиту с целью овладения информацией;
В) с прерыванием процесса передачи сообщений, созданием поддельных сообщений, модификацией передаваемых сообщений.

21. От чего зависит выбор способа шифрования?
А) от особенностей передаваемой информации (ее ценности, объема, способа представления, необходимой скорости передачи;
Б) от возможностей владельцев по защите своей информации (стоимость применяемых технических устройств, удобство использования, надежность функционирования;
В) оба ответа верны.

22. Для обнаружения целенаправленного навязывания противником ложной информации
А) в передаваемой информации стирается избыточность;
Б) в передаваемую информацию вносится избыточность;
В) используется код четности.

23. Как называется числовая комбинация, используемая для проверки целостности?
А) имитовставка;
Б) код аутентификации сообщения;
В) оба ответа верны.

24. Какие требования предъявляются к ключевым хэш-функциям $h_K(M)=S$?

А) невозможность вычисления значения $h_k(M) = S$ для заданного сообщения M без знания ключа k;
Б) невозможность подбора для заданного сообщения M с известным значением $h_k(M) = S$ другого сообщения M_1, с известным значением $h_k(M_1) = S_1$ без знания ключа k;
В) оба ответа верны.

25. Какое требование направлено против создания поддельных (сфабрикованных) сообщений при атаках типа имитация?
А) невозможность вычисления значения $h_k(M) = S$ для заданного сообщения M без знания ключа k;
Б) невозможность подбора для заданного сообщения M с известным значением $h_k(M) = S$ другого сообщения M_1, с известным значением $h_k(M_1) = S_1$ без знания ключа k;
В) оба ответа верны.

26. Какое требование направлено против модификации передаваемых сообщений при атаках типа подмена?
А) невозможность вычисления значения $h_k(M) = S$ для заданного сообщения M без знания ключа k;
Б) невозможность подбора для заданного сообщения M с известным значением $h_k(M) = S$ другого сообщения M_1, с известным значением $h_k(M_1) = S_1$ без знания ключа k;
В) оба ответа верны.

27. Какая проверка означает аутентификацию сеанса связи?
А) проверка целостности соединения, невозможности повторной передачи данных противником, сторон взаимодействия;
Б) проверка целостности соединения, невозможности повторной передачи данных противником, своевременности передачи данных;
В) оба ответа верны.

28. Какое средство является основным средством для проведения идентификации?
А) протоколы односторонней идентификации;
Б) протоколы взаимной идентификации;
В) оба ответа верны.

29. Как выглядит цифровая подпись для сообщения?
А) число, полученное в результате хеширования, примененного к этому сообщению;
Б) число, полученное в результате криптографических преобразований, примененных к этому сообщению;
В) код аутентификации сообщения.

30. Для чего применяются специальные системы предварительного распределения ключей?
А) при большом числе взаимодействующих сторон требуется предварительная рассылка значительного объема ключевой информации и последующее ее хранение;
Б) определяется порядок использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения старых ключей;
В) предусматривается распределение и хранение не самих ключей, а некоторой меньшей по объему информации, на основе которой каждая сторона может вычислить ключ для взаимодействия с другой стороной.

31. Каким образом наиболее просто можно осуществить распределение ключей для сетей с большим количеством абонентов?
А) в системах предварительного распределения секретных ключей;
Б) в системах открытого распределения секретных ключей;
В) оба ответа верны.

32. Что такое сертификат открытого ключа?
А) набор данных, заверенных цифровой подписью центра сертификации, и включающий открытый и секретный ключи, имя пользователя, имя сертификационного центра, номер сертификата, время действия сертификата, предназначение открытого ключа (цифровая подпись, шифрование);
Б) набор данных, заверенных печатью центра сертификации, и включающий открытый ключ, список дополнительных атрибутов, принадлежащих абоненту, и предназначение открытого ключа;
В) набор данных, заверенных цифровой подписью центра сертификации, и включающий открытый ключ и список дополнительных атрибутов, принадлежащих абоненту.

33. Что означает термин мощность алфавита?
А) количество символов в открытом алфавите;
Б) число возможных комбинаций символов открытого алфавита;
В) количество шифрвеличин открытого алфавита.

34. К какому классу шифров относится шифр, если фрагмент открытого текста (отдельные буквы или группа букв) заменяются некоторыми их эквивалентами (буквами, цифрами, символами или их комбинацией) в шифртексте?
А) шифры замены;
Б) шифры перестановки;
В) композиционные шифры.

35. К какому классу шифров относится шифр, если буквы открытого текста при шифровании каким-нибудь способом перестанавливаются, то есть изменяется только порядок следования символов открытого текста?
А) шифры замены;
Б) шифры перестановки;
В) композиционные шифры.

36. Что следует делать для увеличения криптостойкости шифра?
А) увеличивать разницу между числом шифрвеличин и числом букв в алфавите;
Б) более равномерной должна быть диаграмма повторяемости знаков шифртекста;
В) оба ответа правильны.

37. Для чего используются блочные шифры?
А) для увеличения количества шифрвеличин;
Б) для увеличения скорости шифрования;
В) оба ответа правильны.

38. В чем состоит основное преимущество асимметричного шифрования перед симметричным?
А) нет необходимости в передаче секретного ключа, который может быть перехвачен злоумышленником;
Б) большая трудоемкость последнего и, как результат, меньшие скорости при шифровании;

В) оба ответа верны.

39. Какие шифры называются омофонами?
А) шифры многозначной замены;
Б) многоалфавитные шифры;
В) шифры гаммирования.

40. Что такое шифрвеличина?
А) число возможных эквивалентов для замены открытых символов;
Б) эквиваленты в шифртексте, заменяющие символы или группы символов в открытого текста;
В) открытый текст перед шифрованием представляется в виде последовательности «подслов», называемых шифрвеличинами.

41. С какими целями в криптографии вводятся модели открытых текстов??
А) служат основой для автоматизации процессов криптоанализа шифртекстов;
Б) служат основой в процессе изучения криптостойкости различных систем шифрования;
В) оба ответа верны.

42. К какому классу шифров относятся аддитивные методы шифрования?
А) омофоны;
Б) шифры многозначной замены;
В) шифры гаммирования.

43. К какому классу шифров относятся аналитические способы шифрования?
А) шифры замены;
Б) шифры перестановки;
В) маршрутные перестановки.

44. Какие из приведенных шифров являются шифрами перестановки?
А) решетка Кардано;
Б) квадрат Полибия;
В) таблица Порто.

45. Какие из приведенных шифров являются шифрами замены?
А) RSA;
Б) AES;
В) ГОСТ 28147-89.

46. Какие свойства открытого текста используются при вскрытии шифра перестановки?
А) ограничением может послужить появление запретных биграмм;
Б) наиболее частые биграммы открытого текста, которые можно составить из букв рассматриваемого шифрованного текста;
В) оба ответа верны.

47. Какая из математических моделей соответствует алгоритму шифра Атбаш?
А) $Y_{ij} = ij$;
Б) $Y_i = X_{i+3} (\mathrm{mod}\ n)$;
В) $Y_i = X_{(n-i+1)}$.

48. Зашифруйте с помощью матричного шифра с ключевой матрицей $A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$ и цифрового эквивалента букв открытого текста слово *забава.*

А) 28,35,67,21,26,38;
Б) 24,38,42,21,32,46;
В) 12,32,7634,17,19.

49. Что более целесообразно для надежной защиты информации?

А) архивация открытого текста с последующим;
Б) шифрование открытого текста с последующей архивацией;
В) не имеет значения.

50. К каким шифрам относится система шифрования Петра I «Цифирь»?

А) омофоны;
Б) шифры биграммной замены;
В) шифры простой замены.

51. На каком способе шифрования был основан биграммный шифр Плэйфера (Playfair, Великобритания), применявшийся Великобританией во время Первой мировой воны?

А) способ шифрования состоял в разбивке входного текста на биграммы;
Б) на лозунговом способе заполнения шифртаблицы;
В) оба ответа верны.

52. Какие шифры относятся к шифрами многозначной замены?

А) шифр Виженера и шифр Тритемия;
Б) шифр Плэйфера и шифр Хилла;
В) шифр Вернама и шифр Порта.

53. Сформулируйте основное требование к криптографически стойкому генератору псевдослучайной последовательности или гаммы.

А) период гаммы должен быть достаточно большим для шифрования сообщений различной длины;
В) гамма должна быть трудно предсказуемой, т.е. если известны тип генератора и кусок гаммы, то невозможно предсказать следующий за этим куском бит гаммы с вероятностью выше заданной.
Б) оба ответа верны;

54. Приведите пример совершенного шифра.

А) шифр Виженера с самоключом;
Б) одноразовый блокнот Шеннона;
В) система Вернама для телеграфа с бумажным кольцом, содержащим гамму.

55. Какие шифры являются шифрами гаммирования?

А) шифр Тритемия;
Б) шифр Виженера;
В) оба ответа верны.

56. По какому модулю производится суммирование гаммы с открытым текстом в режиме гаммирования ГОСТ28147-89?

А) суммирование по модулю 2;

Б) суммирование по модулю 2^{32};
В) оба ответа верны.

57. Каков размер блока шифруемого текста в криптосистеме ГОСТ28147-89?
А) 32 бита;
Б) 64 бита;
В) ГОСТ28147-89 – поточная криптосистема.

58. Какие функции выполняет криптосистема?
А) усиление защищенности данных и облегчение работы с криптоалгоритмом со стороны человека;
Б) усиление защищенности данных и обеспечение совместимости потока данных с другим программным обеспечением;
В) оба ответа верны.

59. Для чего в поточных шифрах используются регистры сдвига с обратной связью?
А) для генерации ключевой последовательности;
Б) для организации режима обратной связи в блочных шифрах;
В) оба ответа верны.

60. Что такое скремблер?
А) программные или аппаратные реализации генератора псевдослучайно гаммы;
Б) программные или аппаратные реализации алгоритма, позволяющего шифровать побитно непрерывные потоки информации;
В) оба ответа верны.

61. В чем состоит главная проблема шифров на основе скремблеров?
А) синхронизация передающего (кодирующего) и принимающего (декодирующего) устройств;
Б) кодирующая последовательность бит производится из небольшого начального объема информации;
В) маленький период гаммы.

62. Какие методы синхронизации применяются на практике в системах шифрования на основе скремблеров?
А) добавление в поток информации синхронизирующих битов, заранее известных приемной стороне, что позволяет ей при отсутствии такого бита активно начать поиск синхронизации с отправителем;
Б) использование высокоточных генераторов временных импульсов, что позволяет в моменты потери синхронизации производить расшифрование принимаемых битов информации "по памяти" без синхронизации;
В) оба ответа верны.

63. Какой метод используется для рандомизации сообщений?
А) внесение случайных бит в сам шифруемый файл с игнорированием их на дешифрующей стороне;
Б) шифрование исходного файла случайным ключом;
В) оба ответа верны.

64. Какие шифрсистемы из перечисленных ниже являются поточными?
А) A5, SEAL, RC4;
Б) DES, AES, Rijndael;

В) RC2, RC5, IDIA .

65. Перечислите основные режимы работы, предусмотренные в стандарте шифрования данных ГОСТ28147-89.
А) простой замены, гаммирования, гаммирования с обратной связью, гаммирования с обратной связью по шифр тексту;
Б) простой замены, гаммирования, гаммирования с обратной связью, выработки имитовставки;
В) электронная кодовая книга, сцепления блоков, обратная связь по выводу, обратная связь по шифртексту.

66. Перечислите основные режимы работы, предусмотренные в стандарте шифрования данных DES.
А) простой замены, гаммирования, гаммирования с обратной связью, гаммирования с обратной связью по шифртексту;
Б) простой замены, гаммирования, гаммирования с обратной связью, выработки имитовставки;
В) электронная кодовая книга, сцепления блоков, обратная связь по выходу, обратная связь по шифртексту?

67. Назовите действующий стандарт шифрования в Америке?
А) DES;
Б) AES;
В) Triple DES.

68. Какой криптографический алгоритм лег в основу стандарта шифрования AES?
А) Lucifer;
Б) Blowfish;
В) Rijndael.

69. Какие из приведенных криптографических алгоритмов используют в основе сеть Фейстеля?
А) DES;
Б) Rijndael;
В) оба ответа верны.

70. Что общего в стандартах DES и ГОСТ28147-89?
А) размер блока, размер ключа, количество циклов;
Б) размер блока, преобразование, количество циклов;
В) оба ответа верны.

71. Назовите размер ключа (в битах), используемого в криптосистеме ГОСТ28147-89?
А) 32;
Б) 56;
В) 256.

72. Почему криптографический алгоритм ГОСТ28147-89 более устойчив к вскрытию путем полного перебора по множеству возможных значений ключа, чем DES?
А) функция шифрования ГОСТ гораздо сложнее функции шифрования DES;
Б) в силу намного большей длины ключа;
В) оба ответа верны.

73. Что такое дайджест сообщения?
А) результата вычисления хеш-функции;
Б) цифровой отпечаток пальца;
В) оба ответа верны.

74. Какая математическая проблема лежит в основе схемы открытого распределения ключей Диффи и Хеллмана (Diffi W., Hellman M.E.)?
А) операция вычисления дискретного логарифма;
Б) факторизация большого числа;
В) оба ответа верны.

75. В чем состоит основное отличие асимметричных криптосистем от симметричных?
А) для передачи открытого ключа от получателя к отправителю секретный канал не нужен. Вместо него используется аутентичный канал, гарантирующий подлинность источника информации;
Б) для шифрования и дешифрования используются различные ключи;
В) оба ответа верны.

76. Назовите наиболее распространенные области применения асимметричных криптографических систем?
А) ассиметричная система используется для шифрования короткого сеансового ключа, а информационные потоки в течение сеанса приходят по симметричной системе;
Б) ассиметричная система используется для доказательства принадлежности в случае отказа отправителя/получателя от ранее переданного/принятого сообщения;
В) оба ответа верны.

77. Для решения каких задач используется цифровая подпись?
А) для доказательства принадлежности в случае отказа отправителя/получателя от ранее переданного/принятого сообщения;
Б) для обеспечения аутентификации и контроля целостности;
В) оба ответа верны.

78. Является ли верным утверждение, что применение асимметричных систем в общем случае приводит к существенным задержкам при шифровании (по сравнению с симметричными)?
А) да;
Б) нет;
В) зависит от размеров используемых ключей.

79. Каким образом вычисляется цифровая подпись?
А) последовательное вычисление хеш-функции от исходного сообщения и шифрование полученного значения на секретном ключе отправителя (или расшифрование на открытом ключе при проверке подписи);
Б) последовательное шифрование исходного сообщения на секретном ключе отправителя и вычисление хеш-функции от зашифрованного сообщения;
В) последовательность операций не имеет значения.

80. Верно ли утверждение, что в асимметричной системе никто, кроме отправителя подписанного сообщения, не знает секретного ключа, на котором сообщение было подписано?
А) да;

Б) нет, секретный ключ известен также удостоверяющему центру, выдавшему отправителю сертификат цифровой подписи;
В) нет, секретный ключ известен также центру аутентификации, в котором используется криптосистема.

81. Какая функция называется односторонней (one-way function)?
А) Функция $f(x)$ называется односторонней (one-way function), если для всех x из ее области определения легко вычислить $y=f(x)$, но нахождение по заданному y_0 такого x_0, для которого $f(x_0)=y_0$, вычислительно неосуществимо;
Б) Функция $f(x)$ называется односторонней (one-way function), если для нахождение по заданному y_0 такого x_0, для которого $f(x_0)=y_0$ требуется настолько огромный объем вычислений, что за них просто и не стоит браться;
В) оба ответа верны.

82. Верно ли утверждение, что целочисленная показательная функция $f(x)=a^x(mod\ n)$, где основание a и показатель степени x принадлежат интервалу $(1,n-1)$, является односторонней функцией?
А) да;
Б) существование односторонних функций не доказано, но она может быть взята в качестве приближения;
В) нет.

83. К каким криптографическим системам относится система RSA?
А) к блочным экспоненциальным системам, так как каждый блок M открытого текста рассматривается как целое число в интервале от 0 до $(n-1)$ и преобразуется в блок шифртекста;
Б) к шифрам однозначной замены;
В) оба ответа верны.

84. Чем определяется стойкость криптосистемы RSA?
А) сложностью извлечения корня степени e из большого целого числа по заданному модулю n;
Б) сложностью разложения на простые сомножители большого целого числа;
В) оба ответа верны.

85. Какая функция используется в криптосистеме RSA для генерации секретного ключа?
А) функция Эйлера;
Б) функция Мебиуса;
В) оба ответа верны.

86. Какой фактор определяет размер ключа в криптосистеме RSA?
А) ресурсами ЭВМ, на которой установлена криптосистема;
Б) длиной шифруемого открытого текста;
В) размером модуля n, по которому идет шифрование.

87. Чем определяется стойкость криптосистемы Elgamal?
А) сложностью дискретного логарифмирования;
Б) сложностью разложения на простые сомножители большого целого числа;
В) оба ответа верны.

88. Какая схема шифрования легла в основу стандартов электронной цифровой подписи в США (DSA – Digital Signature Algorithm) и России (ГОСТ 334.10-2001)?

А) схема Райвеста, Шамиля и Адлемана (Rivest R., Shamir A., Adleman L.;
Б) схема Эль-Гамаля (Elgamal);
В) схема Диффи и Хеллмана (Diffi W., Hellman M.E.).

89. По какой формуле вычисляется секретный ключ в шифре Эль-Гамаля?
А) $y \equiv g^x \pmod p$;
Б) $ed \equiv 1 \pmod{\varphi(n)}$;
В) выбирается произвольно из условия $1 < x < p$.

90. По какой формуле вычисляется секретный ключ в шифре RSA?
А) $y \equiv g^x \pmod p$;
Б) $ed \equiv 1 \pmod{\varphi(n)}$;
В) выбирается произвольно из условия $1 < x < p$.

91. К какому классу шифров относится шифр по схеме Эль-Гамаля?
А) шифры многозначной замены;
Б) схемы вероятностного шифрования;
В) оба ответа верны.

92. Что общего между криптосистемами Эль-Гамаля и RSA?
А) шифры многозначной замены;
Б) шифры однозначной замены;
В) асимметричные шифры.

93. В чем состоит способ взлома шифра RSA ?
А) в том, чтобы найти метод вычисления корня степени *e* из *mod n*,. поскольку криптограмма $C = M^e \pmod n$, то корнем степени *e* из *(mod n)* является сообщение М;
Б) в том, чтобы найти главные сомножители общего модуля *n* (*p* и *q*), поскольку с их помощью можно легко вычислить секретный ключ *d* для расшифрования $M = C^d \pmod n$;
В) оба ответа верны.

94. В чем состоят преимущества шифрсистем с открытыми ключами?
А) для обмена ключами абонентам секретный канал не нужен;
Б) применение симметричных систем приводит к существенным задержкам при шифровании (по сравнению с асимметричными);
В) оба ответа верны.

95. Какие хэш-функции используются для формирования цифровой подписи?
А) бесключевые односторонние хэш-функции;
Б) ключевые односторонние хэш-функции;
В) криптографические хэш-функции.

96. Хэш-значение какой длины (в байтах) вычисляет стандарт ГОСТ Р34.11-2001?
А) 32;
Б) 16;
В) 20.

97. Какой шифр использует отечественный стандарт хэширования ГОСТ Р 34.11-94 для шифрования исходных данных, чтобы обеспечить невозможность подбора сообщений с одинаковым хэш-значением,?
А) RSA;

Б) ГОСТ 28147-89;
В) шифр Эль-Гамаля.

98. Перечислите алгоритмы электронной цифровой подписи?
А) RSA, DSA, EGDA, схема Шнорра, ГОСТ Р34.10;
Б) ГОСТ 28147, DES, AES, ESIGN, ECDSA;
В) СТБ 1176.2-99, McEliece, Rijndael,Схема Диффи – Лампорта.

99. К каким видам атак уязвима цифровая подпись RSA?
А) к мультипликативной атаке;
Б) нецелевого использования секретного ключа;
В) оба ответа верны.

100. Какими преимуществами обладает схема цифровой подписи Эль-Гамаля по сравнению со схемой цифровой подписи RSA?
А) при заданном уровне стойкости алгоритма цифровой подписи целые числа, участвующие в вычислениях, имеют запись на 25% короче, что уменьшает сложность вычислений почти в два раза и позволяет заметно сократить объем используемой памяти;
Б) при выборе модуля *P* достаточно проверить, что это число является простым;
В) оба ответа верны.

Оценочные средства для промежуточной аттестации
Экзамен
Список вопросов для экзамена

1. Нарисовать блок-схему алгоритма и привести числовой пример криптоанализа шифра Вернама.
2. Нарисовать блок-схему генератора гаммы на основе регистров сдвига с линейной обратной связью. Привести числовой пример гаммы с максимальным периодом.
3. Нарисовать блок-схему алгоритма и привести числовой пример обмена ключами по схеме Диффи-Хеллмана.
4. Нарисовать блок-схему алгоритма и привести числовой пример криптоанализа шифра RSA.
5. Нарисовать блок-схему алгоритма и привести числовой пример криптоанализа шифра Эль-Гамаля.
6. Нарисовать блок-схему алгоритма частотного анализа шифртекста и привести числовой пример криптоанализа.
7. Нарисовать блок-схему алгоритма поиска вероятного слова в шифр тексте и привести числовой пример криптоанализа.
8. Нарисовать блок-схему алгоритма частотного анализа и привести числовой пример криптоанализа шифра RSA с посимвольным шифрованием.
9. Нарисовать блок-схему алгоритма и привести числовой пример криптоанализа шифров простой замены.
10. Нарисовать блок-схему генерации секретного ключа по алгоритму RSA. Привести числовой пример слабого и сильного ключей при заданном модуле.
11. Нарисовать блок-схему генератора гаммы с максимальным периодом на базе регистра сдвига с линейной обратной связью. Привести числовой пример.
12. Нарисовать блок-схему линейного конгруэнтного генератора гаммы с максимальным периодом. Привести числовой пример.
13. Нарисовать блок-схему криптоанализа шифрующей гаммы. Привести числовой пример.

14. Нарисовать блок-схему криптоанализа начального заполнения генератора гаммы на регистре сдвига. Привести числовой пример.
15. Нарисовать блок-схему криптоанализа ключевой инициализации регистра сдвига с линейной обратной связью. Привести числовой пример.
16. Нарисовать блок-схему криптоанализа ключевой инициализации регистра скремблера. Привести числовой пример.
17. Нарисовать блок-схему криптоанализа шифра многозначной замены Белазо. Привести числовой пример.
18. Нарисовать блок-схему криптоанализа шифра вертикальной перестановки. Привести числовой пример.
19. Нарисовать блок-схему конструкции Фейстеля. Привести числовой пример рассеивания знака открытого текста по шифртексту.
20. Нарисовать блок-схему функции шифрования данных по алгоритму ГОСТ Р 34.12-2015 (Магма) в режиме простой замены. Привести числовой пример неправильного использования режима.
21. Нарисовать блок-схему функции шифрования данных по стандарту DES. Привести числовой пример.
22. Нарисовать блок-схему алгоритма и привести числовой пример слабой таблицы замены ГОСТ 28147-89.
23. Нарисовать блок-схему шифрования данных по алгоритму Elgamal. Привести числовой пример дискретного логарифмирования.
24. Нарисовать блок-схему шифрования данных по алгоритму DES. Привести числовой пример силового криптоанализа слабого ключа.