

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»

Уфимский филиал Финуниверситета

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Основы криптографии»

Разработчик: кафедра «Математика и информатика»

Направления подготовки: 09.03.03 Прикладная информатика

Образовательная программа: Прикладные информационные системы в экономике и финансах


Профиль: Прикладные информационные системы в экономике и финансах

Форма образования: заочная

РАССМОТРЕН
На заседании кафедры
«Математика и информатика»

Протокол № 12
от « 30 » июня 2023 г.

Зав. кафедрой



/С.А. Фархиева

Подпись

Разработан на основе

ОС ФГОБУ ВО Финуниверситета по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата) № 1523/о от 28.06.2021 г.

Оценочные средства для оценки сформированности компетенций

ПКН-2 Способность разрабатывать алгоритмы и программы с использованием современных технологий программирования

ПКН-7 Способность выполнять сервисное обслуживание и настройку аппаратного и программного обеспечения, в том числе с учетом требований информационной безопасности

Задания в виде расчетных задач (ПКН-2, ПКН-7)

Задание 1 (ПКН-2)

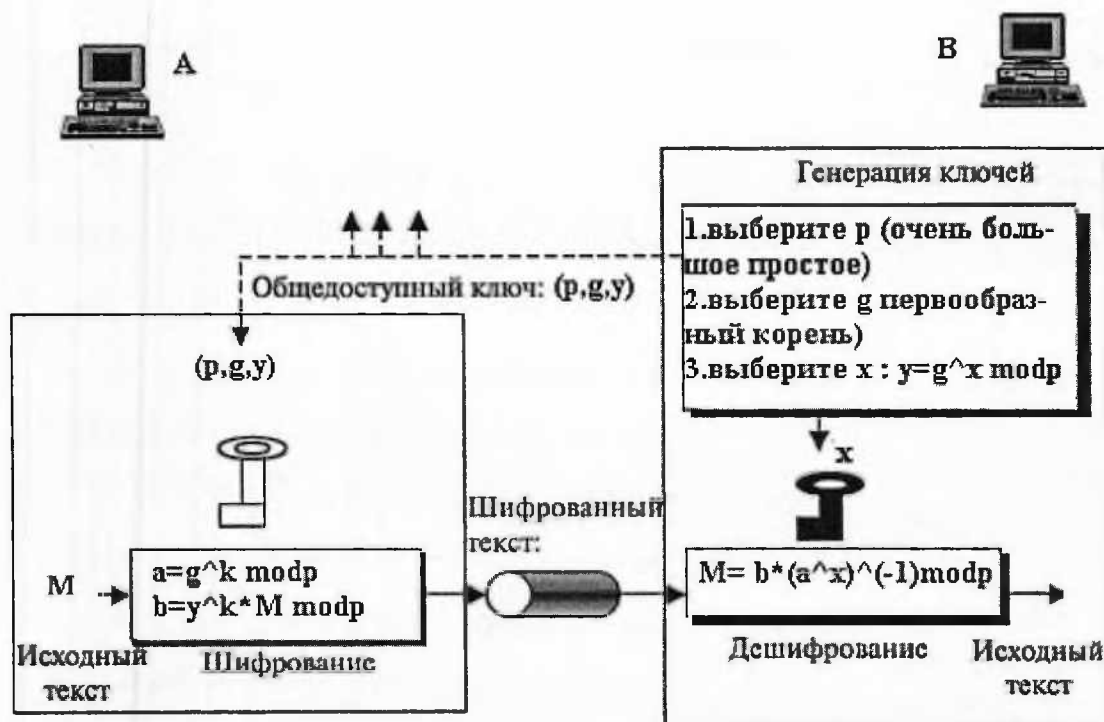
Используя шифр Порты (см. ниже таблицу кодирования)

1	А Б	а р	б с	в т	г у	д ф	е х	ж ц	з ч	и ш	й щ	к ъ	л ы	м ь	н э	о ю	п я
2	В Г	а с	б т	в у	г ф	д х	е ц	ж ч	з ш	и щ	й ъ	к ы	л ь	м э	н ю	о я	п р
3	Д Е	а т	б у	в ф	г х	д ц	е ч	ж ш	з щ	и ъ	й ы	к ь	л э	м ю	н я	о р	п с
4	Ж З	а у	б ф	в х	г ц	д ч	е ш	ж щ	з ъ	и ы	й ь	к э	л ю	м я	н р	о с	п у
5	И Й	а ф	б х	в ц	г ч	д ш	е щ	ж ъ	з ы	и ь	й э	к ю	л я	м р	н с	о т	п у
6	К Л	а х	б ц	в ч	г ш	д щ	е ъ	ж ы	з ь	и э	й ю	к я	л р	м с	н т	о у	п ф
7	М Н	а ц	б ч	в ш	г щ	д ъ	е ы	ж ь	з э	и ю	й я	к р	л с	м т	н у	о ф	п х
8	О П	а ч	б ш	в щ	г ъ	д ы	е ь	ж э	з ю	и я	й р	к с	л т	м у	н ф	о х	п ц
9	Р С	а ш	б щ	в ъ	г ы	д ь	е э	ж ю	з я	и р	й с	к т	л у	м ф	н х	о ц	п ч
10	Т У	а щ	б ъ	в ы	г ь	д э	е ю	ж я	з р	и с	й т	к у	л ф	м х	н ц	о ч	п ш
11	Ф Х	а ъ	б ы	в ь	г э	д ю	е я	ж р	з с	и т	й у	к ф	л х	м ц	н ч	о ш	п щ
12	Ц Ч	а ы	б ь	в э	г ю	д я	е р	ж с	з т	и у	й ф	к х	л ц	м ч	н ш	о щ	п ъ
13	Ш Щ	а ь	б э	в ю	г я	д р	е с	ж т	з у	и ф	й х	к ц	л ч	м ш	н щ	о ъ	п ы
14	Ъ Ы	а э	б ю	в я	г р	д с	е т	ж у	з ф	и х	й ц	к ч	л ш	м щ	н ъ	о ы	п ь
15	Ь Э	а ю	б я	в р	г с	д т	е у	ж ф	з х	и ц	й ч	к ш	л щ	м ъ	н ы	о ь	п э
16	Ю Я	а я	б р	в с	г т	д у	е ф	ж х	з ц	и ч	й ш	к щ	л ъ	м ы	н ь	о э	п ю

и пароль «порт» зашифровать открытый текст «криптоалгоритм»

Задание 2 (ПКН-7)

Проведите шифрование и дешифрование слова «Криптоанализ» согласно схеме, представленной ниже на рисунке



Задание 3 (ПКН-2)

Согласно теореме

Любая приведенная система вычетов по модулю n представляет собой систему $\varphi(n)$ чисел $x_1, x_2, \dots, x_{\varphi(n)}$, где $x_i \not\equiv x_j \pmod{n}$ при $i \neq j$ и для всех i $\text{НОД}(x_i, n) = 1$.

Определите значение функции Эйлера в точке 12.

Задание 4 (ПКН-2)

Зашифровать текст «Шла Саша по шоссе» с помощью криптоалгоритма RSA при $p=971$ и $q=563$.

Задание 5 (ПКН-2)

Провести генерацию (детерминистическая) больших простых чисел по стандарту ГОСТ Р 34.10-94 согласно следующим условиям (см. рис. ниже)

Пусть $p = qN + 1$, где q – нечетное простое число, N – четное, и $p < (2q + 1)^2$. Число p является простым, если выполняются следующие два условия:

- 1) $2^{qN} \equiv 1 \pmod{p}$,
- 2) $2^N \not\equiv 1 \pmod{p}$.

Тесты (ПКН-7, ПКН-2)

Вопрос 1. (ПКН-7) Какой метод шифрации не применялся на заре становления криптографии?

- (1) Шифр Гая Юлия Цезаря
- (2) Шифр перестановки «считала»
- (3) Шифр Полибия
- (4) Шифр Чизкейка

Вопрос 2. (ПКН-7) После ВОВ в СССР задачи шифрации и дешифрации были переданы в ...

- (1) Радиодивизион Особого НАЗначения
- (2) Гидрометеослужбу СССР
- (3) МИД СССР
- (4) Специальную службу СССР

Вопрос 3. (ПКН-7, ПКН-2) Свойство информации, предотвращающее ее неавторизованное изменение или разрушение называется

- (1) целостность
- (2) аутентификация
- (3) верификация
- (4) электронная подпись

Вопрос 4. (ПКН-7) Советский и Российский стандарт симметричного шифрования, введенный в 1990 году

- (1) ГОСТ 3344-2006
- (2) ГОСТ 21874-98
- (3) ГОСТ 28147-89
- (4) ГОСТ 11345-91

Вопрос 5. (ПКН-2) Отношение эквивалентности не обладает свойством

- (1) рефлексивность
- (2) симметричность
- (3) антисимметричность
- (4) транзитивность

Вопрос 6. (ПКН-2) Каким свойством должны обладать элементы некоторого множества по отношению к некоторой операции между ними, чтобы образовать универсальную алгебру с множеством главных элементов и множеством главных операций?

- (1) замкнутость
- (2) ассоциативность
- (3) коммутативность
- (4) существование нейтрального элемента

Вопрос 7. (ПКН-2) Числа x и y называются равными (сравнимыми) по модулю натурального числа n , если и только если разность $x - y$

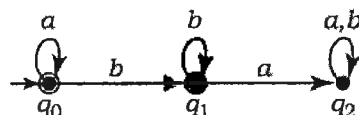
- (1) обратно пропорционален n
- (2) Извлекается корень n -й степени
- (3) Сопоставим с n
- (4) Делится на n

Вопрос 8. (ПКН-2) На рисунке ниже приведена таблица истинности булевых функций двух аргументов. Под каким обозначением находится функция с названием «штрих Шеффера»?

		0	·	\rightarrow	x	\leftarrow	y	+	\vee	\downarrow	\leftrightarrow	y'	\leftarrow	x'	\rightarrow		1
x	y	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

- (1) g_1
- (2) g_{14}
- (3) g_8
- (4) g_2

Вопрос 9. (ПКН-7, ПКН-2) Какой язык распознает конечный автомат



- (1) ab^*
- (2) a^*b^*
- (3) ba
- (4) b^*a

Вопрос 10. (ПКН-7, ПКН-2) Что не относится к вероятностным моделям источников открытых сообщений?

- (1) Стационарный источник независимых символов алфавита
- (2) Стационарный источник независимых биграмм
- (3) Стационарная модель полужависимых конечных грамматик
- (4) Стационарный источник марковски зависимых букв

Вопрос 11. (ПКН-7) Какой из свойств не относится к поточным методам шифрования

- (1) Передача гаммы в линию связи
- (2) Кодирование гаммы симметричным ключом до отправки в канал
- (3) Повторное использование гаммы
- (4) Восстановление текста, зашифрованного неравновероятной гаммой

Вопрос 12. (ПКН-7) Какой из пунктов не имеет отношения к режимам использования блочных шифров?

- (1) режим асимметричной открытой замены
- (2) с зацеплением блоков шифротекста;
- (3) с обратной связью по выходу;
- (4) с обратной связью по выходу и нелинейной функцией

Вопрос 13. (ПКН-7) Схема шифрования Эль-Гамала – это...

- (1) поточный шифр
- (2) блочный шифр в режиме шифрования с зацеплением
- (3) синхронный поточный шифр
- (4) криптосистема с открытым ключом

Вопрос 14. (ПКН-7, ПКН-2) Генератор g называется криптографически стойким псевдослучайным генератором, если для любой полиномиальной вероятностной машины Тьюринга A , для любого полинома p и всех достаточно больших n выполняется неравенство

- (1) $|P_1(A,n)-p(n)| < P_2(A,n)$
- (2) $|P_1(A,n)+P_2(A,n)| < 1/p(n)$
- (3) $|P_1(A,n)-P_2(A,n)| < 1/p(n)$
- (4) $|P_1(A,n)-P_2(A,n)| < p(n)$

Вопрос 15. (ПКН-7, ПКН-2) В число единиц криптостойкости не входит...

- (1) временная сложность наилучшего известного алгоритма, нарушающего безопасность
- (2) требуемый объем памяти для вскрытия ключа
- (3) сложность генератора ключа
- (4) физический объем вычислительной модели для вскрытия ключа

Вопрос 16. (ПКН-7) Какой из пунктов не входит в список направлений обеспечения информационной безопасности?

- (1) Аутентификация и идентификация
- (2) Управление доступом
- (3) Аудит и оповещение об опасности
- (4) Обеспечение отказуемости

Вопрос 17. (ПКН-7) В наши дни «PKI» больше ассоциируется с предоставляемыми инфраструктурой открытых ключей службами либо в виде приложений, либо в виде протоколов. Какой из ответов не имеет отношения к PKI?

- (1) Интерфейс SATA
- (2) протокол безопасных соединений SSL
- (3) программа шифрования PGP
- (4) протокол IPSec

Вопрос 18. (ПКН-7) Открытый торговый протокол Интернет определяет некоторое число различных операций IOTP, что не входит в их число?

- (1) Аутентификация
- (2) Постгарантийное обслуживание
- (3) Отзыв платежа
- (4) Депозит

Вопрос 19. (ПКН-7, ПКН-2) К методам аутентификации не относится

- (1) На основе применения электронной подписи
- (2) На основе параметров подлинности
- (3) На основе вещественной факторизации
- (4) На основе дискретного логарифмирования, связанного с простыми или с составными числами

Вопрос 20. (ПКН-7, ПКН-2) К аналоговым скремблерам не относится...

- (1) дискретный периодический
- (2) аналоговый частотный
- (3) аналоговый временной
- (4) двумерный

Ключ к тесту

Вопрос	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Ответ	4	4	1	3	3	1	4	2	2	3	2	1	4	3	3	4	1	2	3	1
Баллы	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Критерии оценки знаний при проведении устного/письменного опроса

Оценка «**отлично**» (зачтено) – выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания вопросов дисциплины.

Оценка «**хорошо**» (зачтено) – выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, но допускает в ответе некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «**удовлетворительно**» (зачтено) – выставляется обучающемуся, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными понятиями, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «**неудовлетворительно**» (не зачтено) – выставляется обучающемуся, который не знает большей части основного содержания вопросов тем дисциплины, допускает грубые ошибки в формулировках основных понятий.

Критерии оценки знаний при решении задач

Оценка «**отлично**» (зачтено) – выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания вопросов дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «**хорошо**» (зачтено) – выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «**удовлетворительно**» (зачтено) – выставляется обучающемуся, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными понятиями, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «**неудовлетворительно**» (не зачтено) – выставляется обучающемуся, который не знает большей части основного содержания вопросов тем дисциплины, допускает грубые ошибки в формулировках основных понятий, не умеет использовать полученные знания при решении типовых практических задач.

Критерии оценки знаний при проведении тестирования

Оценка «**отлично**» (зачтено) выставляется при условии правильного ответа студента не менее чем на 85 % тестовых заданий;

Оценка «**хорошо**» (зачтено) выставляется при условии правильного ответа студента не менее чем на 70 % тестовых заданий;

Оценка «**удовлетворительно**» (зачтено) выставляется при условии правильного ответа студента не менее чем на 51 %;

Оценка «**неудовлетворительно**» (не зачтено) выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.