Государственное образовательное учреждение
«Приднестровский государственный университет им. Т. Г. Шевченко»
Физико-технический институт
Физико-математический факультет
Кафедра высшей и прикладной математики и информатики

УТВЕРЖДАЮ
Зав. кафедры-разработчика

_____/Коровай А.В.

Протокол № 1 « 30 » 08 2024 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
По дисциплине

Б1.О.09 «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОДИРОВАНИЯ ДАННЫХ И КРИПТОГРАФИИ»

Направление
01.04.01 «Математика»

Профиль
«Математика. Преподавание математики и информатики»

Квалификация
магистр

Форма обучения
Очная

ГОД НАБОРА 2024

Разработал: доцент. кафедры
ВиПМиИ,
_____ / Малютина Н.Н.
(подпись)

«30» августа 2024 г.

Тирасполь 2024

Паспорт фонда оценочных средств по учебной дисциплине «Математические основы кодирования данных и криптографии»

1. В результате изучения дисциплины «Математические основы кодирования данных и криптографии» у обучающихся должны быть сформированы следующие компетенции:

Категория (группа) компетенций	Код и наименование	Код и наименование индикатора достижения универсальной компетенции
Обязательные профессиональные компетенции и индикаторы их достижения		
	ПК-1 Способен на самостоятельное построение целостной картины дисциплины	ИД-1$_{ПК-1}$ Знает: историю, теорию, закономерности и принципы построения и функционирования образовательных систем, роль и место образования в жизни личности и общества
		ИД-2$_{ПК-1}$ Умеет: разрабатывать и реализовывать программы учебных дисциплин в рамках основной общеобразовательной программы
		ИД-3$_{ПК-1}$ Владеет: формами и методами обучения, в том числе выходящими за рамки учебных занятий: проектная деятельность, лабораторные эксперименты, полевая практика и т.п.
	ПК-2. Владеет методами математического моделирования при анализе глобальных проблем на основе глубоких знаний фундаментальных математических дисциплин и компьютерных наук	ИД-1$_{ПК-2}$ Знает: преподаваемый предмет в пределах требований федеральных государственных образовательных стандартов и основной общеобразовательной программы, его истории и места в мировой культуре и науке
		ИД-2$_{ПК-2}$ Умеет: обеспечивать коммуникативную и учебную «включенности» всех учащихся в образовательный процесс (в частности, понимание формулировки задания, основной терминологии, общего смысла идущего в классе обсуждения)
		ИД-3$_{ПК-2}$ Владеет: предметно-педагогической ИКТ-компетентностью (отражающей профессиональную ИКТ-компетентность соответствующей области человеческой деятельности)
	ПК-7. Способен к организации учебной деятельности в конкретной предметной области (математика, физика, информатика)	ИД-1$_{ПК-7}$Знает: преподаваемый предмет в пределах требований федеральных государственных образовательных стандартов и основной общеобразовательной программы, его истории и места в мировой культуре и науке
		ИД-2$_{ПК-7}$ Умеет: использовать информационные источники, следить за последними открытиями в области математики и знакомить с ними обучающихся, квалифицированно набирать математический текст, проводить различия между точным и (или) приближенным математическим доказательством, в частности,

		компьютерной оценкой, приближенным измерением, вычислением и др.
		ИД-З$_{ПК-7}$ Владеет: основными математическими компьютерными инструментами визуализации данных, зависимостей, отношений, процессов, геометрических объектов; вычислений - численных и символьных; обработки данных (статистики); экспериментальных лабораторий (вероятность, информатика)

2. Программа оценивания контролируемой компетенции:

Текущая аттестация	**Контролируемые модули, разделы**	**Код контролируемой компетенции (или ее части)**	**Наименование оценочного средства**
№1	Коды. Расстояние Хэмминга. Линейные коды. Границы. Коды Хэмминга. Синдром. Циклические коды. БЧХ коды.	ПК-1; ПК-2; ПК-7	Контрольная работа №1 и сообщение №1, Контрольная работа №2 и сообщение №2
№2	N-арные квазигруппы. Коды с одним проверочным символом (ISBN-код). Тотально антикоммутативные квазигруппы. Ортогональность группоидов.	ПК-1; ПК-2; ПК-7	Контрольная работа №3 и сообщение №3
№3	Криптография. Шифры с симметрическим ключом. Алгоритм Марковского. Алгоритм Эль-Гамаля.	ПК-1; ПК-2; ПК-7	Контрольная работа №4 и сообщение №4
Промежуточная аттестация		**Код контролируемой компетенции (или ее части)**	**Наименование оценочного средства**
№1. (II семестр) зачет с оценкой		ПК-1; ПК-2; ПК-7	вопросы к зачету с оценкой
№2 (III семестр) экзамен		ПК-1; ПК-2; ПК-7	вопросы к экзамену, комплект билетов

Комплект вопросов для проведения зачета с оценкой по дисциплине «Математические основы кодирования данных и криптографии»
II семестр

1. Сравнения: некоторые свойства и теоремы.
2. Теорема Ферма.
3. Функция Эйлера.
4. Расширенный алгоритм Евклида.
5. Показатели и первообразные корни.
6. Вычисление наибольшего общего делителя и его линейного представления.
7. Китайская теорема об остатках.
8. Нахождение первообразных корней.
9. Алгоритмы факторизации.
10. Оптимизация переборного метода.
11. Метод вычисления индексов.
12. Метод Полларда.
13. Специальный случай дискретного логарифмирования по составному модулю.
14. Метод дискретного логарифмирования.
15. Открытое распределение ключей.
16. Гомоморфизмы групп двумерных векторов.
17. Группы четырехмерных векторов частного вида.
18. Строение примарных подгрупп.
19. Коды. Определение. Примеры.
20. Алгоритм Эль-Гамаля.
21. Построение поля Галуа порядка 4.
22. Построение поля Галуа порядка 9.
23. Построение кольца вычетов по модулю 6. Его нетривиальные идеалы.
24. Кольцо. Идеал.
25. Кольцо многочленов.
26. Построение поля порядка 7.
27. Ортогональность квазигрупп. Примеры.
28. Бинарные квазигруппы. Определение. Применение.
29. N-арные квазигруппы. Определение. Применение.
30. Построение левой квазигруппы порядка 5.
31. Построение правой квазигруппы порядка 6.
32. Порождающий многочлен кода.

Критерии оценки:

- 30 баллов выставляется студенту, если продемонстрированы знание вопроса и самостоятельность мышления, ответ соответствует требованиям правильности, полноты и аргументированности;
- 20 баллов в неполном, недостаточно четком и убедительном, но в целом правильном ответе;
- 10 баллов ставится, если студент отвечает неконкретно, слабо аргументировано и не убедительно, хотя и имеется какое-то представление о вопросе;
- меньше 10 баллов ставится, если студент отвечает неправильно, нечетко и неубедительно, дает неверные формулировки, в ответе отсутствует какое-либо представление о вопросе.

Комплект вопросов для проведения экзамена
по дисциплине «Математические основы кодирования данных и криптографии»
III семестр

1. Расстояние Хэмминга. Определение. Примеры.
2. Алгоритм Марковского.
3. Код Хэмминга. Определение. Примеры. Характеристики.
4. Криптография.
5. Построение кольца многочленов $F[x]/<(x_2+x+1)>$ над полем Галуа из трех элементов.
6. Линейные коды. Определение, свойства. Границы.
7. Шифры с симметрическим ключом. Примеры.
8. Построение пары ортогональных группоидов.
9. Построение тройки ортогональных группоидов.
10. Порождающая матрица линейного кода.
11. Проверочная матрица линейного кода.
12. Коды с одним проверочным символом (ISBN-код).
13. Построение тернарной квазигруппы порядка 4.
14. Синдром.
15. Декодирование кода Хэмминга.
16. БЧХ-коды. Определение. Свойства. Примеры.
17. Построение циклического кода.
18. Коды Рида-Соломона. Примеры. Свойства.
19. Криптосистема RSA.
20. Открытое распределение ключей.
21. Система Диффи-Хеллмана.
22. Распределение ключей в системе RSA.
23. Криптографические преобразования в RSA.
24. Вопросы выбора параметров в системе RSA.
25. Протокол бесключевого шифрования.
26. Открытое шифрование.
27. Способ Эль-Гамаля.
28. Способ Рабина.
29. Системы электронной цифровой подписи.
30. Схема Эль-Гамаля.
31. Американский стандарт DSA.
32. Российский стандарт ГОСТ Р 34.10-94.
33. Схема Онга-Шнорра-Шамира.
34. ЭЦП Шнорра.
35. Слепая подпись.
36. Слепая подпись на основе ЭЦП Шнорра.
37. Слепая подпись Чаума.
38. Схемы ЭЦП с восстановлением сообщения.
39. Схема RSA.
40. ЭЦП Рабина.
41. Схемы с восстановлением сообщения.
42. Новый подход к уменьшению размера подписей до 160 бит.
43. Схемы ЭЦП на основе сложности дискретного логарифмирования.
44. Схемы ЭЦП на основе сложности факторизации RSA-модуля.
45. Схемы ЭЦП с восстановлением сообщения.
46. Схемы ЭЦП с сокращённым размером подписи.
47. Синтез алгоритмов ЭЦП.
48. Протоколы формирования коллективной ЭЦП.

Критерии оценки:

- 30 баллов выставляется студенту, если продемонстрированы знание вопроса и самостоятельность мышления, ответ соответствует требованиям правильности, полноты и аргументированности;
- 20 баллов в неполном, недостаточно четком и убедительном, но в целом правильном ответе;
- 10 баллов ставится, если студент отвечает неконкретно, слабо аргументировано и не убедительно, хотя и имеется какое-то представление о вопросе;
- меньше 10 баллов ставится, если студент отвечает неправильно, нечетко и неубедительно, дает неверные формулировки, в ответе отсутствует какое-либо представление о вопросе.

Комплект вопросов для сообщений
по дисциплине «Математические основы кодирования данных и криптографии»
Семестр II
Сообщения №1 и №2.

33. Сравнения: некоторые свойства и теоремы.
34. Теорема Ферма.
35. Функция Эйлера.
36. Алгоритм Евклида.
37. Расширенный алгоритм Евклида.
38. Показатели и первообразные корни.
39. Теоремы о числе классов с заданным показателем.
40. Теоремы о числе решений степенных сравнений.
41. Вычисление наибольшего общего делителя и его линейного представления.
42. Китайская теорема об остатках.
43. Алгоритм быстрого возведения в степень по модулю.
44. Нахождение первообразных корней.
45. Нахождение чисел относящихся к заданному показателю.
46. Генерация простых чисел.
47. Детерминистическая генерация больших простых чисел.
48. Способ на основе подбора разложения функции Эйлера.
49. Способ по стандарту ГОСТ Р 34.10-94.
50. Извлечение квадратных корней по простому модулю.
51. Извлечение корней степени N>2 по простому модулю.
52. Случай модуля, равного степени простого числа.
53. Модуль со специальной структурой.
54. Вычисление корня большой простой степени.
55. Сведение трудных случаев извлечения корней к задаче дискретного логарифмирования.
56. Алгоритмы факторизации.
57. Факторизация B-гладкого модуля RSA.
58. Факторизация модуля RSA с использованием метода Флойда.
59. Оптимизация переборного метода.
60. Метод вычисления индексов.
61. Метод Полларда.
62. Случай составного порядка.
63. Специальный случай дискретного логарифмирования по составному модулю.
64. Метод дискретного логарифмирования.
65. Выполнение модульного умножения по Монтгомери.
66. Нахождение чисел заданного порядка.
67. Нахождение чисел простого порядка.
68. Элементы теории чисел.
69. Открытое распределение ключей.
70. Гомоморфизмы групп двумерных векторов.
71. Группы четырехмерных векторов частного вида.
72. Строение примарных подгрупп.

Критерий оценки сообщений №1 и №2	**Максимальный балл**
Соответствие содержания выступления сформулированной теме; степень раскрытия темы	2
Качество структуры выступления: композиция, логичность изложения, аргументированность, доказательность	2

Общая эрудиции: компетентность, использование специальной терминологии.	2
Авторские выводы и предложения по обсуждаемой проблематике. Проявление позиции студента по дискуссионным вопросам.	2
Культура выступления: четкость и доступность изложения, речевая культура, чувство времени.	1
Качество ответов на вопросы: полнота ответов, убедительность, готовность к дискуссии, наличие собственной позиции и умение ее отстаивать, доброжелательность, контактность	1
Итого максимум	10 (за одно сообщение)

Комплект вопросов для собеседования
по дисциплине «Математические основы кодирования данных и криптографии»
Семестр III

1. Открытое распределение ключей.
2. Система Диффи-Хеллмана.
3. Распределение ключей в системе RSA.
4. Криптографические преобразования в RSA.
5. Вопросы выбора параметров в системе RSA.
6. Криптосистема RSA.
7. Протокол бесключевого шифрования.
8. Коммутативные механизмы шифрования.
9. Применение в электронной игре в покер.
10. Открытое шифрование.
11. Способ Эль-Гамаля.
12. Способ Рабина.
13. Системы электронной цифровой подписи.
14. Схема Эль-Гамаля.
15. Американский стандарт DSA.
16. Российский стандарт ГОСТ Р 34.10-94.
17. Схема Онга-Шнорра-Шамира.
18. ЭЦП Шнорра.
19. Класс доказуемо стойких криптосистем.
20. Минимизация числа расшифрованных текстов.
21. Слепая подпись.
22. Слепая подпись на основе ЭЦП Шнорра.
23. Слепая подпись Чаума.
24. Схемы ЭЦП с восстановлением сообщения.
25. Схема RSA.
26. ЭЦП Рабина.
27. Экзистенциальное подделка подписи и потайные каналы в системах ЭЦП.
28. Схемы с формированием подписей на основе решения системы сравнений.
29. Схемы с RSA- модулем.
30. Применение простого модуля в схемах, основанных на сложности факторизации.
31. Схемы с восстановлением сообщения.
32. Новые схемы ЭЦП с сокращённой длиной подписи.
33. Новый подход к уменьшению размера подписей до 160 бит.
34. Схемы подписи на основе сложности извлечения корней в группах известного порядка.
35. Схема подписи с двухэлементным секретным ключом.
36. Схема подписи с двухэлементным открытым ключом.
37. Конечные группы и поля над векторными пространствами как примитив алгоритмов ЭЦП.
38. Правила умножения базисных векторов.
39. Таблицы умножения базисных векторов для различных случаев.
40. Поля многомерных векторов.
41. Схемы ЭЦП на основе сложности дискретного логарифмирования.
42. Схемы ЭЦП на основе сложности факторизации RSA-модуля.
43. Схемы ЭЦП с восстановлением сообщения.
44. Схемы ЭЦП с сокращённым размером подписи.
45. Генерация числовых примеров.
46. Обзор по схемам ЭЦП.
47. Синтез алгоритмов ЭЦП.

48. Протоколы формирования коллективной ЭЦП.
49. Некоммутативные группы как криптографический примитив.
50. Как запатентовать алгоритм ЭЦП.

Критерий оценки сообщения №3 и №4	**Максимальный балл**
Соответствие содержания выступления сформулированной теме; степень раскрытия темы	2
Качество структуры выступления: композиция, логичность изложения, аргументированность, доказательность	2
Общая эрудиции: компетентность, использование специальной терминологии.	2
Авторские выводы и предложения по обсуждаемой проблематике. Проявление позиции студента по дискуссионным вопросам.	2
Культура выступления: четкость и доступность изложения, речевая культура, чувство времени.	1
Качество ответов на вопросы: полнота ответов, убедительность, готовность к дискуссии, наличие собственной позиции и умение ее отстаивать, доброжелательность, контактность	1
Итого максимум	10 (за одно сообщение)

Комплект заданий для проведения контрольных работ
по дисциплине «*Математические основы кодирования данных и криптографии*»
Семестр II
Контрольная работа №1

Задача 1. Зашифровать **шифром Полибия** следующий текст: «One fire drives out another». Шифр-алфавит состоит из 25 букв, а таблица шифрования имеет вид:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I-J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Задача 2. Зашифровать **шифром Полибия** следующий текст: «1) Уметь наслаждаться прожитой жизнью – значит жить дважды». Таблица шифрования имеет вид:

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	,	.	-

Задача 3. Зашифровать **шифром Цезаря,** с ключом $\boldsymbol{k = 3}$ следующий текст: «Eaten bread is soon forgotten».Таблица шифрования имеет вид:

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Задача 4. Закодировать **шифром Цезаря (буква кодируется предшествующей ей)** и **перестановочным шифром** следующее изречение: «Жизнь не для того, чтобы ждать пока стихнет буря. Она для того, чтобы танцевать под дождём.»

Задача 5. Закодировать **шифром Цезаря (буква кодируется предшествующей ей за две позиции)** и перестановочным шифром следующее изречение: «У людей нет нехватки силы, у них есть нехватка воли.»

Оценочный лист к письменной контрольной работе №1
по дисциплине «*Математические основы кодирования данных и криптографии*»

№ п/п	Ф.И.О. студента	Задание 1	Задание 2	Задание 3	Задание 4	Задание 5	Общее число баллов
	Количество баллов	0-3	0-3	0-3	0-3	0-3	0-15

Критерии оценки контрольной работы:
Максимальное количество возможных баллов – 15.
Отметка «2» ставится от 0 до 8 баллов
Отметка «3» ставится от 9- 11 баллов.
Отметка «4» ставится от 12 - 13 баллов.
Отметка «5» ставится за 14 - 15 баллов.

Контрольная работа №2

Задача 1. Зашифровать **шифром Альберти** с двумя шифроалфавитами текст: «Provision in season makes a rich house». Данная система шифрования использует два шифроалфавита:

0)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
1)	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**
2)	**M**	**N**	**B**	**V**	**C**	**X**	**Z**	**L**	**K**	**J**	**H**	**G**	**F**	**D**	**S**	**A**	**P**	**O**	**I**	**U**	**Y**	**T**	**R**	**E**	**W**	**Q**

Строка (0)– исходный алфавит.
Строка (1)– первый шифроалфавит.
Строка (2)– второй шифроалфавит.

Задача 2. Зашифровать с помощью **квадрата Виженера** текст: «A just war is better than an unjust peace». Данная система шифрования использует таблицу:

0		**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
1	**A**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
2	**B**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**
3	**C**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**
4	**D**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**
5	**E**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**
6	**F**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**
7	**G**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**
8	**H**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**
9	**I**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
10	**J**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
11	**K**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**
12	**L**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**
13	**M**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**
14	**N**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
15	**O**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**

16	**P**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**
17	**Q**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**
18	**R**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**
19	**S**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**
20	**T**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**
21	**U**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**
22	**V**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**
23	**W**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**
24	**X**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**
25	**Y**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**
26	**Z**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**

Задача 3. Зашифровать с помощью **квадрата Виженера** со строками, определенными ключевым словом **SCIENCE**: текст: «**The mad dog bites his master**». Данная система шифрования использует таблицу:

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
S	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
C	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
I	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**
E	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**
N	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**
C	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**
E	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**

Задача 4. Зашифровать с помощью **шифра Плейфера** со строками, определенными ключевым словом **EGYPT**: текст: «**Many hands make light work**». Для шифрования используется таблица:

E	**G**	**Y**	**P**	**T**
A	**B**	**C**	**D**	**F**
H	**I-J**	**K**	**L**	**M**
N	**O**	**Q**	**R**	**S**
U	**V**	**W**	**X**	**Z**

Задача 5. Зашифровать с помощью **шифра ADFGVX** со строками, определенными ключевым словом **IMAGE** текст: «**Frugality is a handsome income**». Для шифрования используется таблица:

	A	**D**	**F**	**G**	**V**	**X**
A	**O**	**P**	**F**	**0**	**Z**	**C**
D	**G**	**3**	**B**	**H**	**4**	**K**
F	**A**	**1**	**7**	**J**	**R**	**2**
G	**5**	**6**	**L**	**D**	**E**	**T**
V	**V**	**M**	**S**	**N**	**Q**	**I**
X	**U**	**W**	**9**	**X**	**Y**	**8**

Оценочный лист к письменной контрольной работе №2
по дисциплине «*Математические основы кодирования данных и криптографии*»

№ п/п	Ф.И.О. студента	Задание 1	Задание 2	Задание 3	Задание 4	Задание 5	Общее число баллов

	Количество баллов	0-3	0-3	0-3	0-3	0-3	0-15

Критерии оценки контрольной работы:
Максимальное количество возможных баллов – 15.
Отметка «2» ставится от 0 до 8 баллов
Отметка «3» ставится от 9- 11 баллов.
Отметка «4» ставится от 12 - 13 баллов.
Отметка «5» ставится за 14 - 15 баллов.

Семестр III

Контрольная работа №3

Задача 1. Зашифровать **шифром Хилла** со строками, определенными ключевым словом **IMAGE**: текст: «**Sparing is the first gaining**». Для шифрования используется таблица:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
0	1	2	3	4	5	6	7	8	9	10	11	12	13
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**@**	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Шифровальная матрица с определителем 1: $\mathbf{A} = \begin{pmatrix} \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{5} \end{pmatrix}$.

Матрицей для расшифровки будет обратная матрица: $\mathbf{A^{-1}} = \begin{pmatrix} \mathbf{5} & \mathbf{-3} \\ \mathbf{-3} & \mathbf{2} \end{pmatrix}$.

Задача 2. Определить сколько потребуется ключей для организации парной секретной связи в сети, состоящей из 1000 абонентов; из 100000000 абонентов.

Задача 3. Вычислить секретные ключи $\boldsymbol{Y_A}$, $\boldsymbol{Y_B}$ и общий ключ $\boldsymbol{Z_{AB}}$ для системы Диффи–Хеллмана с параметрами:

$$\mathbf{1)}\ \boldsymbol{p} = \mathbf{23}, \boldsymbol{g} = \mathbf{5}, \boldsymbol{X_A} = \mathbf{5},\ \boldsymbol{X_B} = \mathbf{7},$$
$$\mathbf{2)}\ \boldsymbol{p} = \mathbf{19}, \boldsymbol{g} = \mathbf{2}, \boldsymbol{X_A} = \mathbf{5},\ \boldsymbol{X_B} = \mathbf{7},$$
$$\mathbf{3)}\ \boldsymbol{p} = \mathbf{23}, \boldsymbol{g} = \mathbf{7}, \boldsymbol{X_A} = \mathbf{3},\ \boldsymbol{X_B} = \mathbf{4},$$

Задача 4. Для шифра Шамира с заданными параметрами $\boldsymbol{p}$, $\mathrm{c}_{\boldsymbol{A}}$, $\mathrm{c}_{\boldsymbol{B}}$ найти недостающие параметры и описать процесс передачи сообщения $\boldsymbol{m}$ от $\boldsymbol{A}$ к $\boldsymbol{B}$:

$$\mathbf{1)}\ \boldsymbol{p} = \mathbf{23}, \boldsymbol{m} = \mathbf{6}, \mathrm{c}_{\boldsymbol{A}} = \mathbf{15},\ \mathrm{c}_{\boldsymbol{B}} = \mathbf{7},$$
$$\mathbf{2)}\ \boldsymbol{p} = \mathbf{19}, \boldsymbol{m} = \mathbf{4}, \mathrm{c}_{\boldsymbol{A}} = \mathbf{5},\ \mathrm{c}_{\boldsymbol{B}} = \mathbf{7},$$
$$\mathbf{3)}\ \boldsymbol{p} = \mathbf{17}, \boldsymbol{m} = \mathbf{9}, \mathrm{c}_{\boldsymbol{A}} = \mathbf{3},\ \mathrm{c}_{\boldsymbol{B}} = \mathbf{13}.$$

Задача 5. Для шифра Эль-Гамаля с заданными параметрами $\boldsymbol{p}$, $\boldsymbol{g}$, $\mathrm{c}_{\boldsymbol{B}}$, $\boldsymbol{k}$ найти недостающие параметры и описать процесс передачи сообщения $\boldsymbol{m}$ пользователю $\boldsymbol{B}$:

$$\mathbf{1)}\ \boldsymbol{p} = \mathbf{19}, \boldsymbol{g} = \mathbf{2},\ \mathrm{c}_{\boldsymbol{B}} = \mathbf{5}, \boldsymbol{k} = \mathbf{7}, \boldsymbol{m} = \mathbf{5},$$
$$\mathbf{2)}\ \boldsymbol{p} = \mathbf{23}, \boldsymbol{g} = \mathbf{5},\ \mathrm{c}_{\boldsymbol{B}} = \mathbf{8}, \boldsymbol{k} = \mathbf{10}, \boldsymbol{m} = \mathbf{10},$$
$$\mathbf{3)}\ \boldsymbol{p} = \mathbf{17}, \boldsymbol{g} = \mathbf{3},\ \mathrm{c}_{\boldsymbol{B}} = \mathbf{10}, \boldsymbol{k} = \mathbf{5}, \boldsymbol{m} = \mathbf{10}.$$

Оценочный лист к письменной контрольной работе №3
по дисциплине «*Математические основы кодирования данных и криптографии*»

№ п/п	Ф.И.О. студента	Задание 1	Задание 2	Задание 3	Задание 4	Задание 5	Общее число баллов
	Количество баллов	0-3	0-3	0-3	0-3	0-3	0-15

Критерии оценки контрольной работы:
Максимальное количество возможных баллов – 15.
Отметка «2» ставится от 0 до 8 баллов
Отметка «3» ставится от 9- 11 баллов.
Отметка «4» ставится от 12 - 13 баллов.
Отметка «5» ставится за 14 - 15 баллов.

Контрольная работа №4

Задача 1. В системе RSA с заданными параметрами $\boldsymbol{P_A, Q_A, d_A}$, найти недостающие параметры и описать процесс передачи сообщения $\boldsymbol{m}$ пользователю $\boldsymbol{A}$:

1) $\boldsymbol{P_A = 5, Q_A = 11, d_A = 3, m = 12}$,

2) $\boldsymbol{P_A = 5, Q_A = 13, d_A = 5, m = 20}$,

3) $\boldsymbol{P_A = 7, Q_A = 11, d_A = 7, m = 17}$.

Задача 2. Пользователю ***RSA*** с параметрами $\boldsymbol{N = 187, d = 3}$ передано зашифрованное сообщение $\boldsymbol{e = 100}$. Расшифровать это сообщение, взломав систему ***RSA.***

Задача 3. Описать процесс проверки подлинности электронной подписи, полученной на базе схемы RSA с параметрами:

1) $\boldsymbol{P = 5, Q = 11, d = 3, \bar{m} = abbbaa}$.

2) $\boldsymbol{P = 7, Q = 11, c = 43, m = 5, h(m) = m}$.

Задача 4. Для указанных открытых ключей пользователя RSA проверить подлинность подписанных сообщений: $\boldsymbol{N = 65, d = 5, \langle 6, 42\rangle, \langle 10, 30\rangle, \langle 6, 41\rangle}$.

Задача 5. Описать процесс проверки подлинности электронной подписи, полученной на базе схемы Эль-Гамаля с параметрами:

1) $\boldsymbol{p = 23, g = 5, x = 7, \bar{m} = baaaab, k = 5}$.

2) $\boldsymbol{p = 23, g = 5, x = 7, \bar{m} = baaaab, k = 5}$.

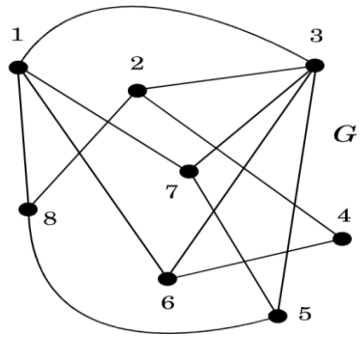
Задача 6. Абоненты некоторой сети применяют подпись Эль-Гамаля с общими параметрами $\boldsymbol{p = 23, g = 5}$. Для указанных секретных параметров абонентов найти открытый ключ $(\boldsymbol{y})$ и построить подпись для сообщения $\boldsymbol{m}$:

1) $\boldsymbol{x = 11, k = 3, m = h = 15}$,

2) $\boldsymbol{x = 10, k = 15, m = h = 5}$.

Задача 7. Пусть **Алиса** и **Боб** хотят честно раздать три карты: тройку $(\boldsymbol{\alpha})$, семерку $(\boldsymbol{\beta})$ и туза $(\boldsymbol{\gamma})$. Пусть на предварительном этапе выбраны следующие параметры: $\boldsymbol{p = 23,\ \widehat{\alpha} = 2,\ \widehat{\beta} = 3,\ \widehat{\gamma} = 5}$. Опишите процесс игры**,** если известными параметрами ментального покера являются**:** $\boldsymbol{c_A = 7, c_B = 9}$.

Задача 8. Дан граф $\boldsymbol{G}$, изображенный ниже. Используя гамильтонов цикл **8, 2, 4, 6, 3, 5, 7, 1** произвести шифрование матрицы с помощью системы RSA с параметрами $\boldsymbol{N = 55}$, $\boldsymbol{d = 3}$. Дать описание протокола доказательства.



Задание 9. 1) Определить по 16-ти значному номеру кредитной карты является ли она действительной двумя способами. А) 1573 2674 2396 3458; Б) 3762 4673 7624 4567. 2) Определить по13-ти значному номеру штрихкода является ли он действительным двумя способами. А) 3267423963458; Б) 2467762445673.

Задание 10. Определите значение утерянной цифры в штрихкоде, а именно, цифры $\boldsymbol{X}$ в следующем коде: А) 3267423 $\boldsymbol{X}$ 63458; Б) 246 $\boldsymbol{X}$ 762445673.

Оценочный лист к письменной контрольной работе №4
по дисциплине «*Математические основы кодирования данных и криптографии*»

№ п/п	Ф.И.О. студента	Задание 1	Задание 2	Задание 3	Задание 4	Задание 5	Задание 6	Задание 7	Задание 8	Задание 9	Задание 10	Общее число баллов
	Количество баллов	0-1,5	0-1,5	0-1,5	0-1,5	0-1,5	0-1,5	0-1,5	0-1,5	0-1,5	0-1,5	0-15

Критерии оценки контрольной работы:
Максимальное количество возможных баллов – 15.
Отметка «2» ставится от 0 до 8 баллов
Отметка «3» ставится от 9- 11 баллов.
Отметка «4» ставится от 12 - 13 баллов.
Отметка «5» ставится за 14 - 15 баллов.