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.В.02 «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОДИРОВАНИЯ ДАННЫХ И КРИПТОГРАФИИ»

Направление
01.04.01 «Математика»

Профиль
«Математика. Преподавание математики и информатики»

Квалификация
магистр

Форма обучения
Очная

ГОД НАБОРА 2023

Разработал: проф. кафедры
ВиПМиИ,
_____/ Щербаков В.А.
(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-3$_{ПК-7}$ 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	Самостоятельное решение упражнений по разделу «Коды».
№2	N-арные квазигруппы. Коды с одним проверочным символом (ISBN-код). Тотально антикоммутативные квазигруппы. Ортогональность группоидов.	ПК-1; ПК-2; ПК-7	Самостоятельное решение упражнений по разделу «N-арные квазигруппы».
№3	Криптография. Шифры с симметрическим ключом. Алгоритм Марковского. Алгоритм Эль-Гамаля.	ПК-1; ПК-2; ПК-7	Самостоятельное решение упражнений по разделу «Криптография»; Самостоятельный разбор тем: «Шифры с симметрическим ключом», «Система RSA».
Промежуточная аттестация		**Код контролируемой компетенции (или ее части)**	**Наименование оценочного средства**
№1. (семестр 3) зачет с оценкой		ПК-1; ПК-2; ПК-7	вопросы к зачету с оценкой

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

1. Коды. Определение. Примеры.
2. Алгоритм Эль-Гамаля.
3. Постройте поле Галуа порядка 4, порядка 9.
4. Расстояние Хэмминга. Определение. Примеры.
5. Алгоритм Марковского.
6. Постройте кольцо вычетов по модулю 6. Укажите его нетривиальные идеалы.
7. Код Хэмминга. Определение. Примеры. Характеристики.
8. Криптография.
9. Постройте кольцо многочленов $F[x]/<(x_2+x+1)>$ над полем Галуа из трех элементов.
10. Линейные коды. Определение, свойства. Границы.
11. Шифры с симметрическим ключом. Приведите примеры.
12. Постройте пару ортогональных группоидов. Тройку ортогональных группоидов.
13. Порождающая и проверочная матрица линейного кода.
14. Коды с одним проверочным символом (ISBN-код).
15. Постройте 3-арную квазигруппу порядка 4.
16. Синдром. Декодирование кода Хэмминга.
17. Кольцо. Идеал. Кольцо многочленов.
18. Ортогональность квазигрупп. Примеры.
19. БЧХ-коды. Определение. Свойства. Примеры.
20. Квазигруппы. Бинарные и n-арные. Определение. Применение.
21. Приведите пример циклического кода.
22. Коды Рида-Соломона. Примеры. Свойства.
23. Кольцо. Идеал. Кольцо многочленов.
24. Постройте левую квазигруппу порядка 6.
25. Криптосистема RSA.
26. Порождающий многочлен кода.
27. Постройте поле порядка 7.

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 заданий для самостоятельных работ по дисциплине

«*Математические основы кодирования данных и криптографии*»

Задача 1. Зашифровать **шифром Полибия** следующий текст: «**Mathematics and modern civilization**». 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 Цезаря,** с ключом $\boldsymbol{k = 3}$ следующий текст: «**Mathematics and modern civilization**».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 3. Зашифровать **шифром Альберти** с двумя шифроалфавитами текст: «**Mathematics and modern civilization**». 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 4. Зашифровать с помощью **квадрата Виженера** текст: «**Mathematics and modern civilization**». 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 5. Зашифровать с помощью **квадрата Виженера** со строками, определенными ключевым словом **SCIENCE**: текст: «**Mathematics and modern civilization**». 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 6. Зашифровать с помощью **шифра Плейфера** со строками, определенными ключевым словом **EGYPT**: текст: «**Mathematics and modern civilization**». 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 7. Зашифровать с помощью **шифра ADFGVX** со строками, определенными ключевым словом **IMAGE** текст: «**Mathematics and modern civilization**». 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

Задача 8. Зашифровать **шифром Хилла** со строками, определенными ключевым словом **IMAGE**: текст: «**Mathematics and modern civilization**». 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 9. Определить сколько потребуется ключей для организации парной секретной связи в сети, состоящей из 1000 абонентов; из 100000000 абонентов.

Задача 10. 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 11. 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 12. 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 $\boldsymbol{B}$:

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

Задача 13. В системе RSA с заданными параметрами $\boldsymbol{P_A}, \boldsymbol{Q_A}, \boldsymbol{d_A}$, найти недостающие параметры и описать процесс передачи сообщения $\boldsymbol{m}$ пользователю $\boldsymbol{A}$:

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

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

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

Задача 14. Пользователю $\boldsymbol{RSA}$ с параметрами $\boldsymbol{N} = \mathbf{187}, \boldsymbol{d} = \mathbf{3}$ передано зашифрованное сообщение $\boldsymbol{e} = \mathbf{100}$. Расшифровать это сообщение, взломав систему $\boldsymbol{RSA}$.

Задача 15. Описать процесс проверки подлинности электронной подписи, полученной на базе схемы RSA с параметрами:

$$\mathbf{1)}\ \boldsymbol{P} = \mathbf{5}, \boldsymbol{Q} = \mathbf{11}, \boldsymbol{d} = \mathbf{3}, \overline{\boldsymbol{m}} = \boldsymbol{abbbaa}.$$
$$\mathbf{2)}\ \boldsymbol{P} = \mathbf{7}, \boldsymbol{Q} = \mathbf{11}, \boldsymbol{c} = \mathbf{43}, \boldsymbol{m} = \mathbf{5}, \boldsymbol{h}(\boldsymbol{m}) = \boldsymbol{m}.$$

Задача 16. Для указанных открытых ключей пользователя RSA проверить подлинность подписанных сообщений: $\boldsymbol{N} = \mathbf{65}, \boldsymbol{d} = \mathbf{5}, \langle \mathbf{6}, \mathbf{42} \rangle, \langle \mathbf{10}, \mathbf{30} \rangle, \langle \mathbf{6}, \mathbf{41} \rangle$.

Задача 17. Описать процесс проверки подлинности электронной подписи, полученной на базе схемы Эль-Гамаля с параметрами:

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

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

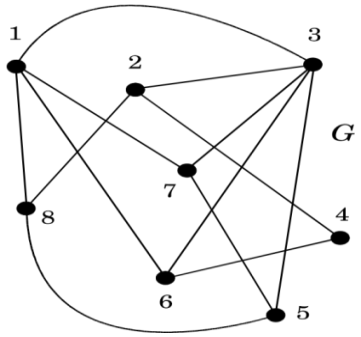
Задача 18. Абоненты некоторой сети применяют подпись Эль-Гамаля с общими параметрами $\boldsymbol{p = 23, g = 5}$. Для указанных секретных параметров абонентов найти открытый ключ $(\boldsymbol{y})$ и построить подпись для сообщения $\boldsymbol{m}$:

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

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

Задача 19. 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: $\boldsymbol{p = 23}$, $\boldsymbol{\widehat{\alpha} = 2}$, $\boldsymbol{\widehat{\beta} = 3}$, $\boldsymbol{\widehat{\gamma} = 5}$. Опишите процесс игры**,** если известными параметрами ментального покера являются**:** $\boldsymbol{c_A = 7, c_B = 9}$.

Задача 20. 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.



Критерии оценки:

30 баллов выставляется студенту, если выполнил 18-20 практических заданий для самостоятельной работы.

20 баллов выставляется студенту, если выполнил 14-17 практических заданий для самостоятельной работы.

10 баллов выставляется студенту, если выполнил 10-13 практических заданий для самостоятельной работы.

0 баллов выставляется студенту в случаях выполнения менее 10 заданий для самостоятельной работы.