

23 2022

**Рабочая программа дисциплины
Б1.В.03 Защита информации**

**01.03.02 Прикладная математика и информатика
Математическое и информационное моделирование**

4

7

72

7

16

10

2022

1. Место дисциплины в структуре ОП

2. Планируемые результаты обучения по дисциплине

УК-8.	Знать: Уметь: Владеть:
ПК-1. -	Знает - Умеет - Владеет -

Лабораторная работа 1 "Реализация методов хеширования".

Задание 1. ruscryptodome SHA3-
кеccak -

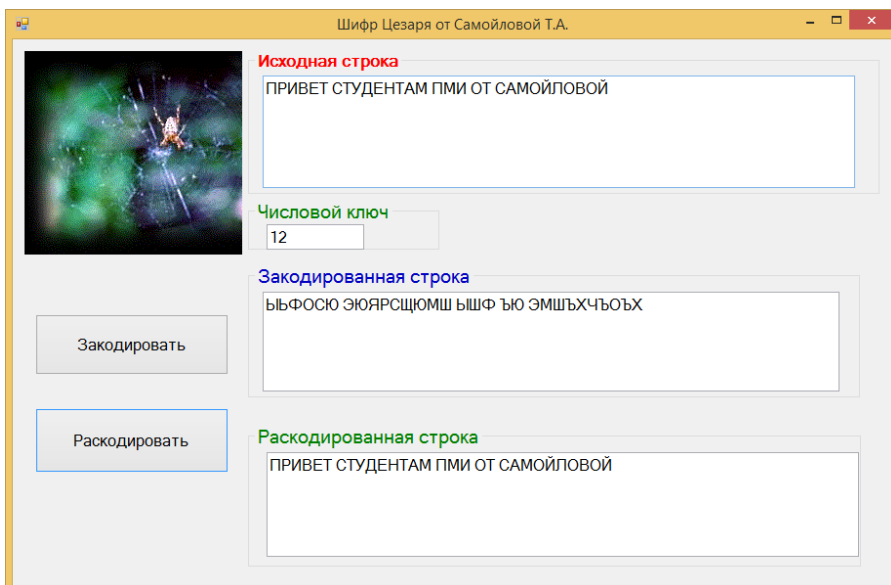
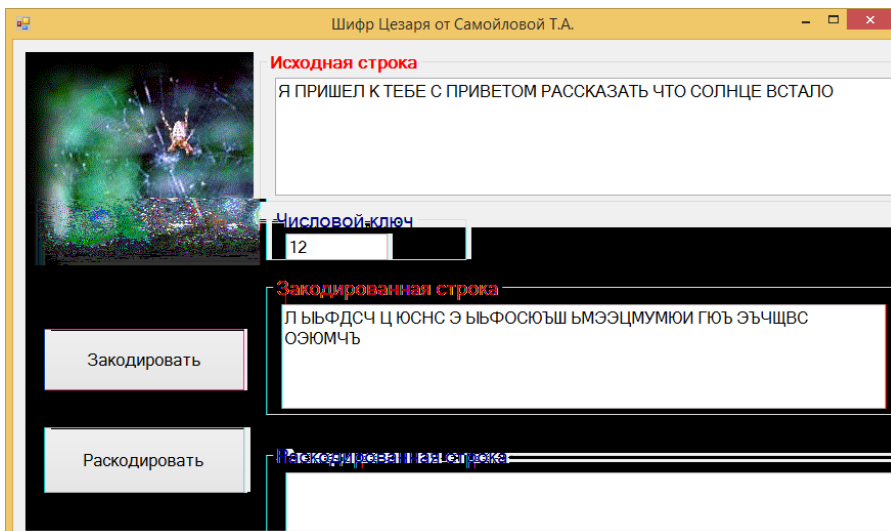
Задание 2
3-

Задание 3 ruscryptodome HMAC

Вычисление MAC SHA
MAC

Лабораторная работа 2 "Шифры замены в симметричных криптосистемах".

Задание 1. VS C



Задание 2

VS C

Задание 3.

VS C

Лабораторная работа 3 "Современная симметричная криптография алгоритмом AES".

Задание 1.

Python -

AES

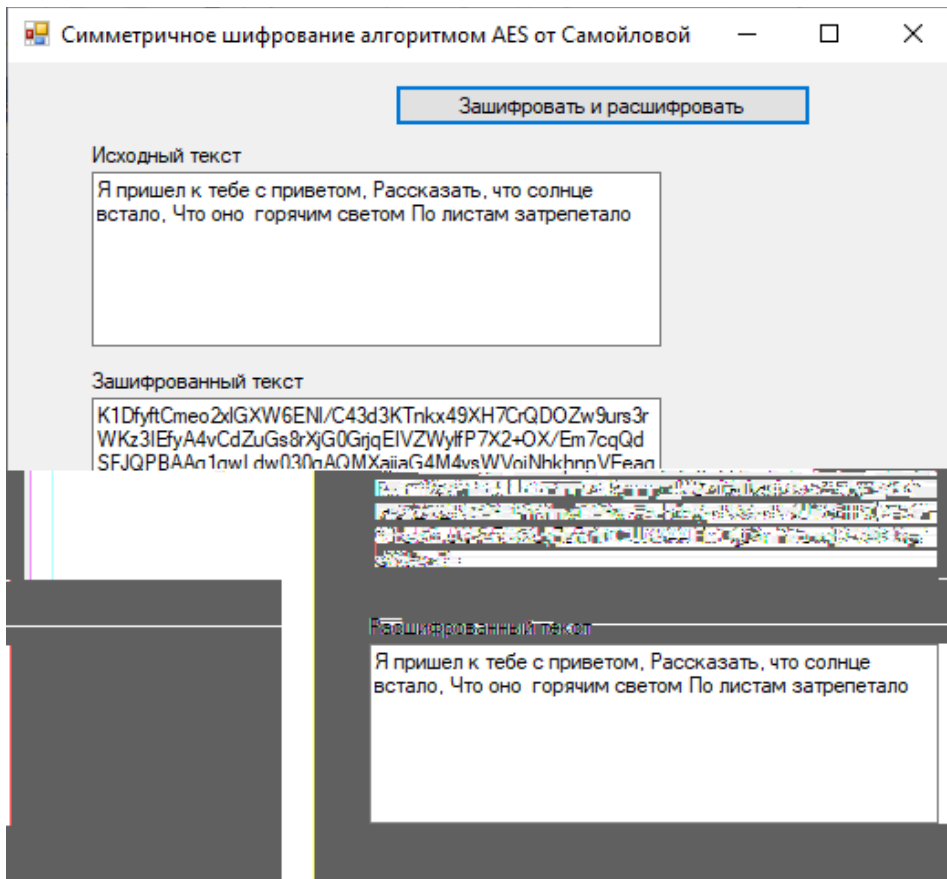
Варианты заданий к лабораторной работе

1	ECB
2	CFB
3	CBC
4	CCM
5	CTR
6	EAX
7	GCM
8	OCB
9	OFB

Задание 2.

IV

CBC.



Варианты задания к лабораторной работе

1	PKCS7
2	ANSIX923
3	PKCS7
4	None
5	ISO10126
6	Zeros
7	PKCS7
8	ANSIX923
9	ISO10126
10	Zeros
11	None
12	ISO10126

Лабораторная работа 4. «Современные поточные шифры»

Задание 1.

Python -

RC4.

Задание 2.

Python -

ChaCha20.

Задание 3.

Python -

ChaCha20_Poly1305.

Лабораторная работа 5. « Асимметричное

Задание 1.

ECDiffieHellmanCng

DH + AES),

Задание 2.

-

PyDH):

-
-
-
-

Задание 3.

Python -

RSA:

-
-
-

public.pem, private.pem

Лабораторная работа 6 " Электронная цифровая подпись".

Задание 1.

RSA.

WORD-

Задание 2 Разработайте десктоп - приложения для реализации ЭЦП:

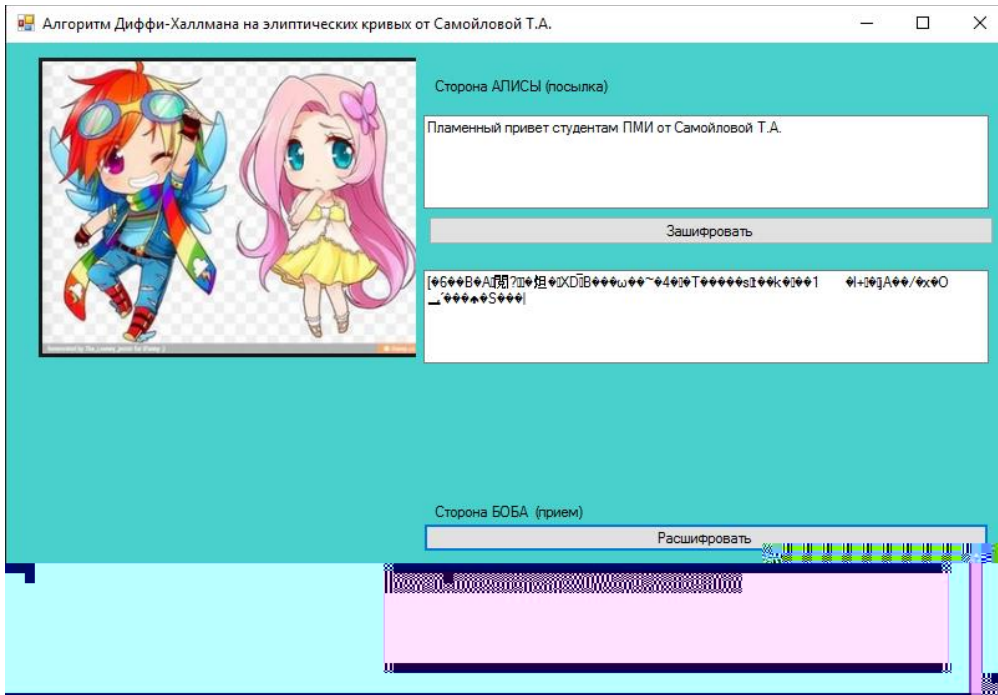
-
-

XML-

Word-

Задание 3.

Security.Cryptography.X509Certificates.

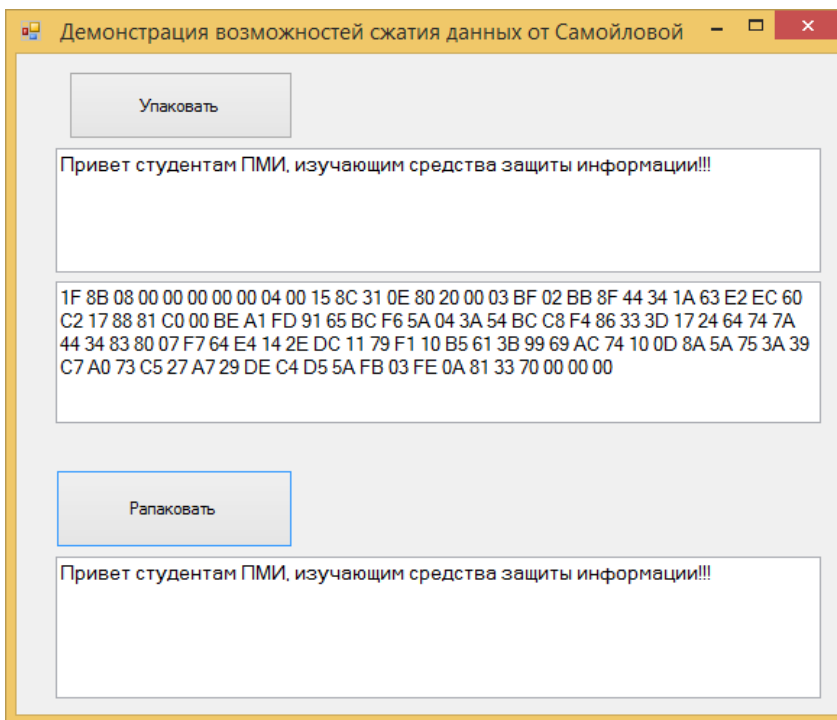


Лабораторная работа 7 " Методы сжатия информации "

Задание 1

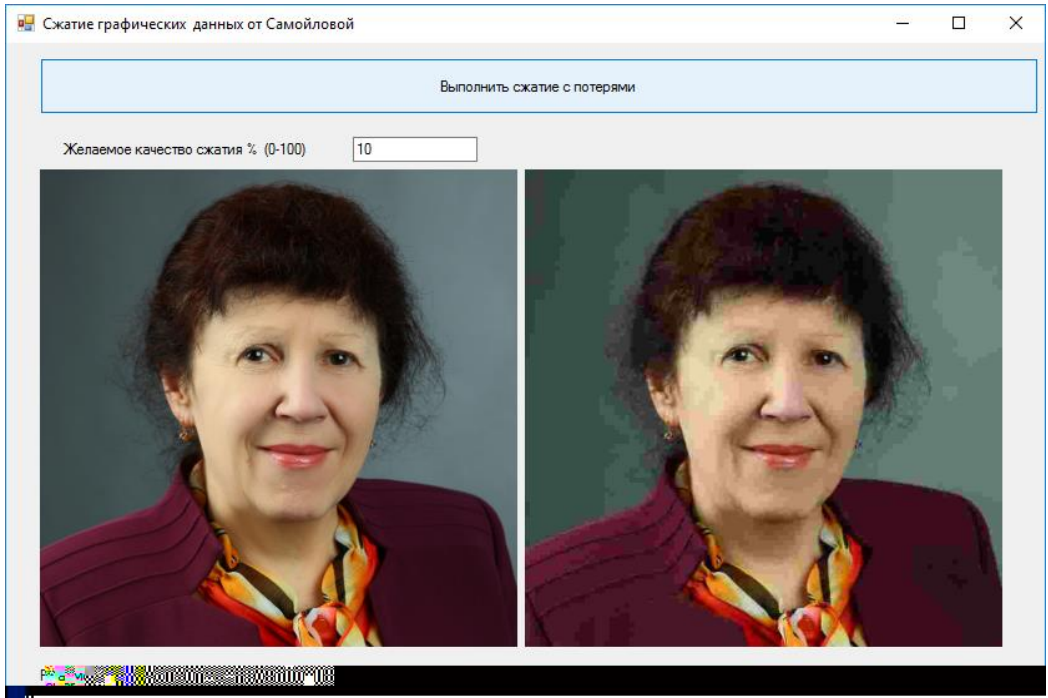
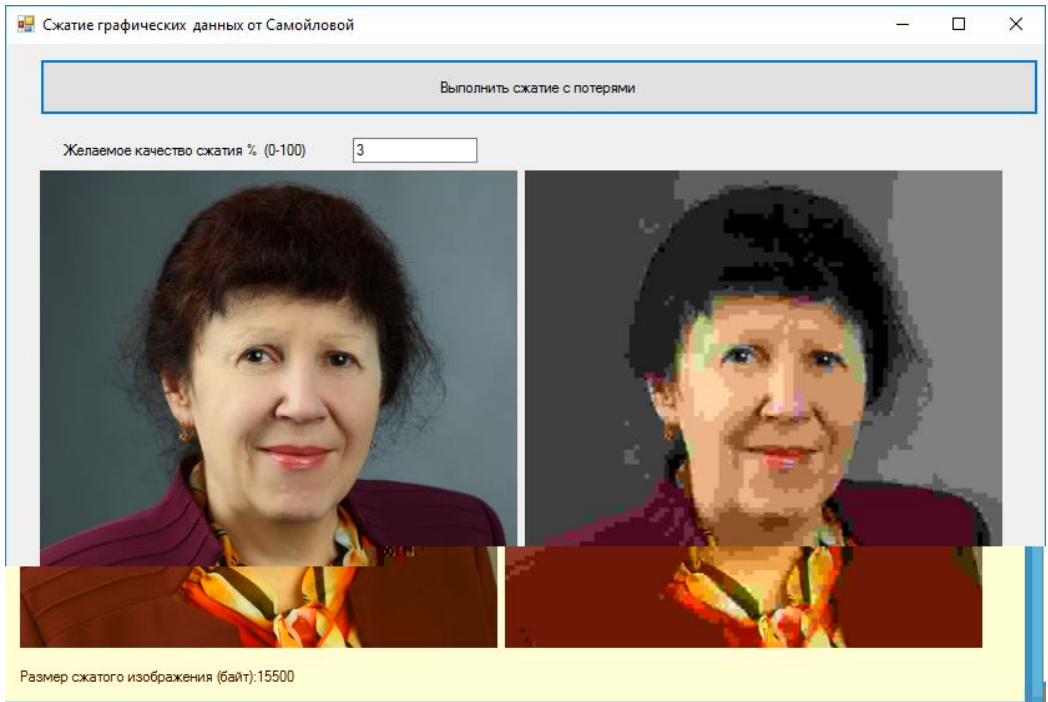
C# , без использования библиотечных средств System.IO.Compression, RLE.

Задание 2. GZipStream



Задание 3

C

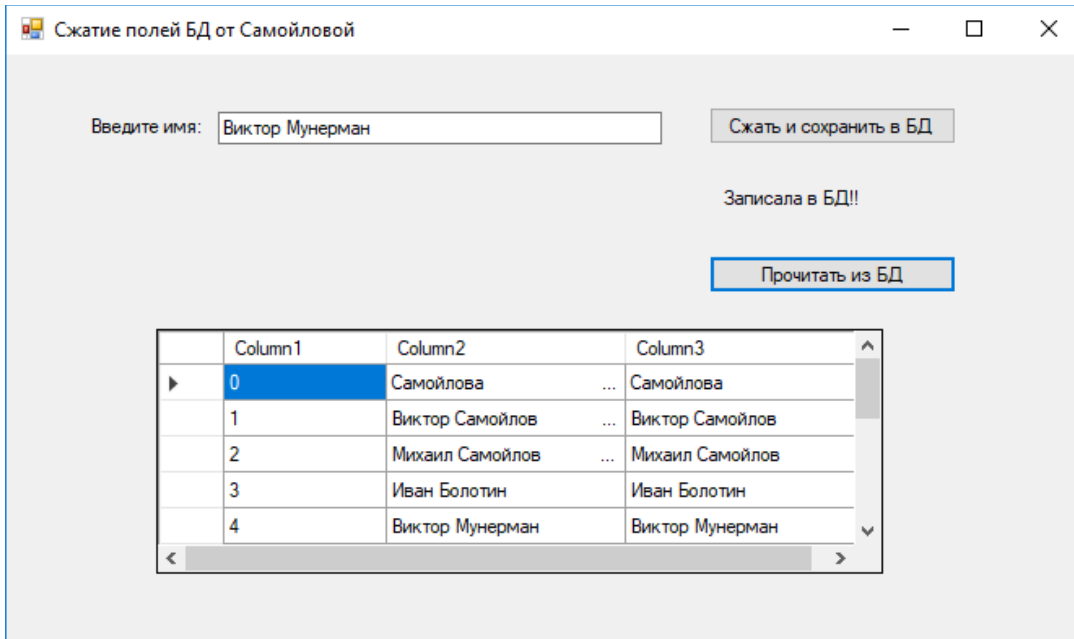


Задание 4.
varbinary(max)

поле

LZ77)
Entity Framework + LINQ

-
GZipStream (System.IO.Compression.

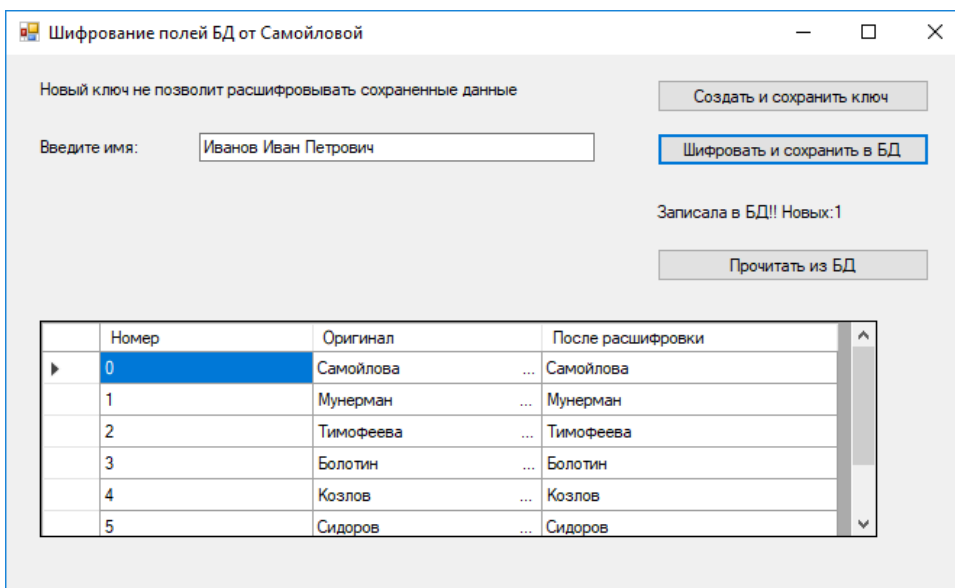


Лабораторная работа 8 " Защита информации в СУБД "

Задание 1. поле
varbinary(max) -

AES.

Entity Framework + LINQ



Задание 2

-SQL.

www.moodle.smolgu.ru).

Самостоятельная работа

-
-
-

Темы для самостоятельного изучения

- 1.
- 2.
3. security cryptography Visual Studio.NET.
- 4.
5. SQL-Server.

1. - -

6. Критерии оценивания результатов освоения дисциплины (модуля) 6.1. Оценочные средства и критерии оценивания для текущей аттестации

Теоретические вопросы

- 1.
- 2.
- 3.
4. - -2, SHA-256, SHA-384, SHA-512,
SHA-
- 5.
- 6.
- 7.
- 8.
- 9.
10. AES. MARS NewDES RC5 RC6 TEA Triple -2018.
DES Twofish.
- 11.
- 12.
- 13.
- 14.

15. -
16. RSA -
17. -
18. DSA, ECDSA (Elliptic Curve Digital Signature Algorithm), KCDSA, .
- 19.
20. - -
- 21.
- 22.
- 23.
- 24.
- 25.

Критерии оценивания теоретических вопросов

		*)
1		
2		

(*)

3

Задания для лабораторных занятий

(www.moodle.smolgu.ru).

Образец задания

1. -
2. RSA.
3. ,

Критерии оценивания выполнения лабораторных работ

		*)
1		1
2		

--	--	--

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

Зачетная работа (пример задания)

1. Python -

2. RC4.

3.

).

Критерии оценивания зачетной работы

		*)
1		
2		

(*)

1		4,75-5
2		3,75-4,5
3		3-3,5
4		

Критерий получения зачета

-
-
-

7. Перечень основной и дополнительной учебной литературы

7.1. Основная литература

1.

/

309

ISBN 978-5-534-04732-5.

URL: <https://urait.ru/bcode/413854>

2.

/

104

ISBN 978-5-534-14590-8.

URL: <https://urait.ru/bcode/477968>

7.2. Дополнительная литература

1.

209

/
ISBN 978-5-9916-7088-3.

URL: <https://urait.ru/bcode/450820>

2.

/
ISBN 978-5-534-02883-6.

349

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1.

2.

3.

4.

<http://www.intuit.ru>

-
t, <http://msdn.microsoft.com>

8. Материально-техническое обеспечение

Учебная аудитория для проведения занятий лекционного типа,

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации -

Помещение для самостоятельной работы

9. Программное обеспечение

Kaspersky Endpoint Security

FB6-161215-133553-1-6231.

Microsoft Open License,

49463448

: Microsoft Windows Professional 7

Russian; Microsoft Office 2010 Russian.

Python 3.9; PyCharm Pro; Microsoft Visual Studio

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 03B6A3C600B7ADA9B742A1E041DE7D81B0
Владелец: Артеменков Михаил Николаевич
Действителен: с 04.10.2021 до 07.10.2022