## Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Лабораторная работа № 4 Изучение шифров DES и Магма

Студент: Усачева Дарья, группа 1384

Руководитель: Племянников А.К., доцент каф. ИБ

Санкт-Петербург, 2024

## Цель работы и задачи

**Цель:** Повысить свою компетенцию в области симметричных блочных шифров и в криптографии в целом.

#### Задачи:

- 1. Изучить преобразования DES по шаблонной схеме DES Visualisation.
- 2. Провести исследование DES в режимах работы ECB и CBC.
- 3. Разработать схему в CrypTool 2 для экспериментального определения всех версий 3-DES.
- 4. Изучить преобразования шифра Магма.
- 5. Провести исследование шифра Магма в режимах работы простой замены и простой замены с зацеплением.

## Изучение преобразований DES

## Ручной расчет

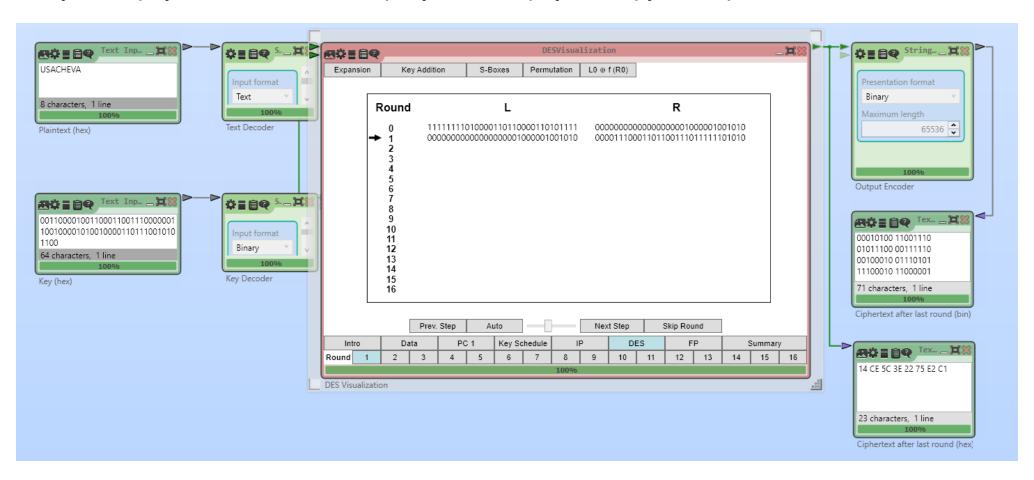
Открытый текст: USACHEVA

Ключ: 138427V (переведен в двоичную сс, в каждый 8 бит записан 0)

I	1 2	2 3	4	5	6	7	8	9	1	0	11	12	13	14	15	16																																																
Число сдвига	1 1	1 2	2	2	2	2	2	1	2	2	2	2	2	2	2	1																																																
	**	1 2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21 2	22 2	23 2	24	25	26	27 2	28 2	9 3	0 3	1 3	2 33	34	35	36	37	38	39	40	41 4	42 4	13 4	4 4	5 4	6 47	48	49	50	51	52	2 58	3 54	4 5!	5 5	6 5	57 5	8 5	59 (	60 /	61 6	52 f	53 (	54	
K	(	0 0	1	1	0	0	0	0	1	0	0	1	1	0	0	0	1	1	0	0	1	1	1	0	0	0	0	0	) 1	1 1	L O	0	1	0	0	0	0	1	0	1	0	0 :	1 (	) (	0	0	1	1	0	1	. 1	. 1	1 0	) [	0	1 /	0	1	0	1	1	0	0	
удалим биты проверки	(	0 0	1	1	0	0	0	1	0	0	1	1	0	0	1	1	0	0	1	1	1	0	0	0	0	0	1	1	) 1	L	0 0	0	0	1	1	0	0	1	0	0	0	1 1	1 (	0 1	. 1	1	0	1	0	1	. 0	1 1	1 1	1 /	0									
PC1	5	7 49	41	33	25	17	9	1	58	50	42	34	26	18	10	2	59	51	43	35	27 1	19 :	11	3 (	60	52	44 3	36	6	3 5	5 4	7 39	31	23	15	7	62	54	46	38	30 2	22 1	.4 (	5 6	1 53	45	37	29	21	13	5 5	21	8 20	0 1	2 4	4		$\perp$	$\Box$	$\perp$		$\Box$		
результат РС1	CO :	1 1	1	0	0	1	1	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	1	1	0 [	0 0	) (	0 0	1	1	1	0	0	1	1	0	0	1	1 (	0 (	0 1	. 1	0	0	0	1	1	. 0	10	0 0	0 1	1	1		$\perp$	$\Box$	$\Box$		$\Box$		
<<<	C1	l 1	0	0	1	1	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	1	1	0	1 [	1 0	) (	) 1	. 1	1	0	0	1	1	0	0	1	1	0 (	0 1	1 1	. 0	0	0	1	1	0	0	1 0	) 1	1 /	1	0								
объеденим C1 и D1	1	1 1	0	0	1	1	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	1	1	0	1	) (	) [	1 1	. 1	0	0	1	1	0	0	1	1	0	0 :	1 1	1 (	0	0	1	1	0	0	0	/ 1	1 1		0	Т		$\perp$	$\Box$	$\Box$		$\perp$		
PC2	1	4 17	11	24	1	5	3	28	15	6	21	10	23	19	12	4	26	8	16	7	27 2	20 :	13	2 4	41	52	31 3	37 4	7 5	5 3	0 4	51	45	33	48	44	49	39	56	34 !	53 4	46 4	2 5	0 3	6 29	32	2				$\perp$	$\perp$	$\perp$	$\perp$		$\perp$		$\Box$				$\Box$		
K1	(	0 0	1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	0	0	0	1	1	1	0	1	1	) 1	L (	) 1	. 0	1	1	0	1	1	0	0	0	0	0 (	0 1	1 1	. 0	1						$\perp$		$\perp$										
									9	10	11	12	13	14	15	16	17	18	19	20	21 2	22 2	23 2	24 :	25	26	27 2	28 2	9 3	0 3	1 3	2 33	34	35	36	37	38	39	40	41 4	42 4	13 4	4 4	5 4	6 47	48	49	50	51	52	2 58	3 54	4 5!	5 5	6 5	57 5	i8 !	59 /	60 /	61 6	52 f	53 /	54	
USACHEVA		) 1							0		0		0	0	1	1	0	1	0	0	0	0	0	1	0	1	0	0	) (	) [	1 1	. 0	1	0	0	1	0	0	0	0	1	0 (	0 (	0 1	. 0	1	0	1	0	1	. 0	1	1 1		0	0 :	1	0	0	0	0	0	1	
IP	5	8 50	42	34	26	18	10	2	60	52	44	36	28	20	12	4	62	54	46	38	30 2	22 :	14	6 (	64	56	48 4	10 3	2 2	4 1	6 8		57	49	41	33	25	17	9	1 !	59 5	51 4	3 3	5 2	7 19	11	1 3	61	53	45	37	7 29	9 21	1 1	3	5 f	i3 !	55 /	47	39 3	31 7	23 /	15	/
результат IP	LO :	1 1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	0	1	1	0	0	0	0	1	1	0	1	0	. 1	1 1	1 1	RO	0	0	0	0	0	0	0	0	0	0 (	0 (	) (	0	0	0	0	0	0	1	. 0	0 0	) [	0	0 /	0	1	0	0	1	0	1 (	)
L1 = R0; R1 = L0 xor f(R0,K1)	L1 (	0 0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0		) [	1 0	R1	0	0	0	0	1	1	1	0	0	0 :	1 1	1 (	1	1	0	0	1	1	1	. 0	1	1 7	1	1	1	1	1	0	1	0	1 (	)
	1 2	2 3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22 2	23 2	24 2	25 :	26	27	28 2	29 3	0 3	1 3	2 3	3 34	35	36	37	38	39	40	41	42	43 4	14 4	5 4	6 4	7 48	3																		
R0	0 (	0 0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1	) 1	L	)																																	
E	32 1	1 2	3	4	5	4	5	6	7	8	9	8	9	10	11	12	13	12	13	14	15 1	16	17 1	16	17	18	19 2	20 2	1 2	0 2	1 2	2 23	24	25	24	25	26	27	28	29 :	28 2	29 3	0 3	1 3	2 1																			
результат Е	0 (	0 0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	) 1	L (	0 0	0	0	0	0	0	1	0	0	1	0	1 (	0 1	1 (	0																			
K1	0	) 1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	0	0	0	1	1	1	0	1	1	0		) [	1 0	1	1	0	1	1	0	0	0	0	0	0 :	1 1	1 (	1																			
К1 + результат	0 (	) 1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	0	0	0	1	1	1	0	1	1	1	. 1	1 1	L O	1	1	0	1	1	1	0	0	1	0	1 1	1 (	) (	1																			
преобразование S			2						2					6	,					15						13						10					14	4					0																					
преобразование S	0 (									1	0		1	1	1	1	1	0	1	1	0	_	0	1			0																																					
Р	6 7	7 20	21	29	12	28	17	1	15	23	26	5	18	31	10	2	8	24	14	32	27	3	9 1	19	13	30	6 2	22 1	1 4	1 2	5												$\perp$																					
f(R0,K1)	1 1	1	1	0	0	0	1	0	1	1	1	0	1	0	1	0	0	0	1	0	1	1	0	0	1	0	0	0	L C	) [	1																																	
	LO	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	0	1	1	0	0	0	0	1	1	0	1	0	1	1 1	1 1																																	
хог	1	1	1	1	0	0	0	1	0	1	1	1	0	1	0	1	0	0	0	1	0	1	1	0	0	1	0	0	) 1	L	) 1																																	
	R1 (	0 0	0	0	1	1	1	0	0	0	1	1	0	1	1	0	0	1	1	1	0	1	1	1	1	1	1	0	L	) [	L O																																	

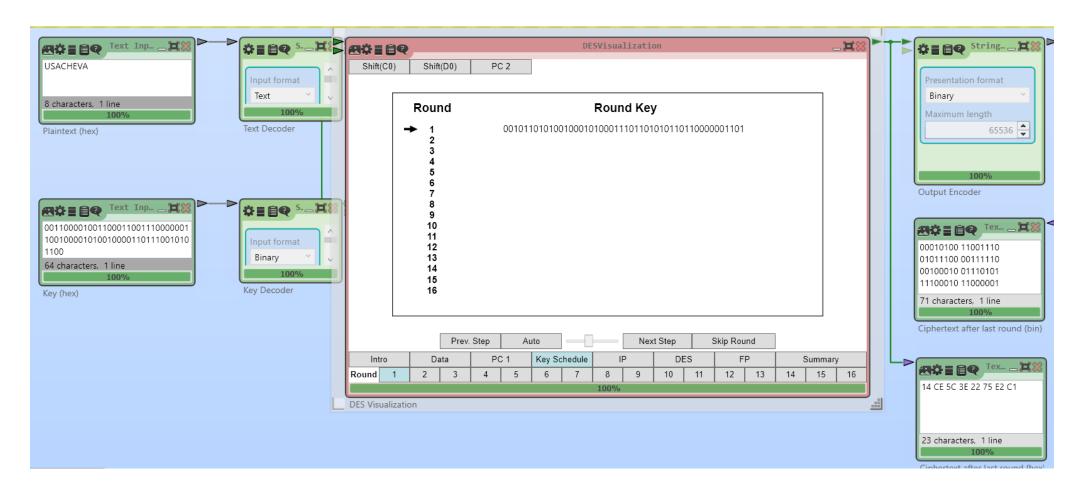
## Результат раунда 1

Результат раунда 1 совпадает с результатом раунда 1 ручного расчета.



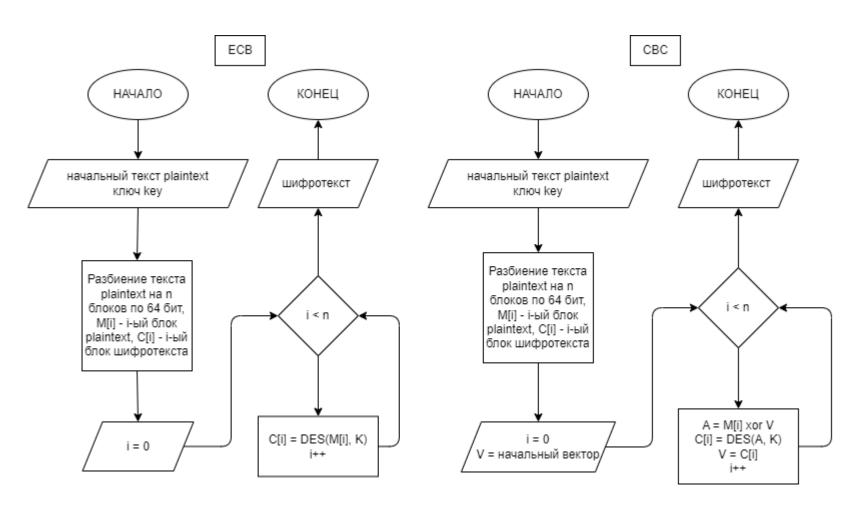
### Ключ раунда 1

Ключ раунда 1 совпадает с результатом ручного расчета ключа 1.



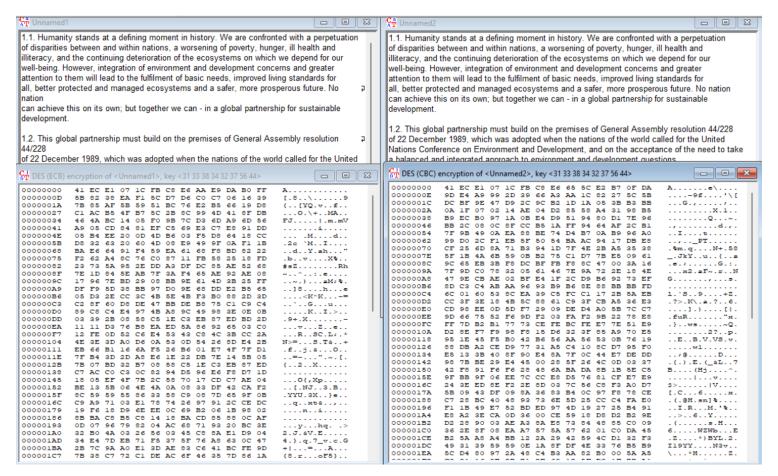
## Исследование DES в режимах работы ECB и CBC

## Схемы алгоритмов работы DES в режимах ECB и CBC



### Результаты шифрования текста

Результаты шифрования текста на английском языке (не менее 1000 символов), полученные с помощью DES в режиме работы ECB и CBC. Ключ: 31 33 38 34 32 37 56 44



## Оценка времени атаки грубой силы

Была проведена оценка времени выполнения атаки грубой силой для шифротекста длины 1009

#### **ECB**

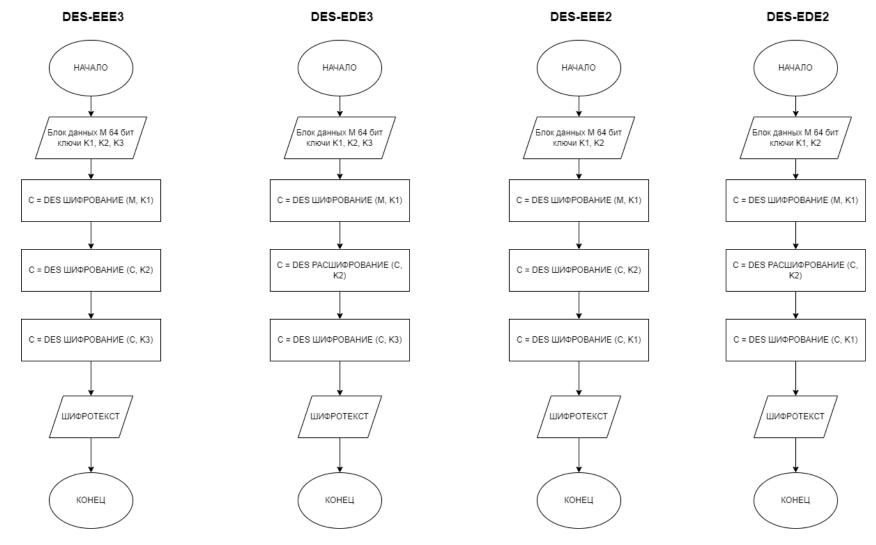
Кол-во	Ожидаемое
известных байт	время
ключа	выполнения
2	1.1 года
4	26 минут
6	<1 секунды

#### **CBC**

Кол-во	Ожидаемое
известных байт	время
	выполнения
2	1.8 года
4	41 минут
6	<1 секунды

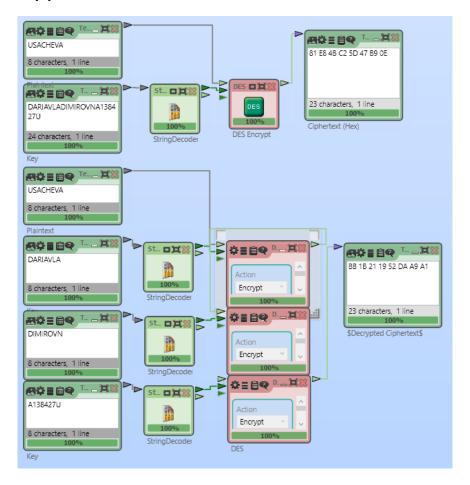
# Разработка схемы в CrypTool 2 для экспериментального определения всех версий 3-DES

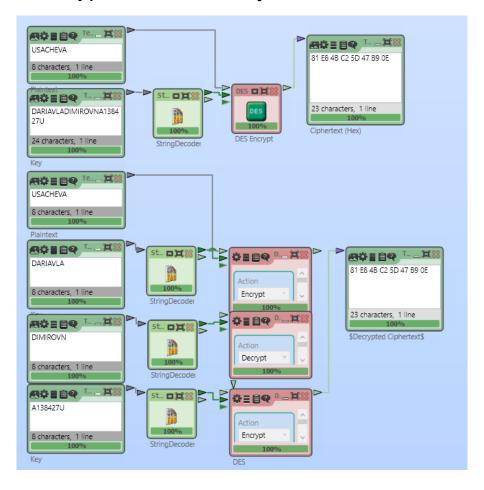
## Схемы алгоритмов работы 3-DES в различных режимах



## Определение версий 3-DES, реализованных в Cryptool 2

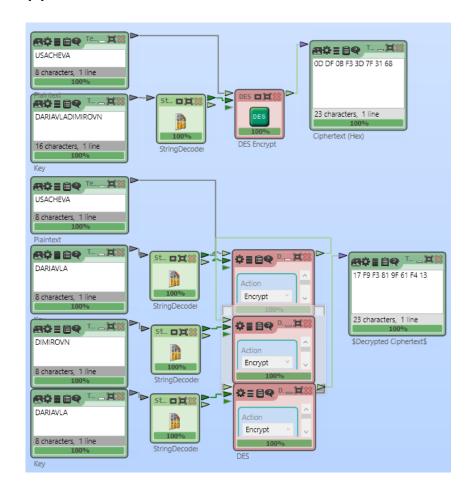
Зашифруем текст алгоритмом 3-DES и вручную в режимах EEE3 и EDE3. Как видим, результаты шифрования совпали для EDE3, что означает, что Cryptool 2 использует его.





## Определение версий 3-DES, реализованных в Cryptool 2

Зашифруем текст алгоритмом 3-DES и вручную в режимах EEE2 и EDE2. Как видим, результаты шифрования совпали для EDE2, что означает, что Cryptool 2 использует его.





## Изучение преобразований шифра Магма

## Ручной расчет

Открытый текст: USACHEVA

Ключ: 138427DARIAVLADIMIRONVA23102002K

							1	1	_	-	_	_																				$\overline{}$
USACHEVA	55	53	41	43	48	45	56	41																								
138427DARIAVLADIMIRONVA23102002K	31	33	38	34	32	37	44	41	52	49	41	56	4C	41	44	49	4D	49	52	4F	4E	56	41	32	33	31	30	32	30	30	32	4B
K1	31	33	38	34																												
разделим на два блока	LO	55	53	41	43	R0	48	45	56	41																						
L1 = R0; R1 = (R0+K1)m	L1	48	45	56	41	R1	56	E5	68	E6																						
(R0+K1)mod 2**32 =	79	78	8E	75																												
преобразование S	S8	<b>S7</b>	S6	<b>S5</b>	S4	<b>S</b> 3	S2	S1																								
номер столбца	7	9	7	8	8	14	7	5																								
Выход S	3	4	10	0	7	6	12	5																								
Выход S в 16cc	34	A0	76	C5																												
двоичный вид	0	0	1	1	0	1	0	0	1	0	1	0	0	0	0	0	0	1	1	1	0	1	1	0	1	1	0	0	0	1	0	1
<<<11	0	0	0	0	0	0	1	1	1	0	1	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	1	0	0	1	0	1
L0 в 2cc	0	1	0	1	0	1	0	1	0	1	0	1	0	0	1	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	1
L0 xor res	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	1	0	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0
R1	56	E5	68	E6																												

## Результат раунда 1

Результат выполнения раунда 1 совпадает с результатом раунда 1 ручного расчета.

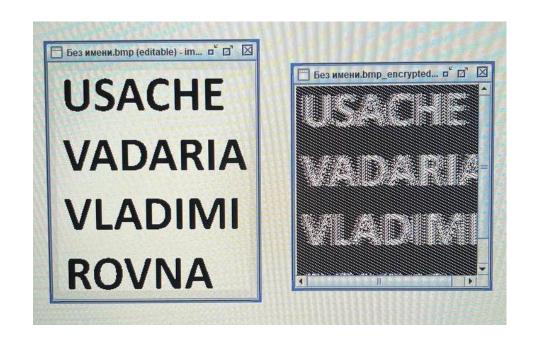
Субблок L: 55 53 41 43	Субблок R: 48 45 56 41		Ключ раунда: 31 33 38 34
		Преобразование: 'сложение по модулю 2^32'	
		Результат: 79 78 8Е 75	
		Преобразование: 'подстановка S'	
		Результат: 34 А0 76 С5	
		Преобразование: 'циклический сдвиг <<11'	
		Результат: 03 В6 29 А5	
		Преобразование: 'сложение XOR'	
		Результат: 56 Е5 68 Е6	
		Раунд №1	>
«			>>

# Исследование шифра Магма в режимах работы простой замены и простой замены с зацеплением

### Результаты шифровки

Была создана картинка в формате bmp и зашифрована с помощью шифра Магма в режиме простой замены(ECB) и в режиме простой замены с зацеплением(CBC). Как можно заметить, изображение, полученное с помощью режима CBC, менее читаемо.

ECB CBC





### Заключение

1. Изучены преобразования DES по шаблонной схеме DES Visualisation.

Выполнено ручное преобразование первого раунда и рассчитан раундовый ключ. Результаты программных и ручных вычислений совпали.

2. Проведены исследования DES в режимах работы ECB и CBC.

Выполнено сравнение скорости дешифрования в различных режимах работы. СВС продемонстрировал большую устойчивость по сравнению с режимом ЕСВ. Установлено, что режим ЕСВ, благодаря параллельности вычислений, работает быстрее, чем режим СВС.

- 3. Разработана схема в CrypTool 2 для экспериментального определения всех версий 3-DES.
- Выяснено, что CrypTool 2 реализует шифр 3-DES по схеме EDE3 и EDE2.
- 4. Изучены преобразования шифра Магма.

Выполнено ручное преобразование первого раунда. Результаты программных и ручных вычислений совпали.

5. Проведено исследование шифра Магма в режимах работы простой замены и простой замены с зацеплением.

Режим простой замены продемонстрировал, что одинаковые блоки исходных данных шифруются в одинаковые блоки, что сохраняет структуру данных и может облегчить сжатие, но при этом снижает безопасность. В режиме замены с зацеплением данные преобразуются в псевдослучайный шум, что значительно повышает их стойкость к анализу, однако делает сжатие практически невозможным.