

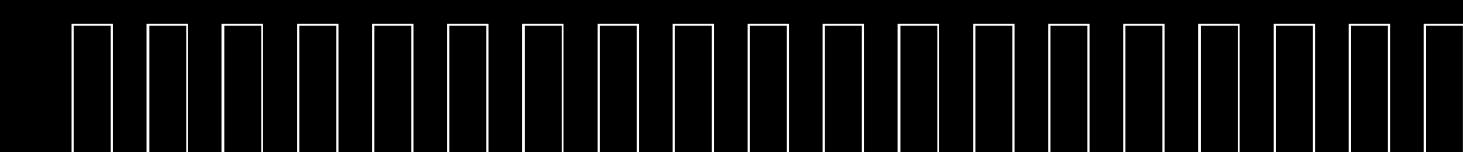


CAST-128

Encryption Algorithms of symmetric block cryptography

AC-22-05

Шелякина Анастасия, Егоркина Маргарита, Желудов Тимофей,
Сайфуллин Булат, Разин Илья, Капаров Алимурад, Скосарь Ростислав



Классификация

MD5 · SHA · DES · RC4 · RC5 · IDEA · AES · TDES

Криптографические алгоритмы

Бесключевые

Одноключевые

Двухключевые

Хэширование

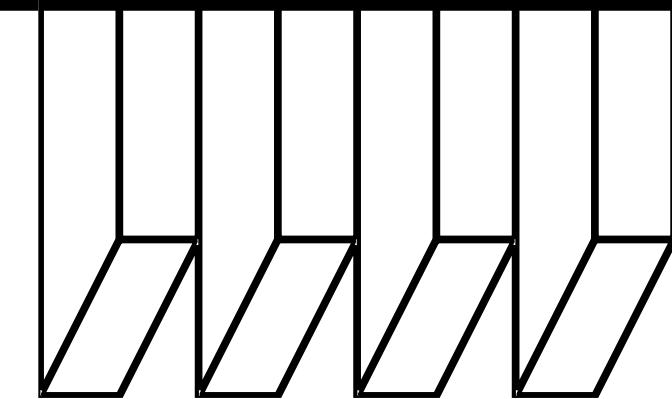
Симметричное шифрование

Асимметричное шифрование

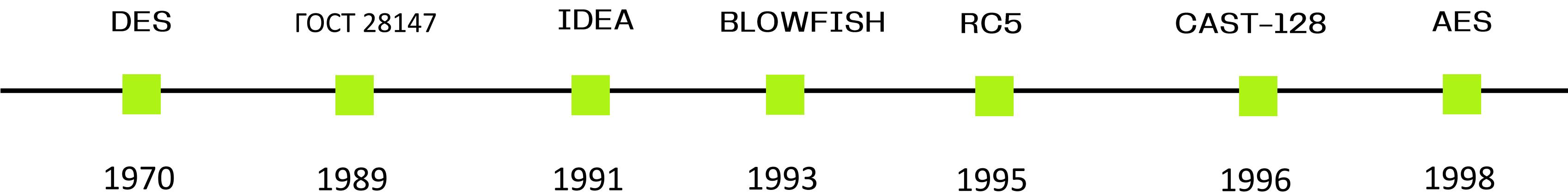
Электронная подпись

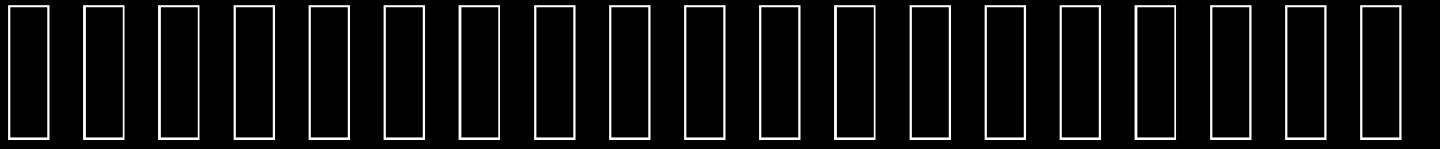
Блочное

Поточное



Алгоритмы симметричного блочного шифрования





ОСНОВНЫЕ ХАРАКТЕРИСТИКИ



Симметричность и блочность

Симметричное блочное шифрование использует один и тот же ключ для шифрования и расшифрования сообщения. Входные данные разбиваются на блоки фиксированного размера перед шифрованием, обычно размер блока составляет 64 бита или 128 бит.



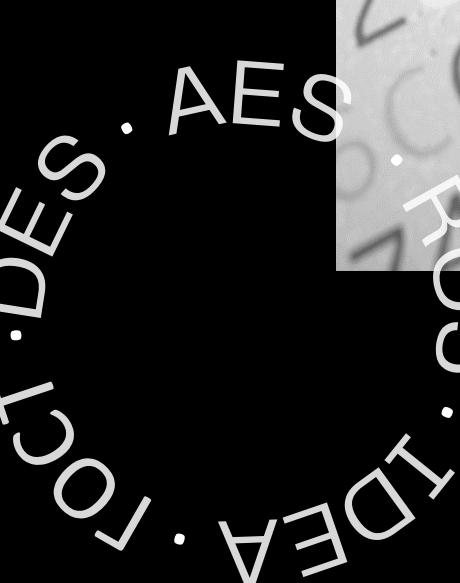
Замена и перестановка

Шифр заменяет каждый блок данных на другой с помощью замен и перестановок. Это обеспечивает защиту данных от простого перебора и анализа.



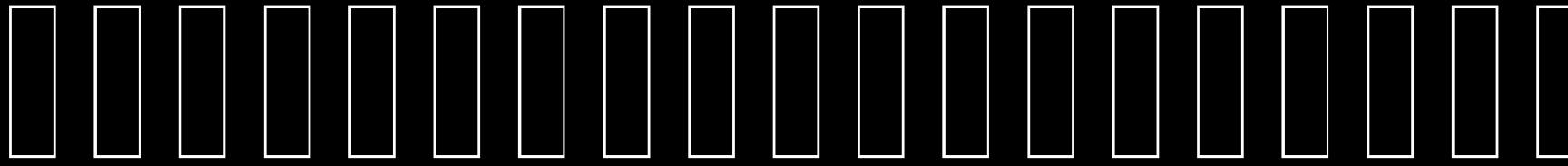
Криптографическая стойкость

Симметричные блочные шифры стремятся предоставить высокий уровень безопасности и выдерживать криптоанализ, такой как атаки перебором ключа, атаки на свободный текст и другие.



AC-22-05



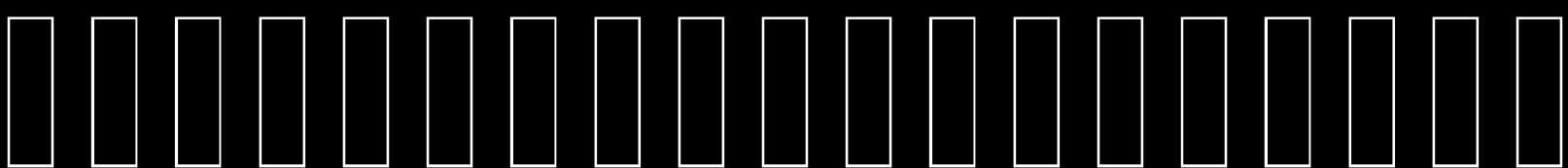


AC-22-05

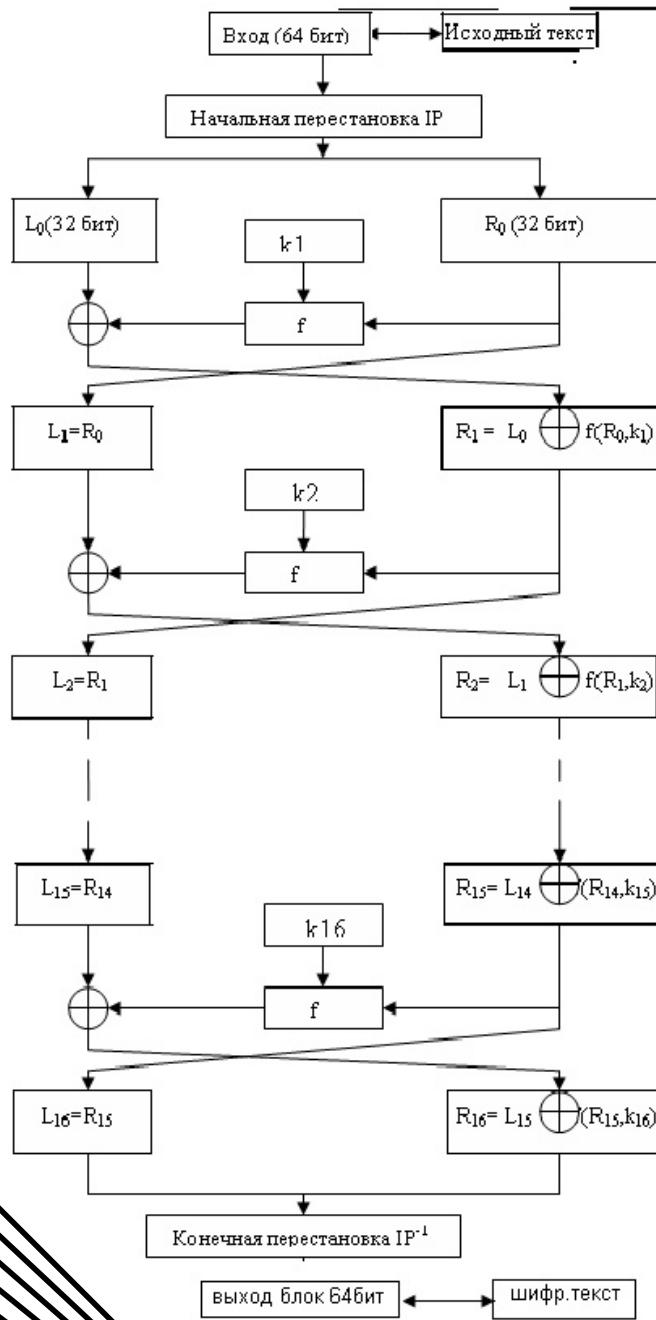


DES

Выполнил : Разин Илья



DES



DES

0 0 0 0 0 0 0 1 1 1 1 1 0 0 1 1 1 1 1 0 0 1 0 0 0 0

1 1 0 0 0 0 0 0 1 0 1 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1

Таблица 3

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Число сдвига	1	1	2	2	2	2	2	2	1	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 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56
0 0 0 0 0 0 0 1 1 1 1 1 0 0 1 1 1 1 0 0 0 0 0 1 1 0 0 0 0 0 0 1 0 1 1 0 0 0 0 1 1 0 1 0 0 1 1 0 0 1 0 0 0 1

0 1 1 1 0 0 0 0 0 0 1 1 0 1 1 0 0 1 1 0 0 0 0 1 0 0 1 1 0 1 0 1 0 0 1 1 0 0 1 0 0 0 1 0

Таблица 4

14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2	41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

DES

0 0 0 0 0 0 1 1 1 1 1 0 0 1 1 1 1 1 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 1 1 0 0 0 0 1 1 0 1 0 0 0 0 0 0 1 1

0 1 1 1 0 0 0 0 0 0 1 1 0 1 1 0 0 1 1 0 0 0 0 1 0 0 1 1 0 1 0 1 0 0 1 1 0 0 1 0 0 0 1 0 **ключ 1-го раунда**

0 1 1 0 0 0 0 0 1 0 0 1 1 1 0 0 1 1 1 0 0 0 0 0 0 1 1 0 0 0 1 0 0 1 0 1 1 0 0 0 0 0 1 1 0 **ключ 2-го раунда**

0 0 0 0 0 0 0 0 0 0 1 0 1 1 1 1 1 1 1 1 0 1 1 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0

Таблица 2

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

XOR

0 0 0 0 0 0 0 0 0 0 1 0 1 1 1 1 1 1 1 1 1 0 1 1 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0

0 1 1 1 0 0 0 0 0 0 1 1 0 1 1 0 0 1 1 0 0 0 0 1 0 0 1 1 0 1 0 1 0 0 1 1 0 0 1 0 0 0 1 0

DES

Таблица 8

		номер строки	номер колонки	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
		0 1 1 1 0 0		0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	S1	0 0 0 0 1 0		1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	S2	0 0 0 1 1 0		2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
		0 1 1 0 0 1		3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
		1 1 0 0 1 0		0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
		0 1 0 1 0 1		1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
		0 0 1 1 1 1		2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
		0 1 0 0 1 0		3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Таблица 8

		номер строки	номер колонки	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
		0 1 1 1 0 0		0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	S1	0 0 0 0 1 0		1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	S2	0 0 0 1 1 0		2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
		0 1 1 0 0 1		3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
		1 1 0 0 1 0		0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
		0 1 0 1 0 1		1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
		0 0 1 1 1 1		2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
		0 1 0 0 1 0		3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Таблица 8

		номер строки	номер колонки	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
		0 1 1 1 0 0		0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	S1	0 0 0 0 1 0		1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	S2	0 0 0 1 1 0		2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
		0 1 1 0 0 1		3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
		1 1 0 0 1 0		0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
		0 1 0 1 0 1		1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
		0 0 1 1 1 1		2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
		0 1 0 0 1 0		3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Таблица 5

0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 1 1 1 0 0 0 1 1 1 1 0 1 1 0 0 1 1 1 0 1 0 0 1 0 0 1 0 0 1
16 7 20 21 29 12 28 17
1 15 23 26 5 18 31 10
2 8 24 14 32 27 3 9
19 13 30 6 22 11 4 25

DES

XOR

1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	1	0	1	1	0	1	1	0	1	0	0	0	0	1	1	0	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

1	1	1	1	1	1	1	1	1	1	0	0	1	0	1	0	0	1	0	1	0	1	1	1	1	0	1	0	0	1	0	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

0	1	0	0	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	0	1	1	0	1	0	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

L16

R16

1 0 1 1 1 1 1 1 0 1 1 1 0 0 1 0 0 0 1 1 1 0 0 0 1 0 0 1 1 1 0 1 0 0

1 0 0 0 0 0 1 0 0 0 0 1 0 0 1 1 0 0 1 1 1 0 0 1 0 1 1 1 0 0 0

R16

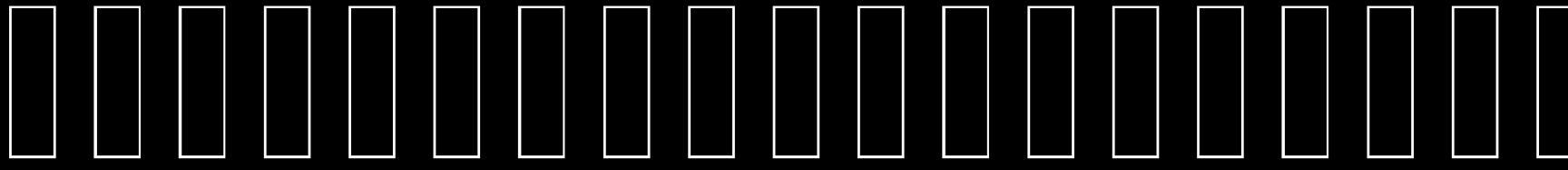
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
1	0	0	0	0	0	1	0	0	0	0	1	0	0	1	1	0	0	1	1	1	0	0	1	1	0	0	0	1	0	1	1	1	1	1	1	0	1	1	0	0	0	1	1	0	0	0	1	1	0	1	0	0	0	1	1	0	1	0	0	0			

L16

1 0 0 1 1 0 0 0 1 1 1 | 1 0 0 0 0 1 0 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 0 1 0 0 0 0 0 1 1 0 0 0 0 0 1

Таблица 7

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

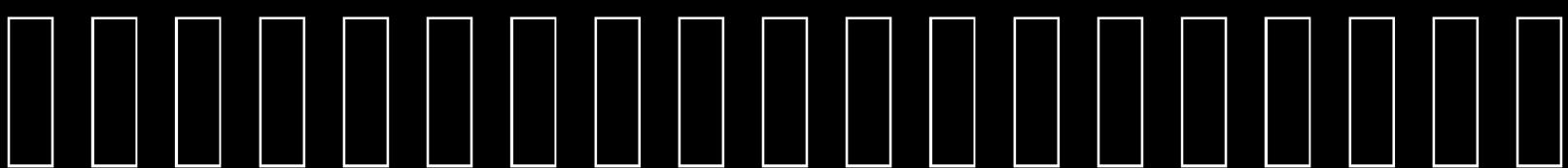


AC-22-05



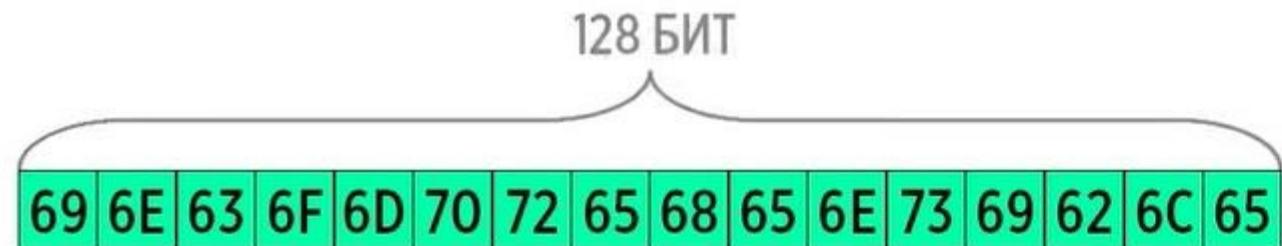
AES

Выполнила : Шелякина Анастасия

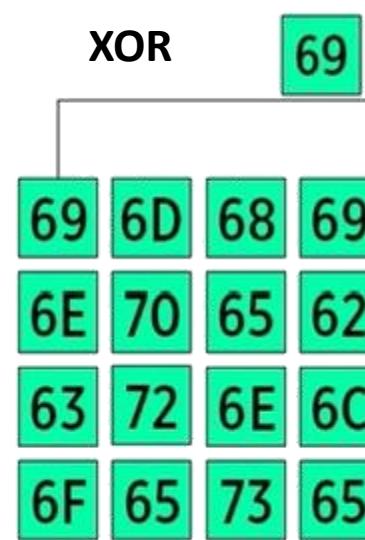
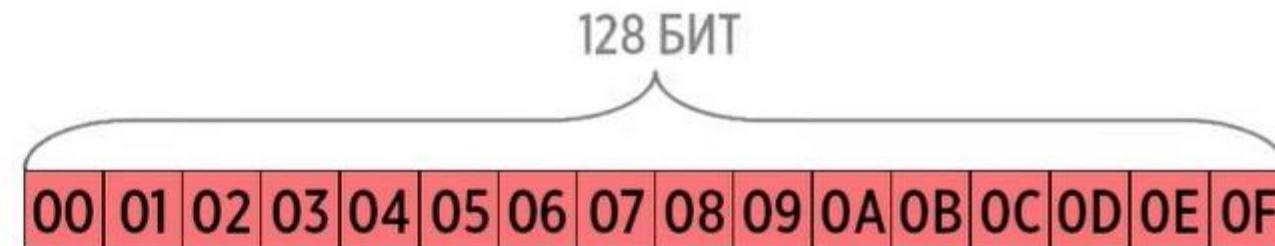


AES

i n c o m p r e h e n s i b l e



00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F



00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

0D
0E
0F
0C

69 69 60 65
6F 75 6C 6F
61 74 64 62
6C 62 78 6A

Таблица 1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	B4
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

AES

04	08
05	09
06	0A
07	0B

00	XOR	D7	XOR	01
01	XOR	AB	XOR	00
02	XOR	76	XOR	00
03	XOR	FE	XOR	00

00	04	08	D7
01	05	09	AB
02	06	0A	76
03	07	0B	FE
D6	D2	DA	D6
AA	AF	A6	AB
74	72	78	76
FD	FA	F1	FE

Таблица 2

AES

1 РАУНД

D6	D2	DA	D6
AA	AF	A6	AB
74	72	78	76
FD	FA	F1	FE

F9	F9	D0	4D
9D	50	A8	A8
43	AA	EF	92
02	50	AA	BC

×

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

$$F9 \times 02 + 9D \times 03 + 43 \times 01 + 02 \times 01$$

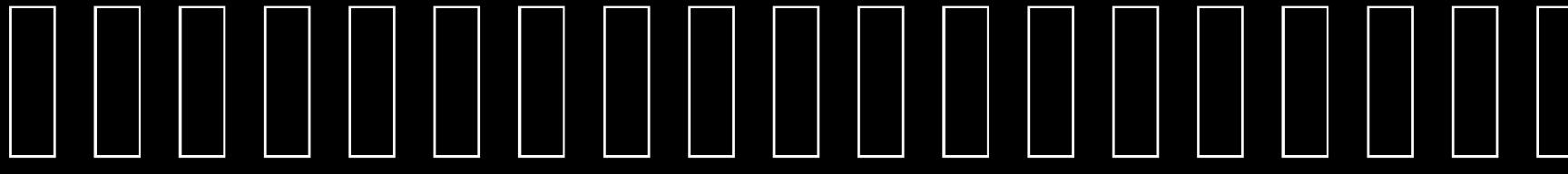
$$\begin{matrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ X7 & + & X6 & + & X5 & + & X4 & + & X3 & + & 1 & \times & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{matrix} = X8 + X7 + X6 + X5 + X4 + X$$

$$\begin{matrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ X7 & + & X4 & + & X3 & + & X2 & + & 1 & \times & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ & & & & & & & & & & X & + & 1 \end{matrix} = X8 + X5 + X4 + X3 + X + X7 + X4 + X3 + X2 + 1$$

$$\begin{matrix} 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ X6 & + & X & + & 1 & \times & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix} = X6 + X + 1$$

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ X & \times & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix} = X$$

$$X4 + 2 = 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0 = 14$$

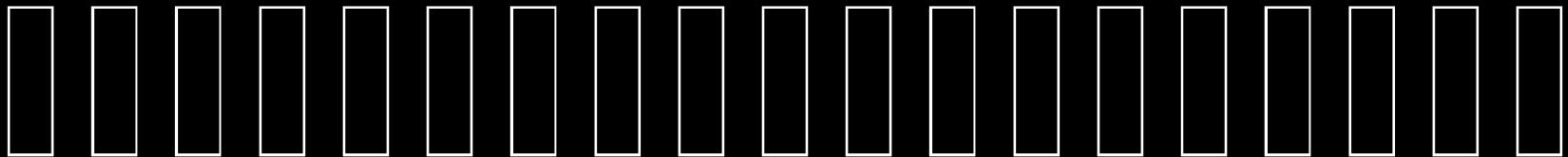


AC-22-05

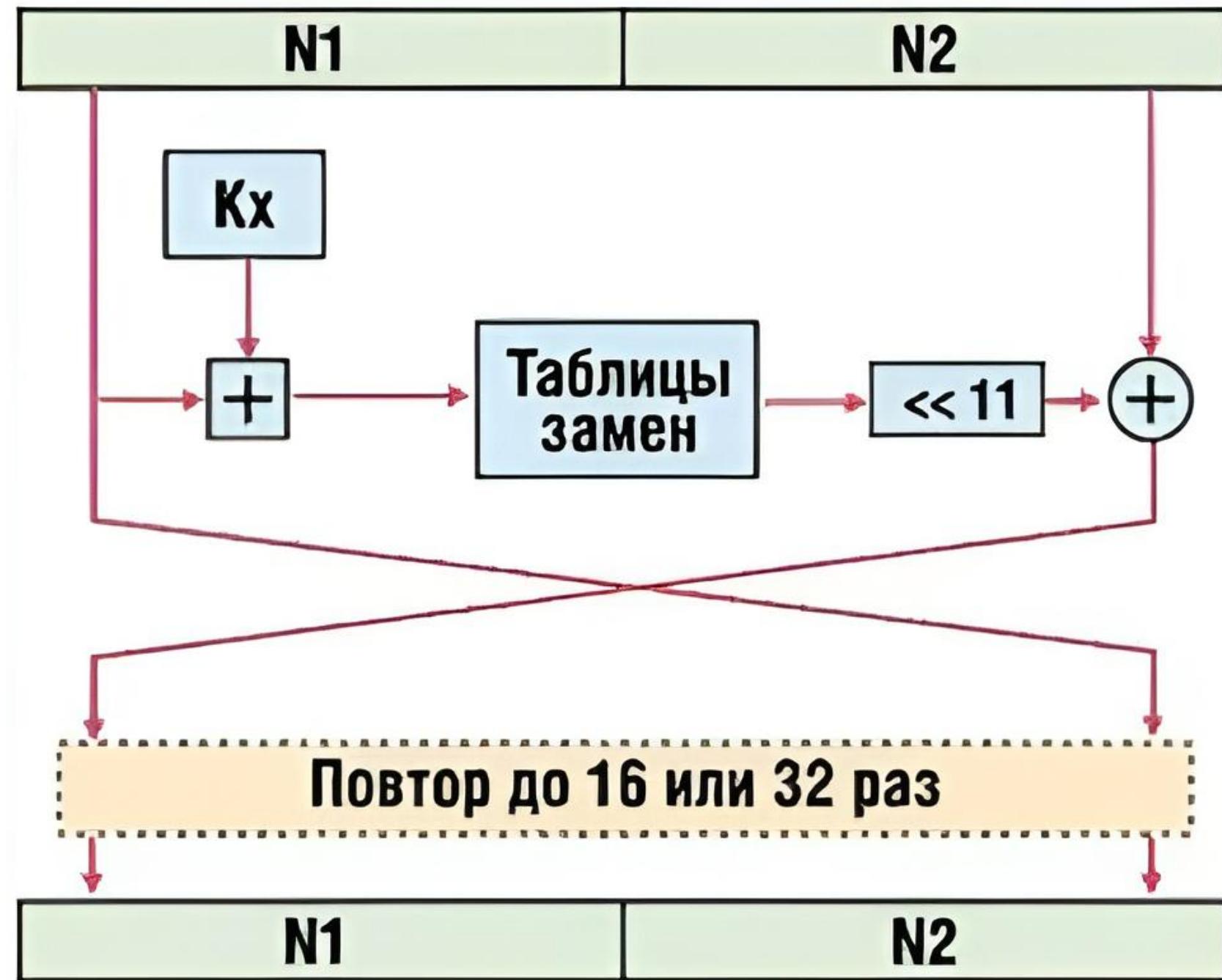


ГОСТ-28147-89

Выполнил : Скосарь Ростислав



ГОСТ-28147-89



ГОСТ-28147-89

```
ulong f(ullong a, ullong x, int pi) { //выполнение функцией f одного раунда шифрования
    a += x;
    a &= mod32;
    int un[8];
    for (int i = 0; i < 8; ++i) {
        x = a & 0xf;
        un[8 - i - 1] = x;
        a >>= 4;
    }
    for (int i = 0; i < 8; ++i) {
        un[i] = piBlock[i][un[i]];
    }
    for (int i = 0; i < 8; ++i) {
        a += un[i];
        a <= 4;
    }
    a >>= 4;
    a = (a << 11) | (a >> 21);
    a &= mod32;
    return a;
}

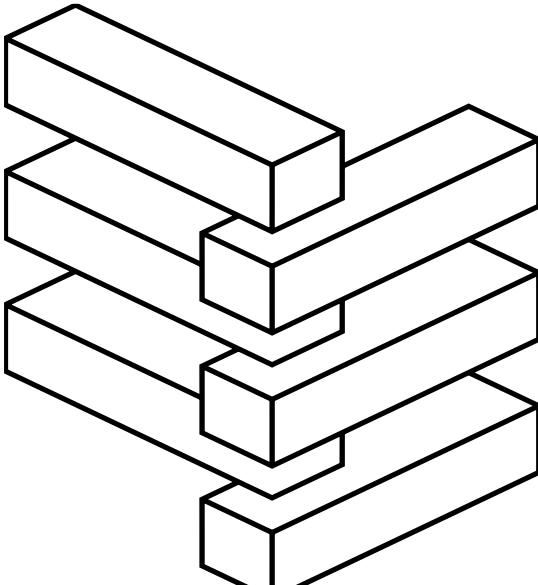
ullong encrypt(ullong data) { //алгоритм шифровки ГОСТ-28147-89
    ullong left = data;
    ullong right = left & mod32;
    left >>= 32;
    setXkey();
    data = round(left, right);
    return data;
}

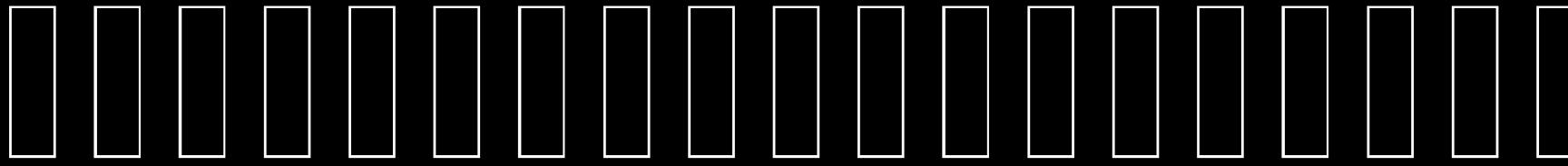
ullong decrypt(ullong data) { //алгоритм дешифровки ГОСТ-28147-89
    ullong left = data;
    ullong right = left & mod32;
    left >>= 32;
    setXkey();
    for (int i = 8; i < 16; ++i) {
        std::swap(xkey[i], xkey[32 - i - 1]);
    }
    data = round(left, right);
    return data;
}
```

The screenshot shows the Microsoft Visual Studio Output window. It displays the original message "Hello, World!", its encrypted form as a long string of hexadecimal digits, and the decrypted message "Hello, World!". The window also includes standard Visual Studio status text at the bottom.

```
Консоль отладки Microsoft Visual Studio
message: Hello, World!
Encrypted message: 11255397442739107563 10264553692270540367 13632281020175927825 13632281020175927825 10678325030459941476 11160188698153070087 2374748129653
458527 6368554407861363274 10678325030459941476 5350113150564831649 13632281020175927825 15505657805635721384 846774926333612681
Decrypted message: Hello, World!

C:\Users\Ростислав\source\repos\GHOST28_Skosar\Debug\GHOST28_Skosar.exe (процесс 7808) завершил работу с кодом 0.
Чтобы автоматически закрывать консоль при остановке отладки, включите параметр "Сервис" ->"Параметры" ->"Отладка" -> "Автоматически закрыть консоль при остановке отладки".
Нажмите любую клавишу, чтобы закрыть это окно...
```



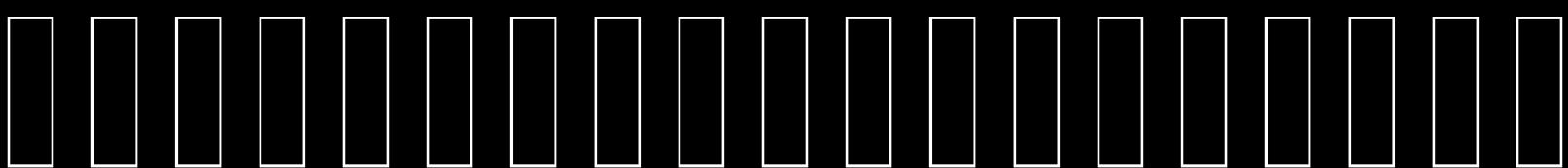


AC-22-05



Blowfish

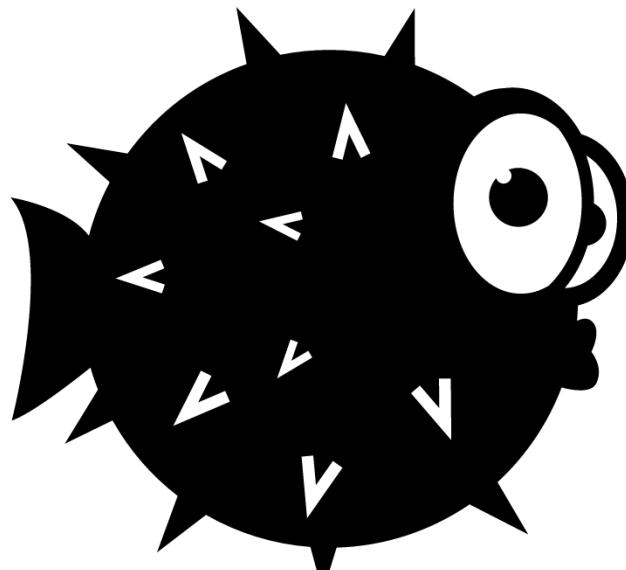
Выполнил : Сайфуллин Булат



Blowfish

Blowfish - это метод шифрования, разработанный Брюсом Шнайером в 1993 году в качестве альтернативы методу шифрования DES. Он значительно быстрее DES и обеспечивает хорошую скорость шифрования.

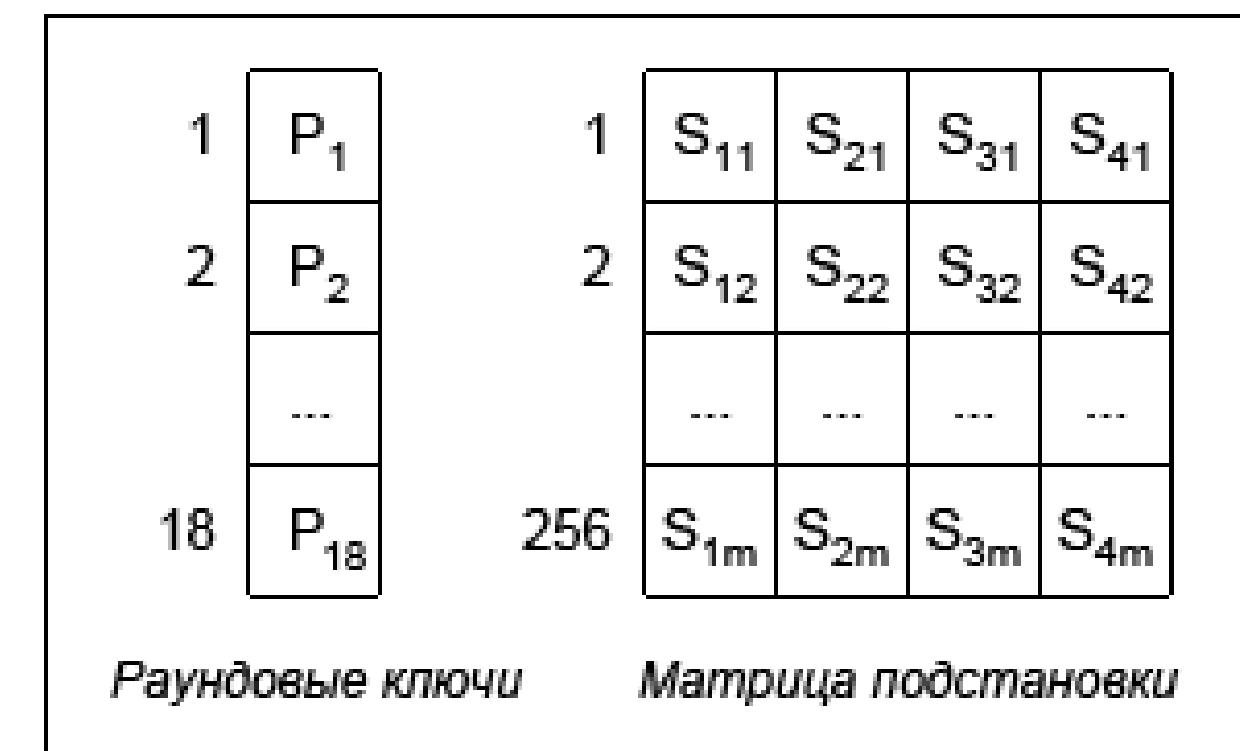
- Размер блока: 64 бита
- Размер ключа: переменный размер от 32 до 448 бит
- количество подразделов: 18 [P-массив]
- количество раундов: 16
- количество блоков подстановки: 4 [в каждом по 512 записей по 32 бита каждая]



Blowfish

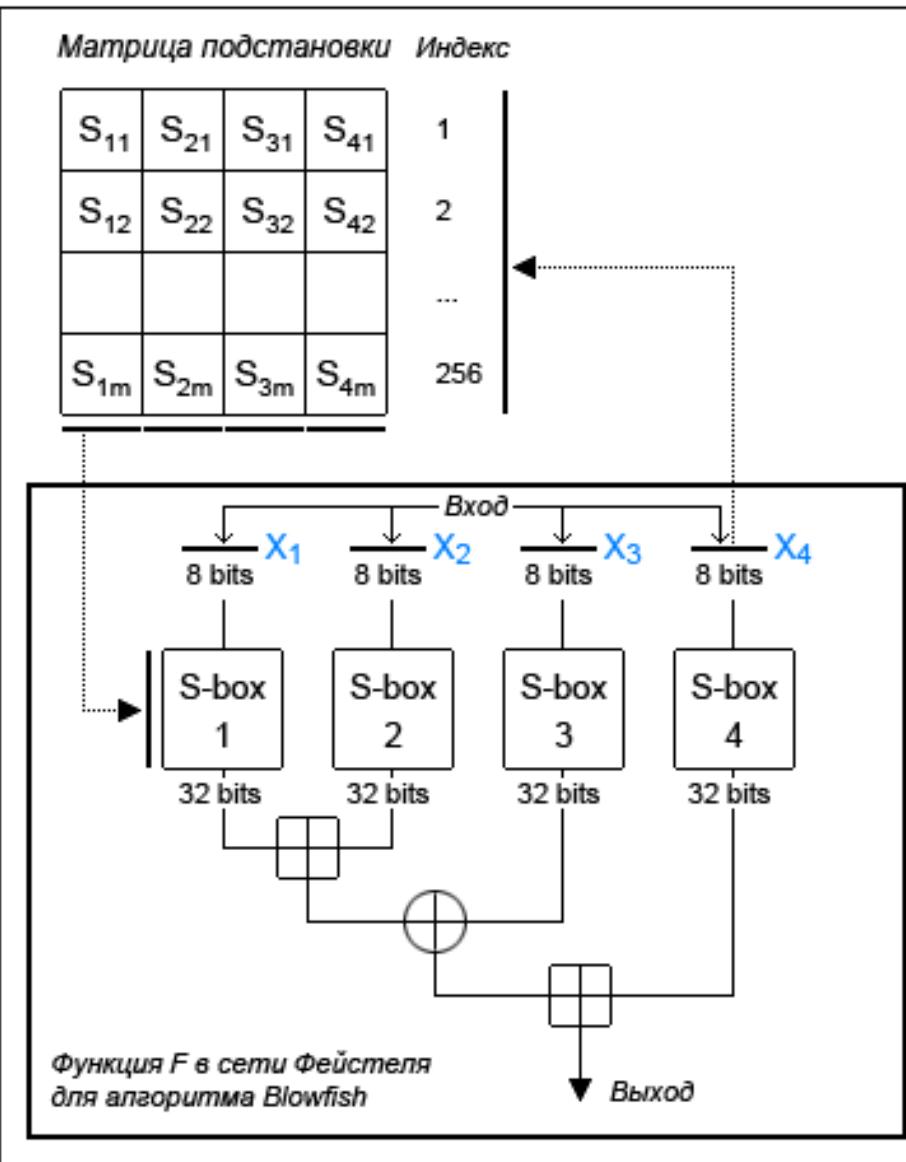


- Количество 32-х битовых подключей - 18.
- 4 блока по 256 32-х битовых значений.
- Подключи и блоки задаются по значению числа r_i

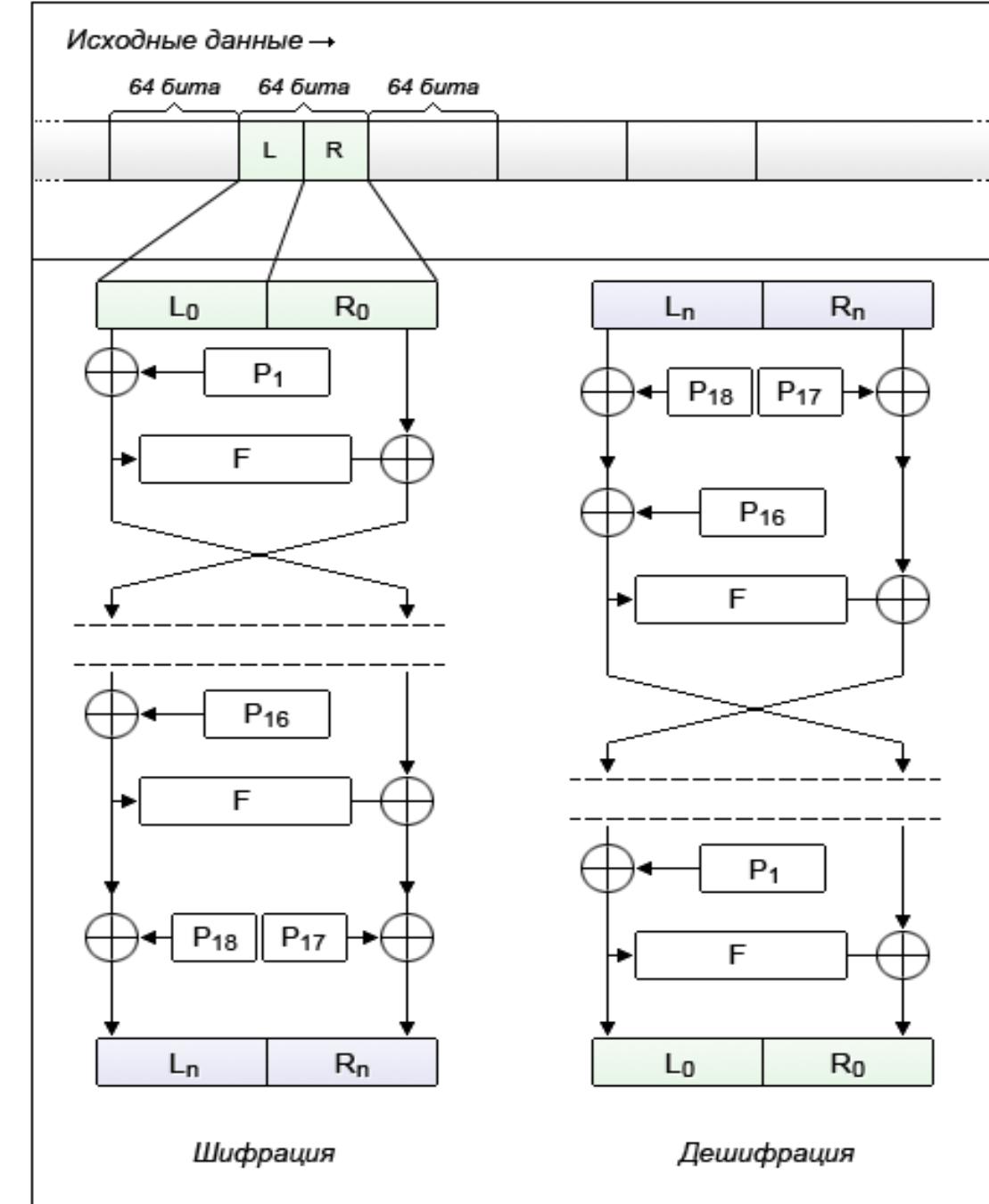


Blowfish

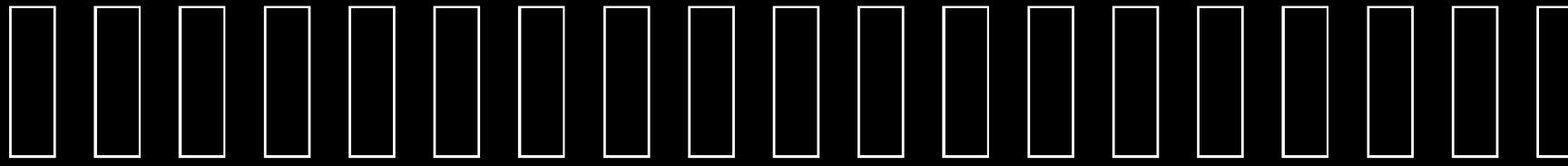
Функция итерации (раунда)



$$F(X_1, X_2, X_3, X_4) = (((S_1[X_1] + S_2[X_2]) \bmod 2^{32} \oplus S_3[X_3]) + S_4[X_4]) \bmod 2^{32}$$



Шифрация / дешифрация исходных данных

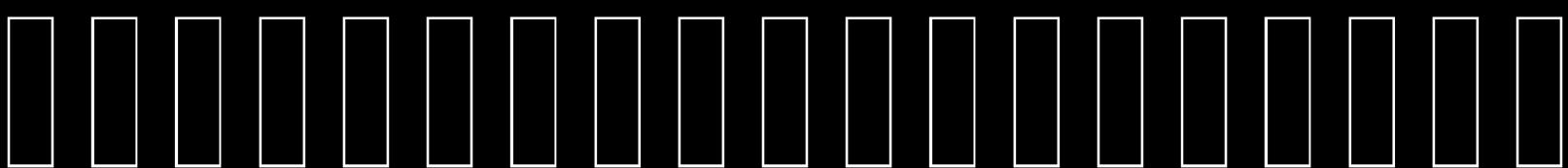


AC-22-05



IDEA

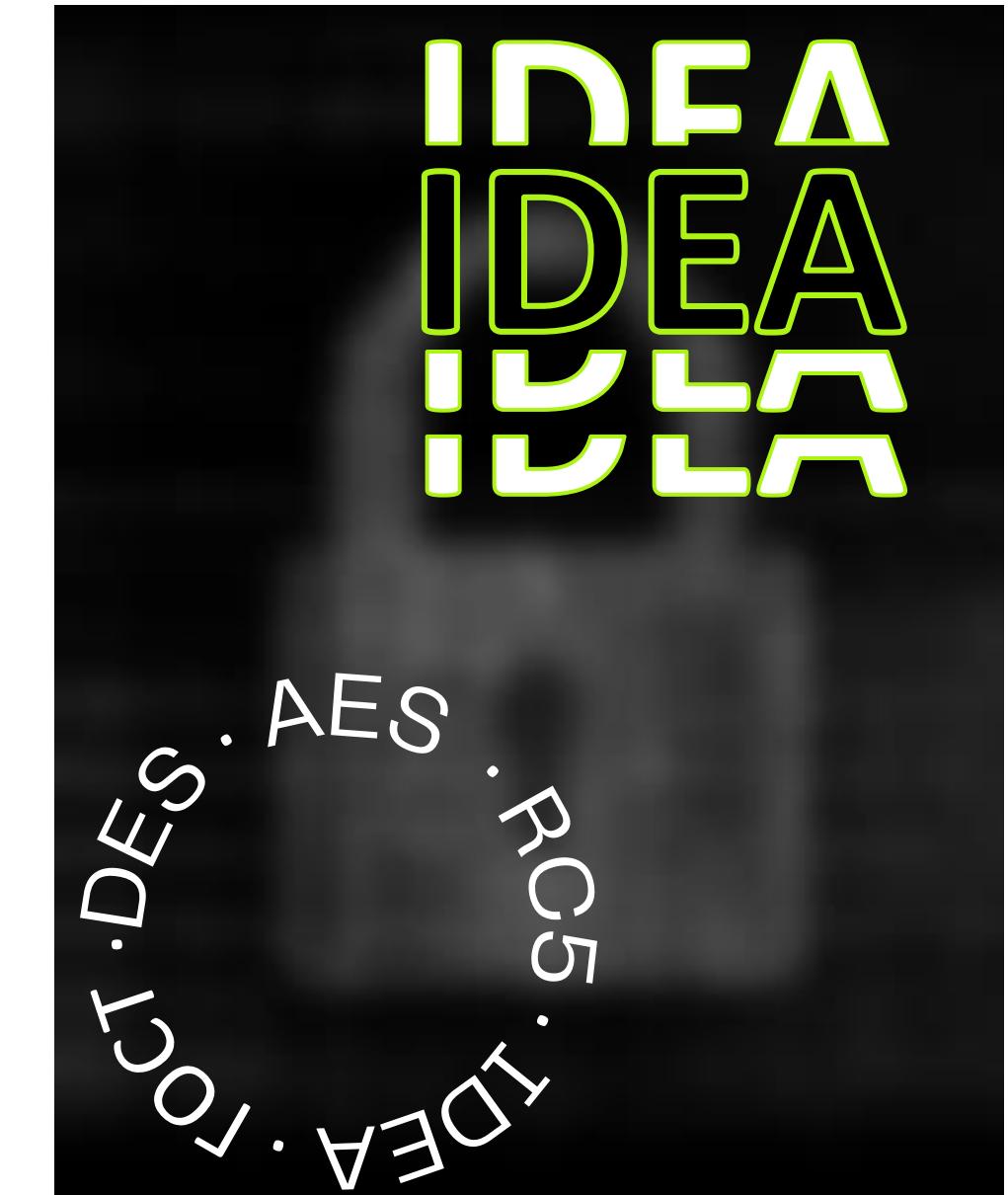
Выполнил : Капаров Алимурад

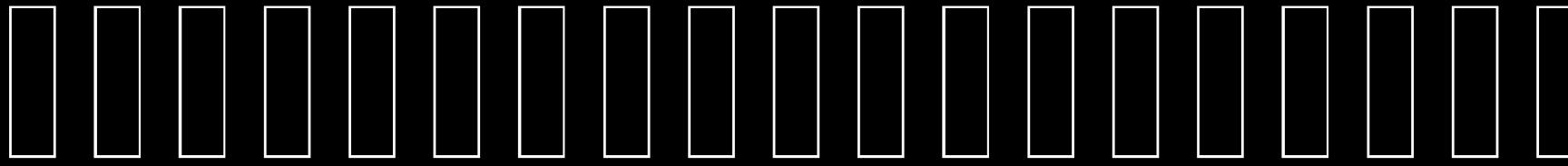


IDEA

■ Алгоритм работает с блоками данных фиксированной длины, а именно 64 бита. Важно отметить, что IDEA оперирует с 64-битными блоками данных как с 128-битным ключом. Такой подход обеспечивает стойкость и эффективность шифрования.

■ IDEA внедряет несколько важных шагов преобразования данных, включая перестановку бит, операции над конечными полями и подстановку. Эти методы обеспечивают высокий уровень безопасности и устойчивость к различным видам криптоанализа.



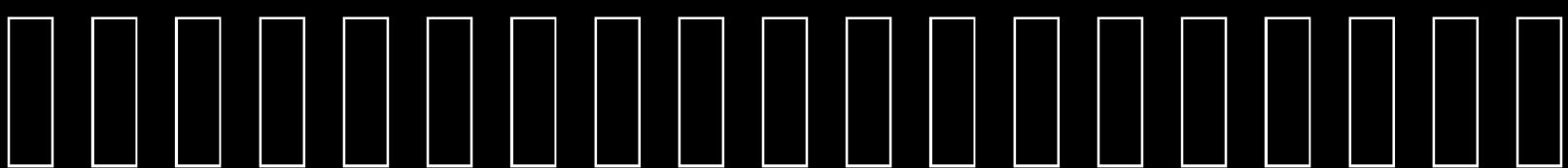


AC-22-05



CAST-128

Выполнила : Егоркина Маргарита

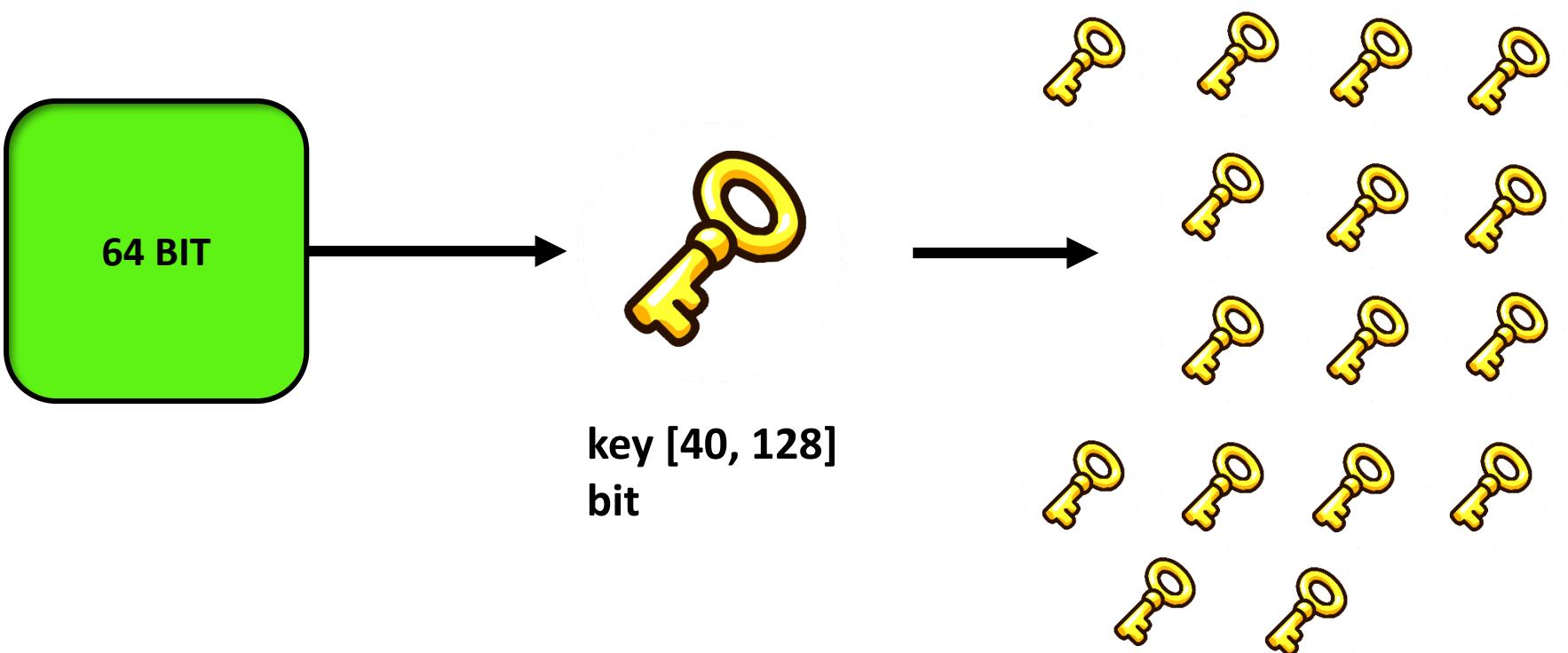


CAST-128

Основные характеристики алгоритма CAST-128:

- Размер блока данных: 64 бита.
- Длина ключа: от 40 до 128 бит (в шагах по 8 бит).
- Количество раундов: 16.
- Существует восемь S-блоков размером 8×32 , четыре из которых используются в расписании ключей, а остальные четыре - в реальном шифровании.

INITIAL INITIALIZATION

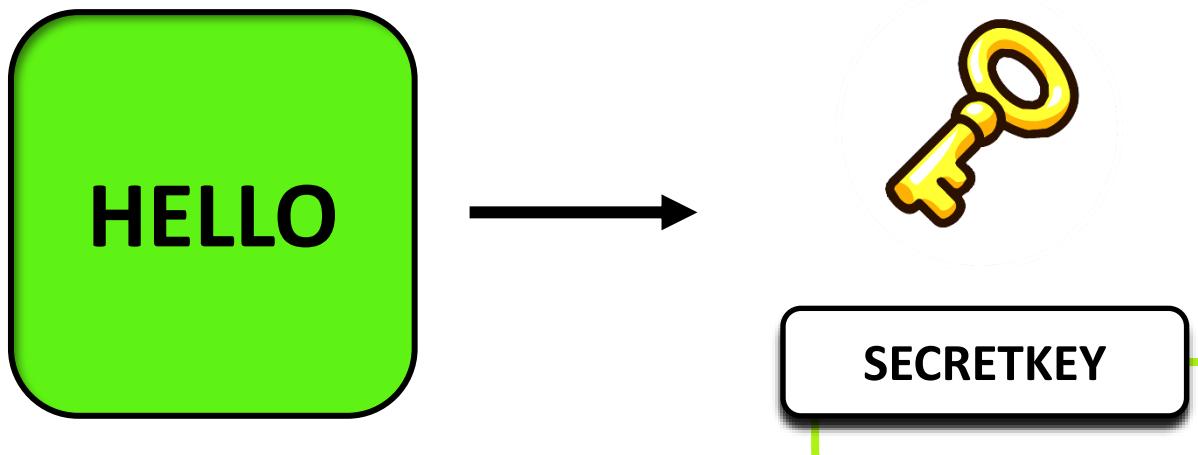


CAST-128

CAST-128

ENCRYPTION ROUNDS

ИСХОДНЫЕ ДАННЫЕ



IDEA · DES · ROT · DES · AES · CABIE-128 · IDEA ·

CAST-128

ENCRYPTION ROUNDS

ПРЕОБРАЗОВАНИЕ В БИНАРНОЕ ПРЕДСТАВЛЕНИЕ

HELLO

H E L L O
01001000 01000101 01001100 01001100 01001111

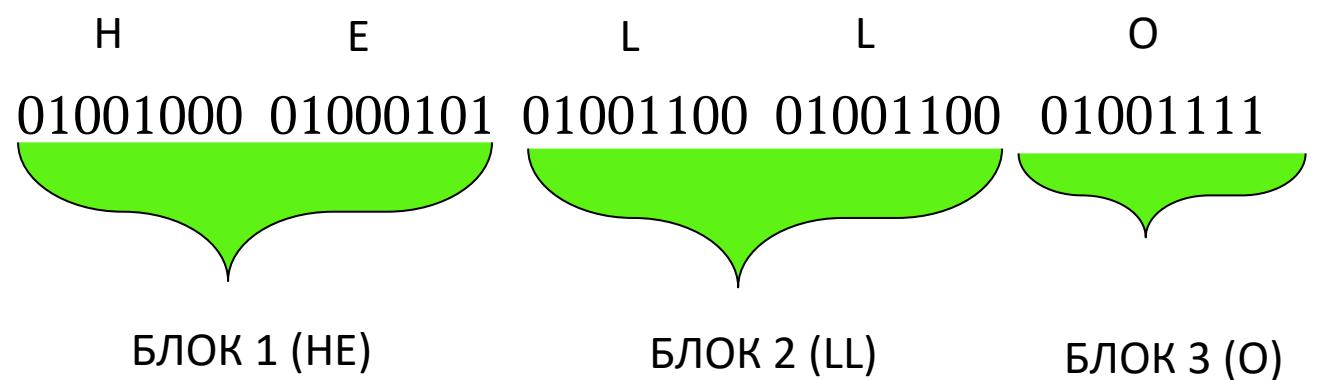
SECRETKEY

S	E	C	R	E
01010011	01000101	01000011	01010010	01000101
T	K	E	Y	
01010100	01001011	01000101	01011001	

CAST-128

ENCRYPTION ROUNDS

ШИФРОВАНИЕ



CAST-128

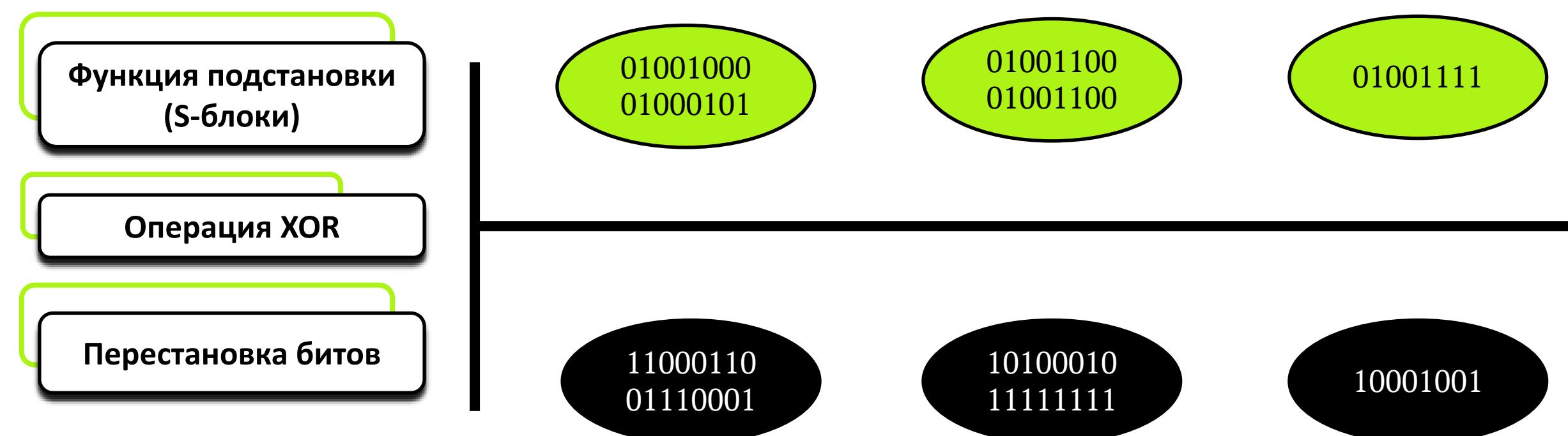
CAST-128

CAST-128

ENCRYPTION ROUNDS

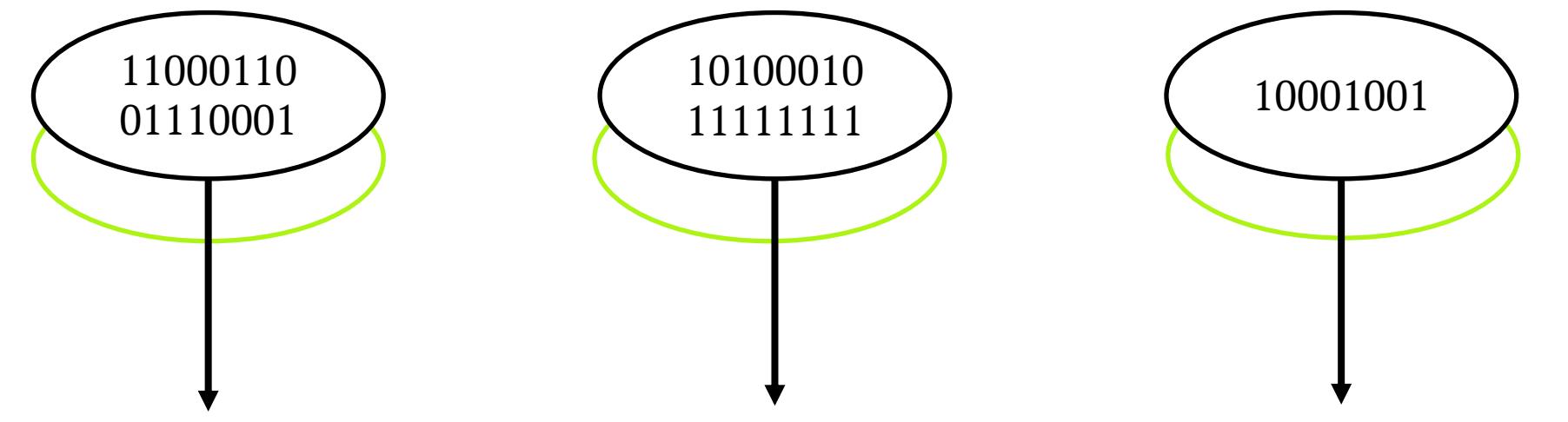
ПРИМЕНЯЕМ АЛГОРИТМ CAST-128 ДЛЯ КАЖДОГО БЛОКА ПООЧЕРЕДНО

ROUND 1 – ROUND 16



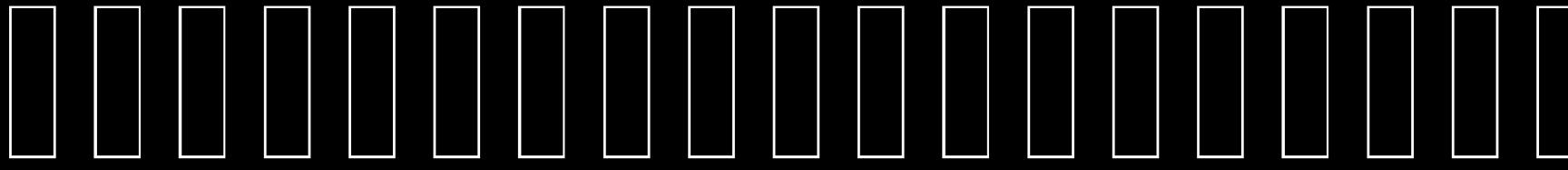
CAST-128

WE RECEIVE ENCRYPTED DATA BLOCKS + CONNECTING ENCRYPTED BLOCKS



11000110 01110001 10100010 11111111 10001001

01001000 01000101 01001100 01001100 01001111

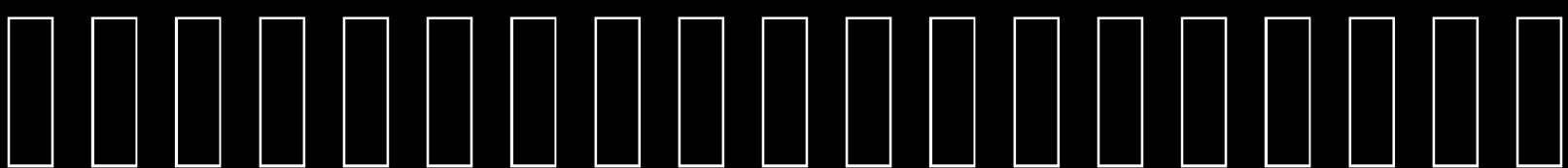


AC-22-05



RC5

Выполнил : Желудов Тимофей



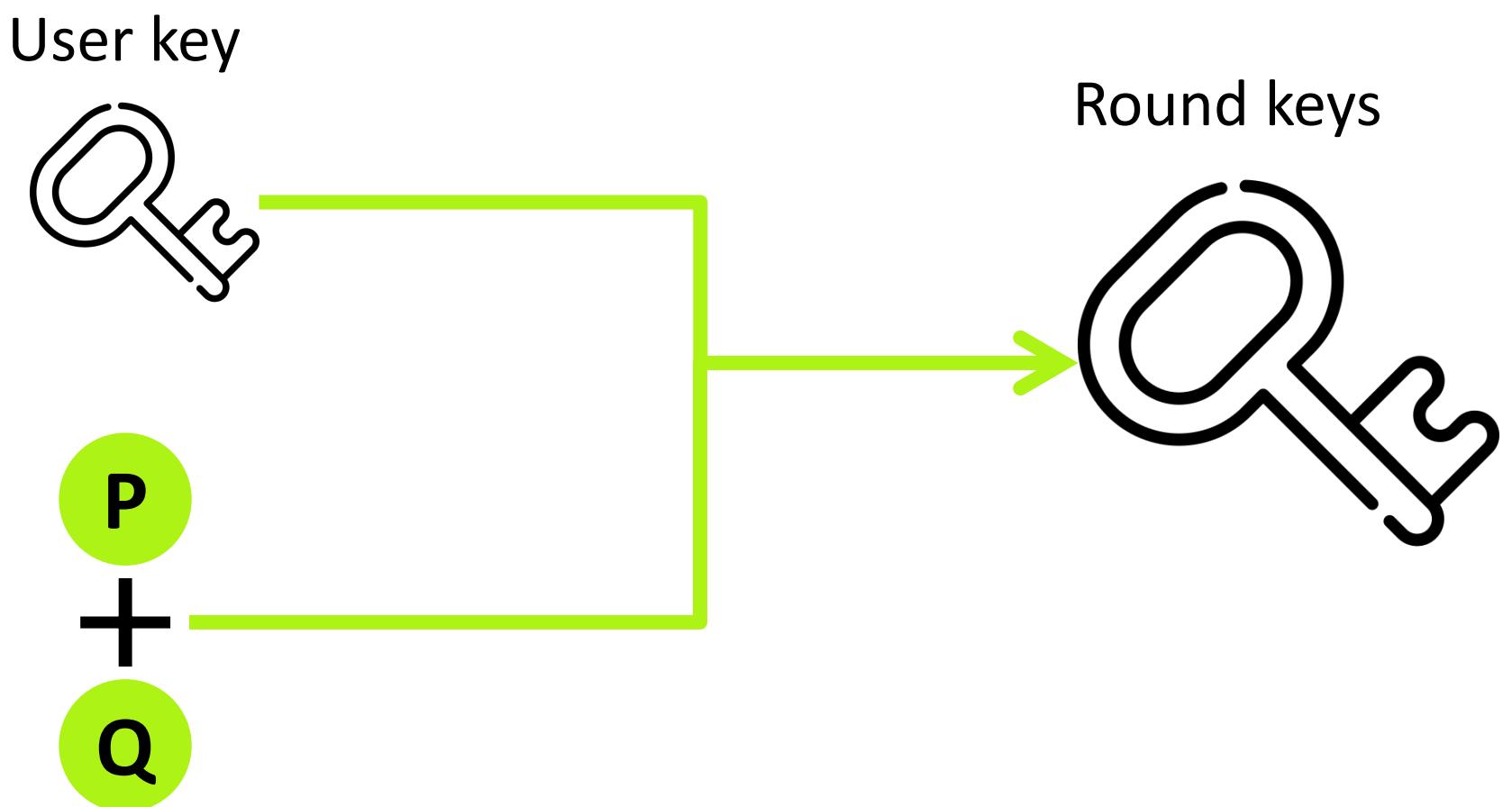
RC5

Основные параметры алгоритма:

- W — половина длины блока в битах, возможные значения 16, 32 и 64
- R — число раундов
- b — длина ключа в байтах

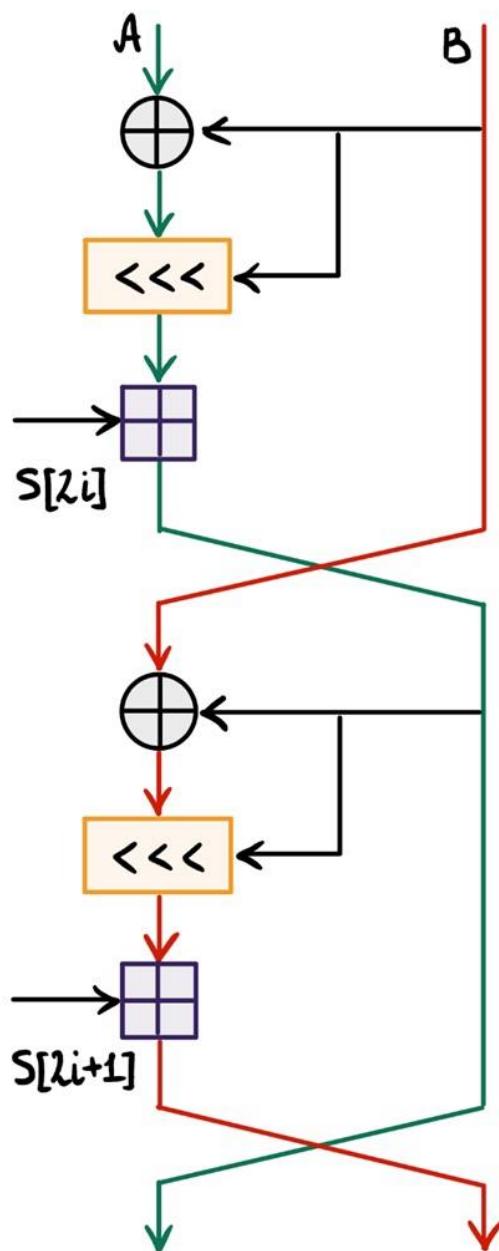
DES · AES · RC5 · IDEA · LOC

Расширение ключа

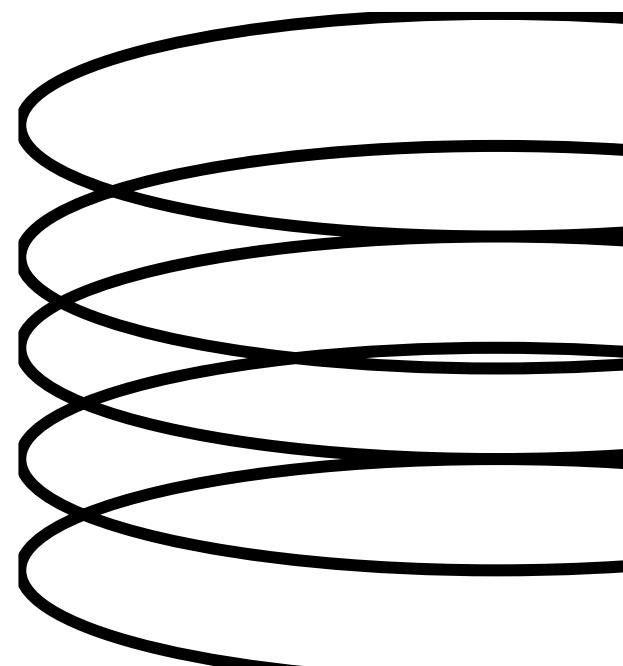
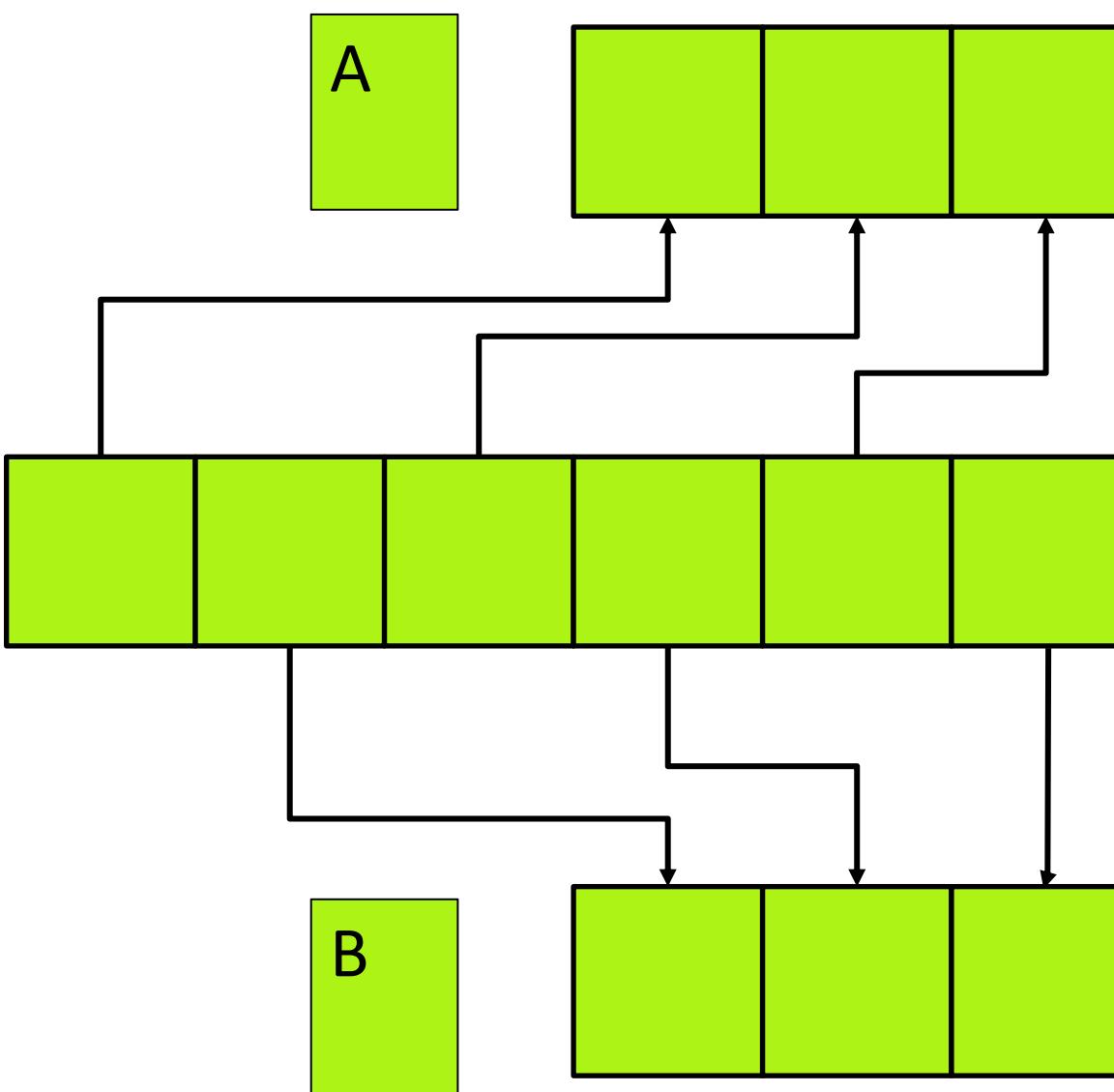


RC5

Шифровка/Дешифровка



User message



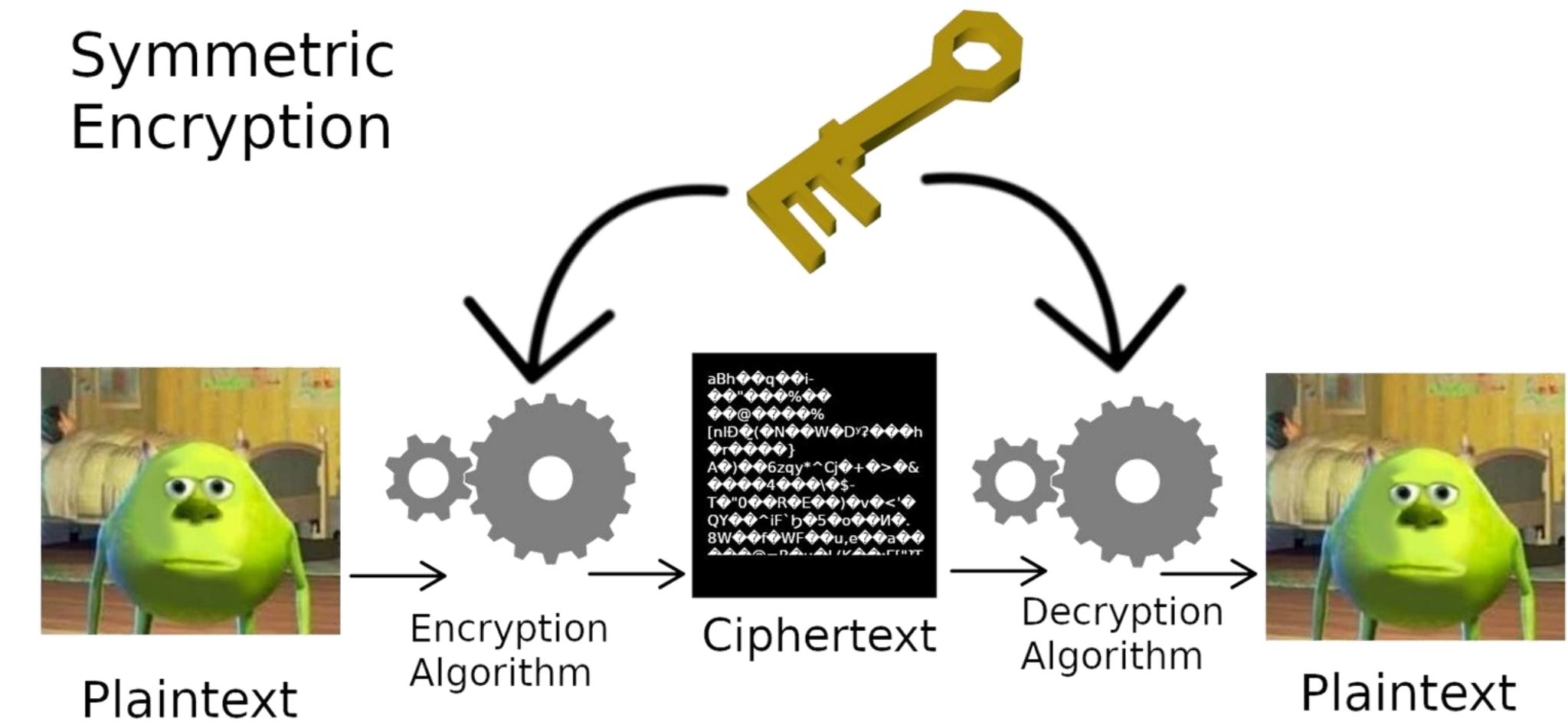
ИТОГИ

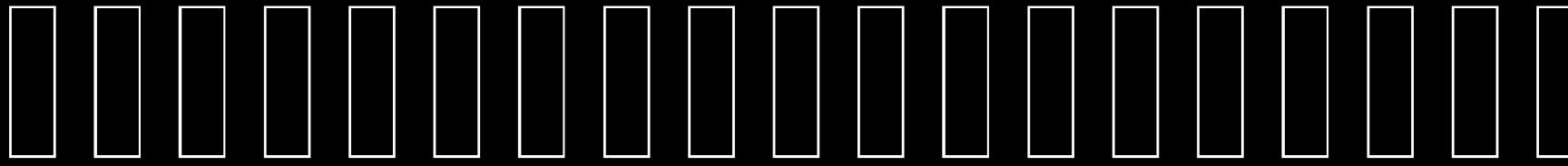
Название алгоритма	Время выполнения алгоритма в мкс на 150 кб данных	Время выполнения алгоритма в мкс на 350 кб данных	Время выполнения алгоритма в мкс на 520 кб данных	Устойчивость к взлому
AES	226	548	874	█ █ █
IDEA	367	725	1367	█ █ █
ГОСТ 28147-89	398	856	1564	█ █ █
Blowfish	420	866	2055	█ █ █
RC5	637	1236	2513	█ █ █
CAST-128	398	849	1644	█ █ █
DES	2301	4704	8227	█ █ █

Ссылка на репозиторий



Symmetric
Encryption





AC-22-05



Спасибо за внимание

