УГАТУ

Лекция №3

БЛОЧНЫЕ АЛГОРИТМЫ СИММЕТРИЧНОГО ШИФРОВАНИЯ

Дисциплина: Криптографическая защита информации
Преподаватель: Миронов Константин Валерьевич
Поток: БПС-3
Учебный год: 2020/21

УГАТУ

Уфимский государственный авиационный технический университет

Содержание лекции

- **Семейство DES**
  - **DES: Операция зашифровывания-расшифровывания**
  - **DES: Операция расширения ключа**
  - **3DES**
- Алгоритм AES
- Семейство RC

УГАТУ

Уфимский государственный авиационный технический университет

Семейство DES

1971-73 Исследовательский проект Lucifer

- Первая версия – SP-сеть, дальнейшие – сбалансированная сеть Фейстеля

1977 Алгоритм DES

- Размер блока – 64 бита, размер ключа – 56 бит
- К середине 1990-х такая длина ключа утратила криптостойкость

1978 3DES

- Алгоритм использует операции за/расшифровывания DES
- Длина ключа – 112 или 168 бит
- Алгоритм имеет некоторое применение в настоящее время, однако чрезвычайно тяжеловесен в программной реализации

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм DES

Операция зашифровывания

Этап 1. Начальная перестановка T=IP(T)

Этап 2. 16 раундов сети Фейстеля

Этап 3. Конечная перестановка T=FP(T)

- Конечная перестановка обратна начальной FP(IP(T)) = T

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

Таблица начальной перестановки DES

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

Таблица конечной перестановки DES.

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм DES

Функция F

Аргументы: полублок 32 бита, раундовый ключ 48 бит

шаг 1. Перестановка-расширение полублока до 48 бит

шаг 2. XOR расширенного полублока с раундовым ключом

шаг 3. Подстановка-сжатие обратно до 32 бит

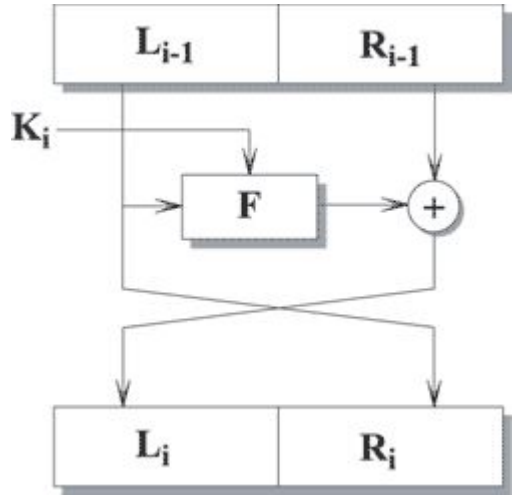
шаг 4. Перестановка

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

Таблица перестановки

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

Таблица перестановки-расширения



Алгоритм DES

Функция F

шаг 3. Подстановка-сжатие обратно до 32 бит

- 48-битный расширенный полублок разбивается на 6-битные слова
- Каждое 6-битное слово заменяется на 4-битное по своей таблице замен (S1..S8)
- В таблице номер строки определяется первым и последним битом слова, номер столбца – 4-мя средними

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	S 1
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	S 2
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	S 3
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	S 4
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	S 5
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
																	S6
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	S 6
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
																	S7
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	S 7
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
																	S8
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	S 8
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм DES

Расширение ключа

шаг 1. Вычисляются C[0] и D[0] как результат перестановки исходного ключа

шаг 2. Для i от 1 до 16 вычисляется C[i] и D[i] как циклический сдвиг C[i-1] и D[i-1] влево
на 1 бит, если i=1,2,9,16
на 2 бита для остальных раундов

шаг 3. i-й раундовый ключ берется как перестановка-сжатие вектора C[i]||D[i]

														C0
50	43	36	29	22	15	8	1	51	44	37	30	23	16	
9	2	52	45	38	31	24	17	10	3	53	46	39	32	
														D0
56	49	42	35	28	21	14	7	55	48	41	34	27	20	
13	6	54	47	40	33	26	19	12	5	25	18	11	4	

Таблица перестановки для расчета C[0] и D[0]

Процедура расширения состоит только из перестановок (включая сжатия и расширения). В расширенном ключе используются только биты исходного ключа, поэтому если исходный ключ состоит лишь из нулей, то и расширенный будет состоять лишь из нулей

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

Таблица перестановки-сжатия для получения раундового

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм 3DES

3DES-EEE3

- ключ 168 бит разбивается на 3 подключа по 56 бит
- текст последовательно зашифровывается по DES на каждом подключе

3DES-EDE3 (Более популярный вариант)

- То же самое, но при шифровании вторым подключом применяется операция расшифровывания

3DES-EEE2 и 3DES-EDE2

- Длина ключа 112 бит, третий подключ равен первому

УГАТУ

Уфимский государственный авиационный технический университет

Семейство DES

Проблемы

- Семейство заточено под аппаратную реализацию, при программной работает медленно
- Размер блока ограничен 64 битами
- Существуют **слабые ключи**
  - Если ключ состоит из одних нулей, то и раундовые подключи будут из одних нулей
  - Если ключ состоит из одних единиц, то и раундовые подключи будут из одних единиц
  - Надежные ключи должны выглядеть как случайные данные
- Если перед зашифровыванием инвертировать открытый текст и ключ, в результате получится инверсия шифротекста:

$$Ш (не(ОТ), не(К)) = не (Ш(ОТ,К))$$

УГАТУ

Уфимский государственный авиационный технический университет

Содержание лекции

- Семейство DES
- **Алгоритм AES**
  - **Операция зашифровывания**
  - **Операция расширения ключа**
- Семейство RC

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм AES

- Rijndael: длина блока и длина ключа 128, 160, 192, 234 или 256 бит
- AES: длина блока 128 бит, длина ключа 128, 192 или 256
- В остальном алгоритмы идентичны
- Число раундов 6+k/32, где k – длина ключа; также есть нулевой раунд
- Классическая SP-сеть

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм AES

Операция зашифровывания

- Байты блока записываются в матрицу State 4 на 4
  - (первые 4 байта в первый столбец, следующие во второй и т. д.)
- На каждом раунде выполняются 4 операции
  - SubBytes – подстановка
  - ShiftRows - перестановка
  - MixColumns - перестановка
  - AddRoundKey – XOR с раундовым ключом
- На нулевом раунде выполняется только AddRoundKey
- На финальном раунде не выполняется операция MixColumns
- При расшифровке выполняются операции InvSubBytes, InvShiftRows, InvMixColumns

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм AES

Операция зашифровывания

- SubBytes – подстановка для каждого байта по общей таблице замен

x \ y	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	84
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

Таблица замен
SubBytes

- ShiftRows – перестановка
  - Первая строка State неизменна
  - Вторая << на 1 байт
  - Третья << на 2 байта
  - Четвертая << на 3 байта
- MixColumns - на каждый столбец в поле Галуа умножается фиксированная матрица
- AddRoundKey – XOR с раундовым ключом

Алгоритм AES

Операция расширения ключа

Для AES-128 (в других версиях – другая процедура)

- Расширенный ключ состоит из 32-битных слов
- Первые 4 слова заполняются исходным ключом, затем, каждое j-е слово вычисляется на основе предыдущих:

```
ЕСЛИ (j mod 4 = 1) ТО
        W_J=SubWord(W[j-1]) \\ аналогично SubBytes
        W_J=RotWord(W_J) \\ циклический сдвиг влево на 1 байт
        W_J = XOR(W_J, RCon]) \\ RCon зависит от номера раунда
        W[j] = XOR(W_J, W[j-4]) 2
ИНАЧЕ
        W[j]=XOR(W[j-1], W[j-4])
```

Раунд	Константа (RCon)	Раунд	Константа (RCon)
1	$(01\ 00\ 00\ 00)_{16}$	6	$(20\ 00\ 00\ 00)_{16}$
2	$(02\ 00\ 00\ 00)_{16}$	7	$(40\ 00\ 00\ 00)_{16}$
3	$(04\ 00\ 00\ 00)_{16}$	8	$(80\ 00\ 00\ 00)_{16}$
4	$(08\ 00\ 00\ 00)_{16}$	9	$(1B\ 00\ 00\ 00)_{16}$
5	$(10\ 00\ 00\ 00)_{16}$	10	$(36\ 00\ 00\ 00)_{16}$

- Ключ i-го раунда K[i] равен словам W[j-3] || W[j-2] || W[j-1] || W[j] где j=(i+1)*4
- Можно либо посчитать расширенный ключ целиком, либо поочередно рассчитывать раундовые ключи для каждого раунда (например, параллельно с зашифровыванием)
- Ключ нулевого раунда идентичен исходному

УГАТУ

Уфимский государственный авиационный технический университет

Содержание лекции

- Семейство DES
- Алгоритм AES
- **Семейство RC**
  - **RC2**
  - **RC5**
  - **RC6**

УГАТУ

Уфимский государственный авиационный технический университет

Семейство RC

Алгоритмы, разработанные Роном Райвестом

(RC – Ron’s Code, Rivest Cipher)

- RC1 – «не вышел за пределы записной книжки»
- RC2 -1987
- RC3 – взломан в процессе разработки
- RC4 – 1987, потоковый
- RC5 - 1994
- RC6 – 1998, переделка RC5 под конкурс AES

УГАТУ
Уфимский государственный авиационный технический университет

Алгоритм RC2

- Разработан как альтернатива DES
- Не был запрещен к экспорту из США
- Быстрее в программной реализации и проще в аппаратной (т.к. подстановка не используется при шифровании, а только при расширении ключа)
- Размер блока – 64 бита
- Размер ключа – от 9 до 1024 бит
  - на практике обычно – 56 бит в эпоху DES и 128/256 теперь
- Длина расширенного ключа – 1024 бита или 128 байт
- Несбалансированная сеть Фейстеля
  - Блок разбивается не на 2 полублока, а на 4 16-битных слова R[0]R[1]R[2]R[3]

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм RC2

Процедура зашифровывания

- Раунды бывают смешивающие и объединяющие
- Всего 16 смешивающих раундов
- После 5-го и 11-го смешивающих раундов выполняется по одному объединяющему
- Смешивающий раунд

  шаг 1. Для i от 0 до 3 выполнить

  $$R_i = R_i \boxplus f(K_{ij}, R_{i-1 \bmod 4}, R_{i-2 \bmod 4}, R_{i-3 \bmod 4})$$

  шаг 2. Циклический сдвиг влево R[0], R[1], R[2] и R[3] на 1, 2, 3 и 5 бит соответственно

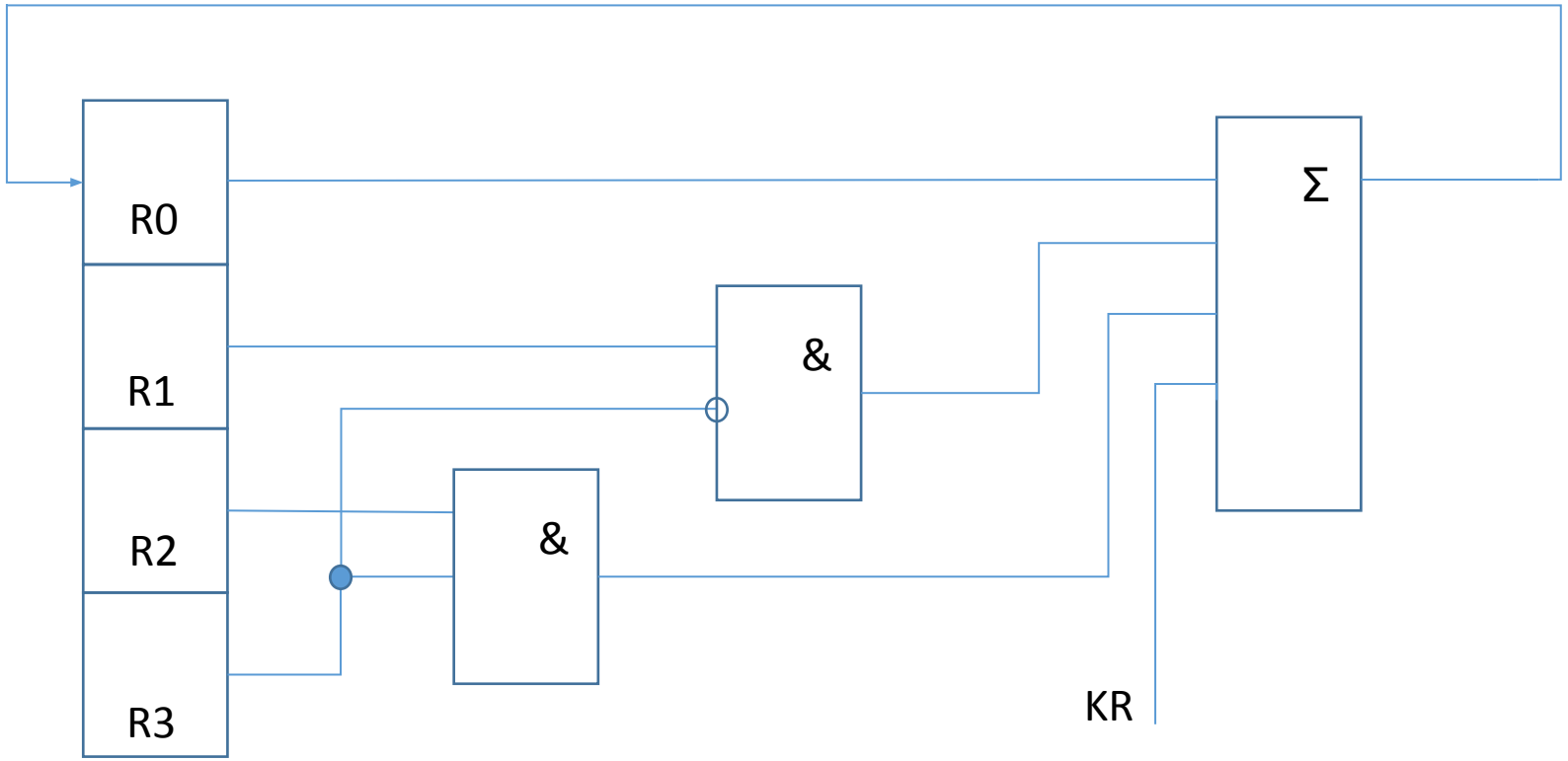
- Объединяющий раунд – каждое слово складывается с соответствующим ему раундовым подключом

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм RC2

Процедура зашифровывания



$$R_i = R_i \boxplus K_{ij} \boxplus (R_{i-1 \bmod 4} \& R_{i-2 \bmod 4}) \boxplus (R_{i-3 \bmod 4} \& \bar{R}_{i-1 \bmod 4})$$

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм RC2

Процедура расширения ключа

- Расширенный ключ записывается в байтовый массив L[0]…L[127]
- Число байт в исходном ключе обозначается как t (округляется вверх)
- Создается байт ТМ, заполненный нулями
- Если число байт нецелое, ключ дополняется единицами и то же число единиц записывается в те же разряды ТМ
- Используется таблица замен на основе 16-чного представления π

d9	78	f9	c4	19	dd	b5	ed	28	e9	fd	79	4a	a0	d8	9d
c6	7e	37	83	2b	76	53	8e	62	4c	64	88	44	8b	fb	a2
17	9a	59	f5	87	b3	4f	13	61	45	6d	8d	09	81	7d	32
bd	8f	40	eb	86	b7	7b	0b	f0	95	21	22	5c	6b	4e	82
54	d6	65	93	ce	60	b2	1c	73	56	c0	14	a7	8c	f1	dc
12	75	ca	1f	3b	be	e4	d1	42	3d	d4	30	a3	3c	b6	26
6f	bf	0e	da	46	69	07	57	27	f2	1d	9b	bc	94	43	03
f8	11	c7	f6	90	ef	3e	e7	06	c3	d5	2f	c8	66	1e	d7
08	e8	ea	de	80	52	ee	f7	84	aa	72	ac	35	4d	6a	2a
96	1a	d2	71	5a	15	49	74	4b	9f	d0	5e	04	18	a4	ec

c2	e0	41	6e	0f	51	cb	cc	24	91	af	50	a1	f4	70	39
99	7c	3a	85	23	b8	b4	7a	fc	02	36	5b	25	55	97	31
2d	5d	fa	98	e3	8a	92	ae	05	df	29	10	67	6c	ba	c9
d3	00	e6	cf	e1	9e	a8	2c	63	16	01	3f	58	e2	89	a9
0d	38	34	1b	ab	33	ff	b0	bb	48	0c	5f	b9	b1	cd	2e
c5	f3	db	47	e5	a5	9c	77	0a	a6	20	68	fe	7f	c1	ad

Таблица замен

Алгоритм RC2

Процедура расширения ключа

ДЛЯ i ОТ t ДО 127

L[i] = L[i-1]+L[i-t]

L[i] = S(L[i]) \\ подстановка по таблице замен

КОНЕЦ

L[128-t] = L[128-t] & TM \\ обнуляются биты, на которые в байте t не приходится дополнение

L[128-t] = S(L[128-t])

ДЛЯ i ОТ 127-t ДО 0

L[i] = XOR (L[i+1],L[i+t])

L[i] = S(L[i])

КОНЕЦ

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм RC2

Выбор раундового ключа

Выбор раундового ключа

- L[0]…L[127] разбивается на 64 раундовых подключа
- В смешивающих раундах подключи используются последовательно (по 4 на раунд)
- В объединяющем раунде для зашифровки текущего слова берется подключ с номером, равным численному выражению младших 6 бит слова, расположенного слева от текущего

УГАТУ

Уфимский государственный авиационный технический университет

Алгоритм RC5

- Версия алгоритма обозначается по типу RC5-32/12/16
  - 32 – длина обрабатываемого слова-полублока (м. б. также 16 и 64); длина блока вдвое больше
  - 12 – число раундов (от 1 до 255)
  - 16 - длина ключа в байтах (от 1 до 255, т. е. от 8 до 2048 бит с шагом 8)
- RC5 условно считается разновидностью сети Фейстеля
- Расшифровывание выполняется в виде операций, обратных зашифровыванию в обратном порядке

Алгоритм RC5

Процедура зашифровывания

На каждом раунде производятся операции:

$$L_i = (L_{i-1} \oplus R_{i-1}) \lll R_{i-1}$$
$$R_i = (R_{i-1} \oplus L_{i-1}) \lll L_{i-1}$$
$$L_i||R_i = L_i||R_i \boxplus K_i$$

- Сложение с подключом выполняется также на нулевом раунде
- Циклический сдвиг обеспечивает лавинный эффект
- Если число раундов больше восьми, изменение любого бита ОТ будет влиять на величину циклических сдвигов

Алгоритм RC5

Процедура расширения ключа (версия с 32-битным полублоком)

- Расширенный ключ – массив 32-битных слов S[0]…S[2r+1]

  r – число раундов
- Раундовый ключ K[i]=S[2i]||S[2i+1]
- Исходный ключ записывается в массив 32-битных слов L[0]…L[c-1]
- Слово L[n] при необходимости дополняется нулями
- Массив S изначально заполняется с помощью конгруэнтного генератора ПСП заданного в 16-чной системе:

  S[0]=B7E15163

  S[i]=(S[i-1] + 9E3779B9) mod FFFFFFFF

```
A = 0; B = 0; i = 0; j = 0;
n = max(c, 2r+2)
ДЛЯ k ОТ 1 ДО n
    S[i] = (S[i]+A+B) <<< 3
    A = S[i]
    L[i] = (L[i]+A+B) <<< (A+B)
    B = L[i]
    i = (i+1) mod (2r+2)
    j = (j+1) mod c
КОНЕЦ
```

Алгоритм RC6

- Адаптация RC5 под условия конкурса AES
- Параметры варьируются как в RC5
- Конкурсные версии - RC6-32/20/16, RC6-32/20/24 и RC6-32/30/32
- Уступил Rijndael из-за медленного выполнения арифметического умножения на ряде платформ
- Является несбалансированной сетью Фейстеля
- Отличия от RC5:
  - Блок делится не на 2 слова, а на 4 A,B,C,D
  - После каждого раунда блок сдвигается на 1 слово влево
  - Преобразование раунда имеет следующий вид:

    t1 = (B * (2B⊞1)) <<< 5;

    t2 = (D * (2D⊞1)) <<< 5;

    A = xor(A,t1) <<< t2

    C = xor(C,t2) <<< t1

УГАТУ

Уфимский государственный авиационный технический университет

Темы докладов

- **Режим XTS**
- **Режим RandomDelta**
- **Алгоритм Blowfish**
- **Алгоритм Twofish**
- **Алгоритм Threefish**