ГОСТ 28147-89

ГОСТ 28147-89

В России принят ГОСТ 28147-89, рекомендуемый к использованию для криптографической защиты данных.

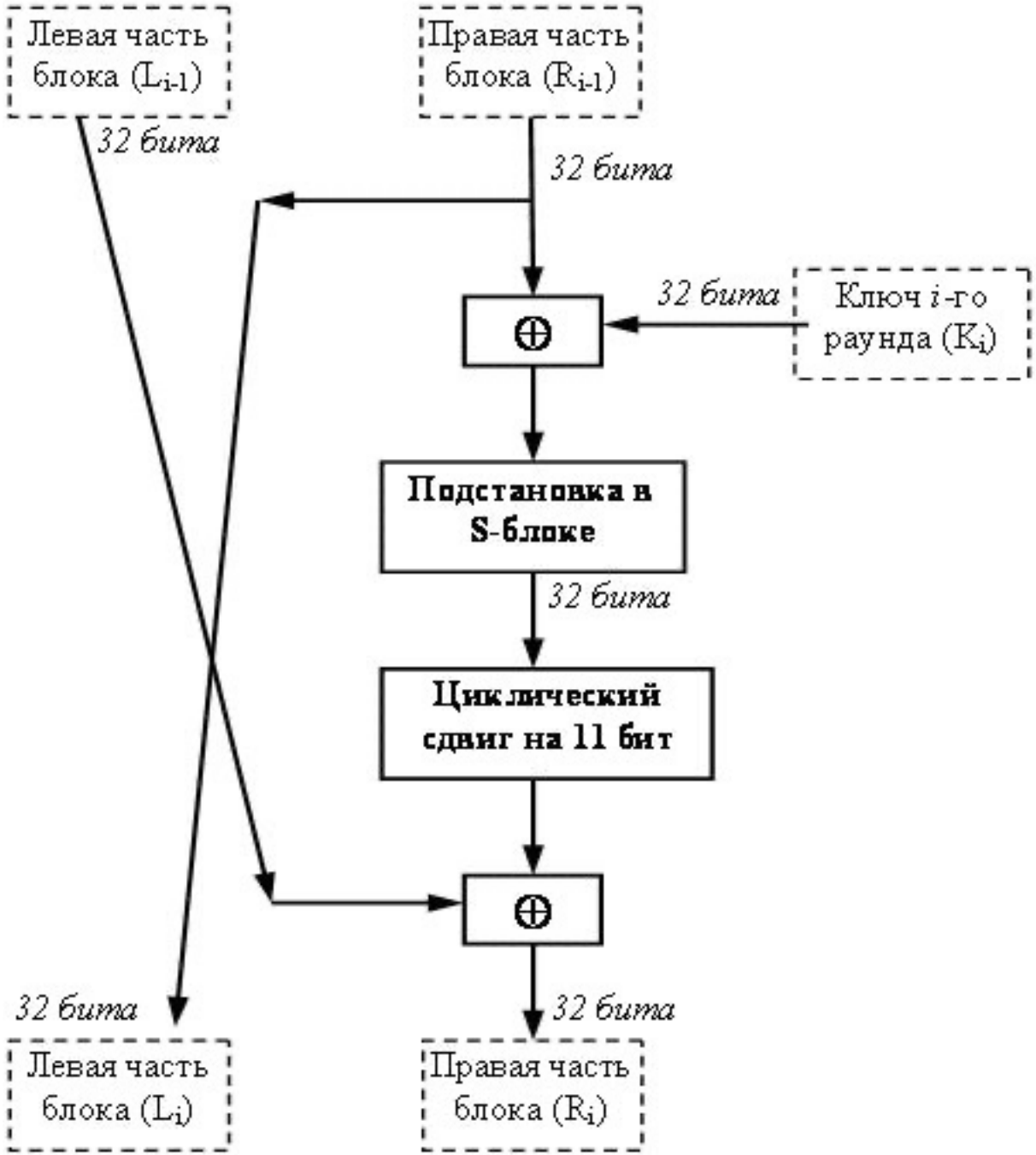
ГОСТ 28147-89 является блочным шифром с закрытым ключом. Основные параметры алгоритма ГОСТ 28147-89 следующие:

- размер блока – 64 бита,
- размер ключа – 256 *бит*,
- количество раундов – 32.
- *Алгоритм* представляет собой классическую *сеть* Фейштеля.

В алгоритме шифрования используются следующие *операции*:

- сложение слов по модулю 2^{32};
- циклический сдвиг слова влево на указанное число бит;
- побитовое сложение по модулю 2;
- замена по таблице.

Алгоритм ГОСТ 28147-89



Подстановка в S блоке

S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
0000	0010	0101	0011	1010	0111	1111	0100
0	2	5	3	10	7	15	4
5	1	3	13	12	2	11	10
0101	0001	0011	1101	1100	0010	1011	1010

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

Последовательность использования подключей при шифровании

Раунд	1	2	3	4	5	6	7	8
Подключ	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
Раунд	9	10	11	12	13	14	15	16
Подключ	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
Раунд	17	18	19	20	21	22	23	24
Подключ	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
Раунд	25	26	27	28	29	30	31	32
Подключ	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0

Последовательность использования подключей при расшифровании

Раунд	1	2	3	4	5	6	7	8
Подключ	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0
Раунд	9	10	11	12	13	14	15	16
Подключ	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0
Раунд	17	18	19	20	21	22	23	24
Подключ	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0
Раунд	25	26	27	28	29	30	31	32
Подключ	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0

Ключевые термины

- **ГОСТ 28147-89** – российский стандарт на блочный *алгоритм симметричного шифрования*.