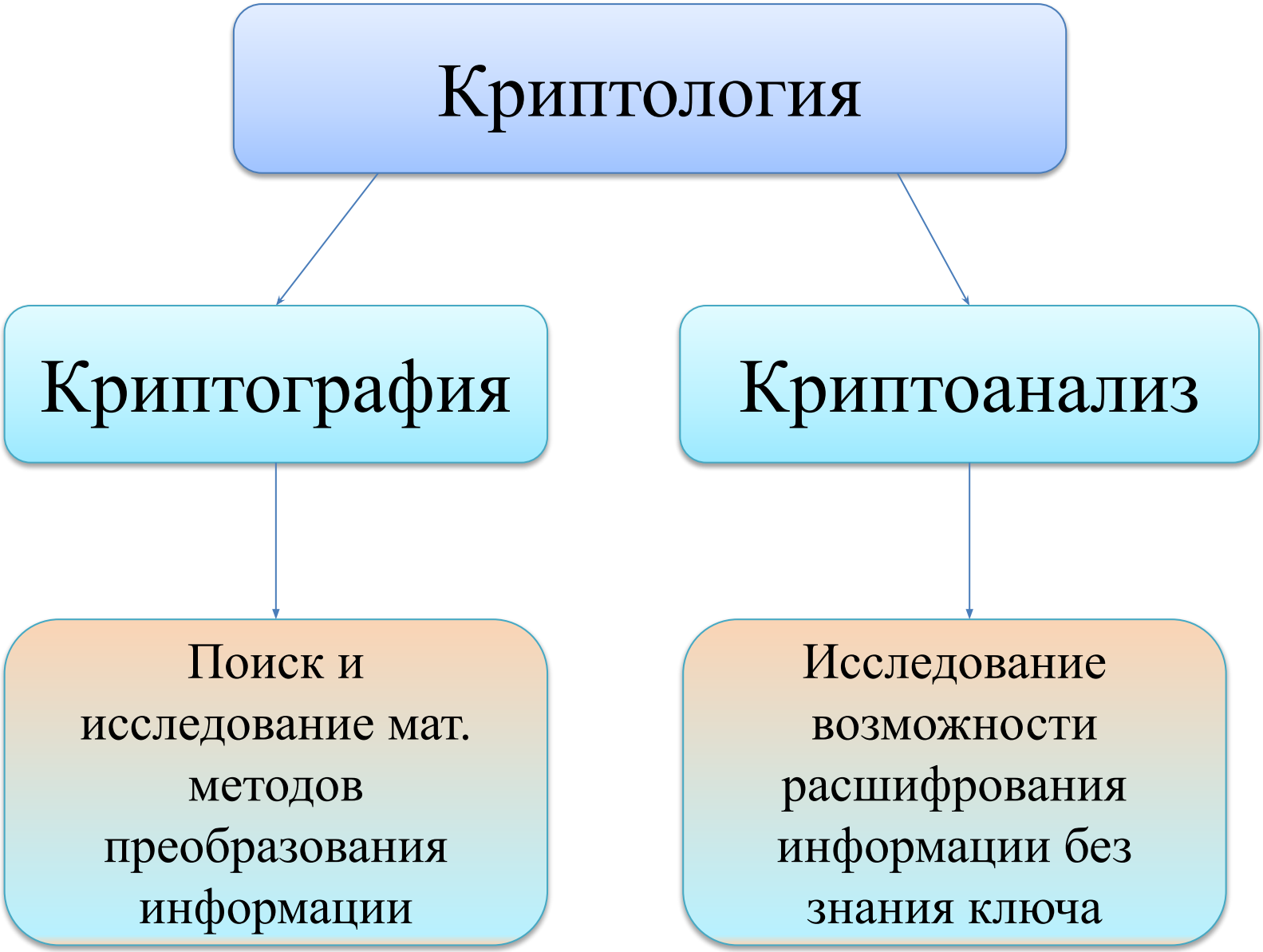
Симметричная криптография

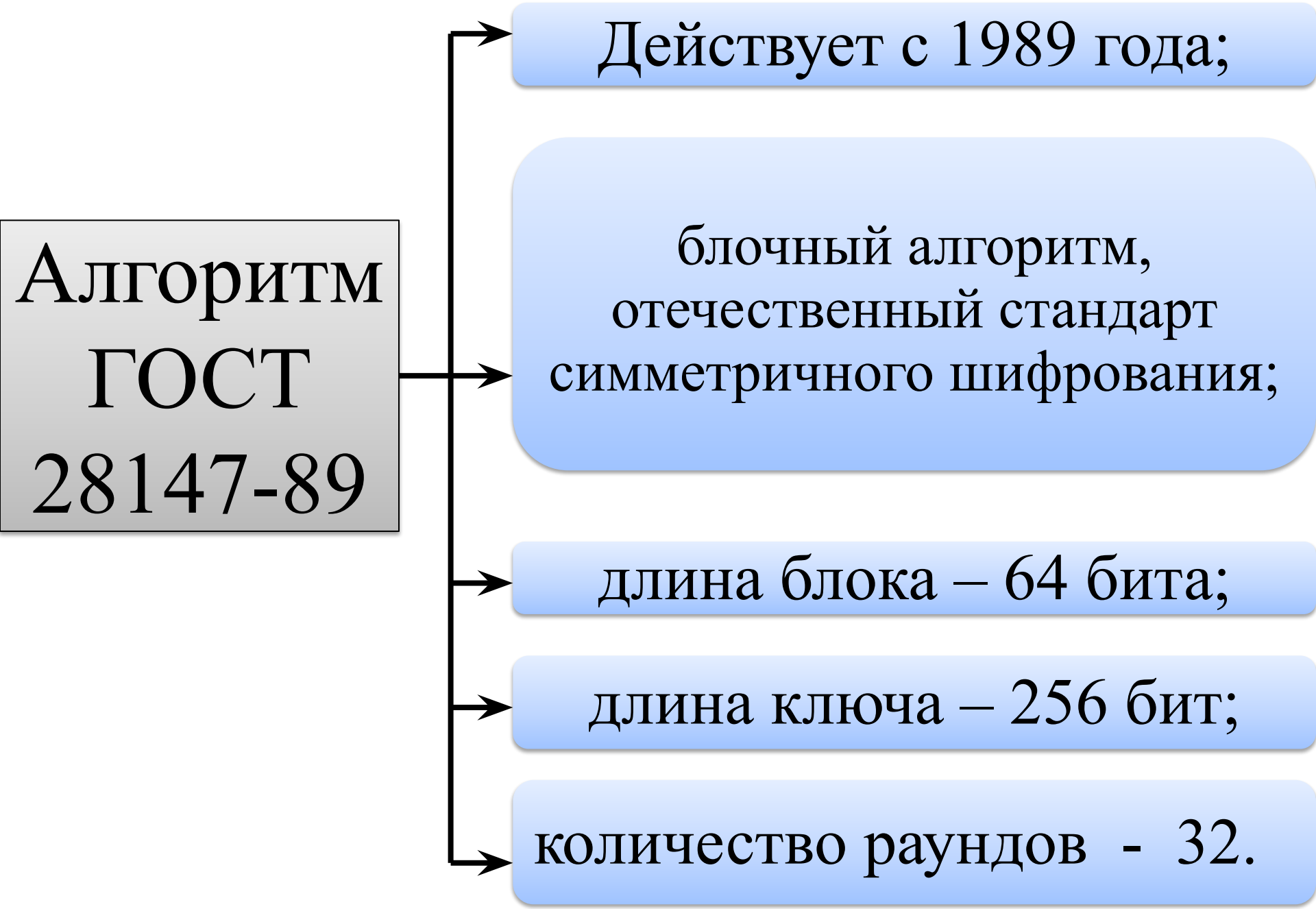

Криптология
Криптография
Криптоанализ
Поиск и исследование мат. методов преобразования информации
Исследование возможности расшифрования информации без знания ключа


Использование криптографических методов
Хранение конфиденциальной и секретной информации
Установление подлинности сообщений
Передача конфиденциальной и секретной информации

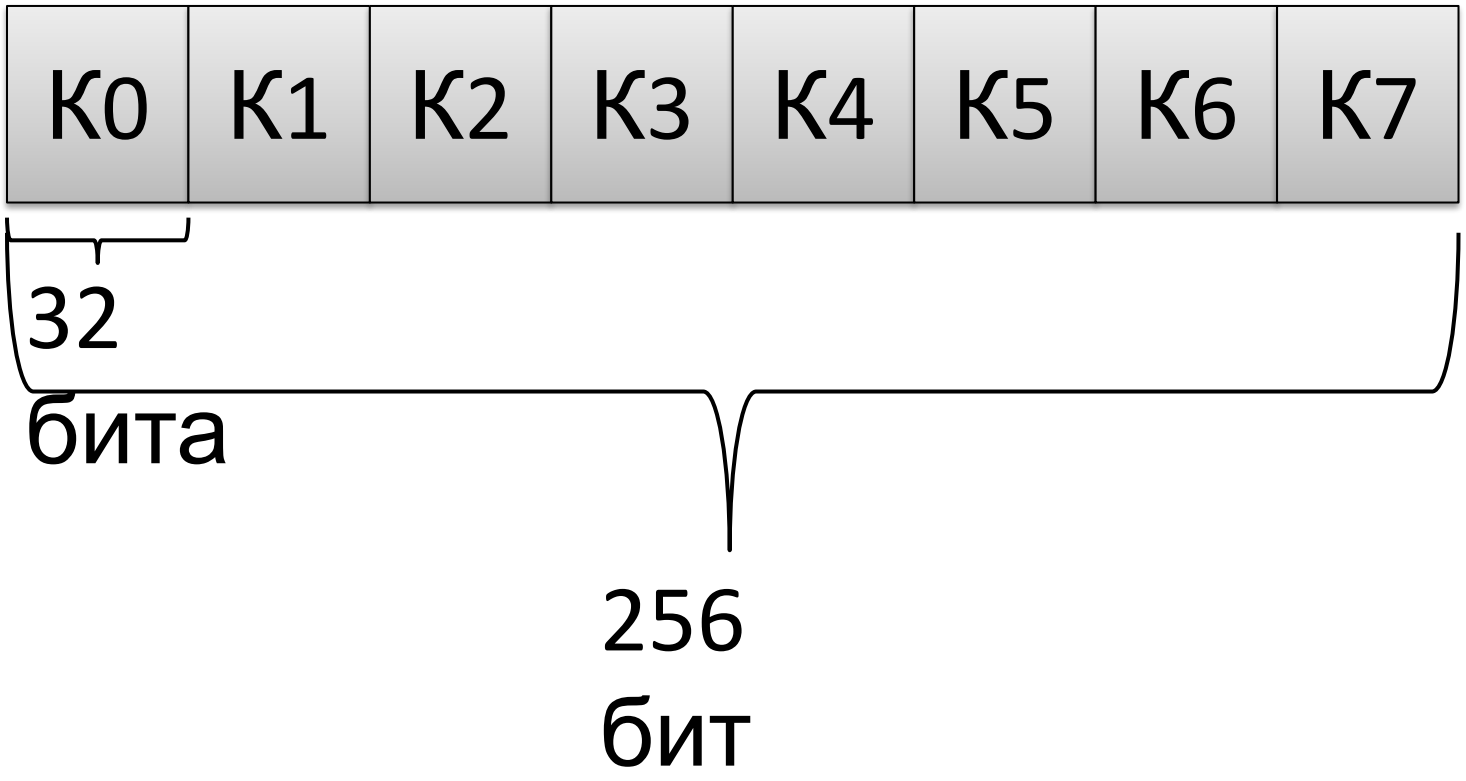
Криптографическая система с секретным ключом (Симметричная криптография)


Криптографические системы
Ограниченного использования
Общего использования
Стойкость основывается на сохранении в секрете алгоритма шифрования
Стойкость – основывается на секретности ключа, Алгоритм шифрования открыт

Алгоритм ГОСТ 28147-89


Алгоритм ГОСТ 28147-89
Действует с 1989 года;
блочный алгоритм, отечественный стандарт симметричного шифрования;
длина блока – 64 бита;
длина ключа – 256 бит;
количество раундов - 32.

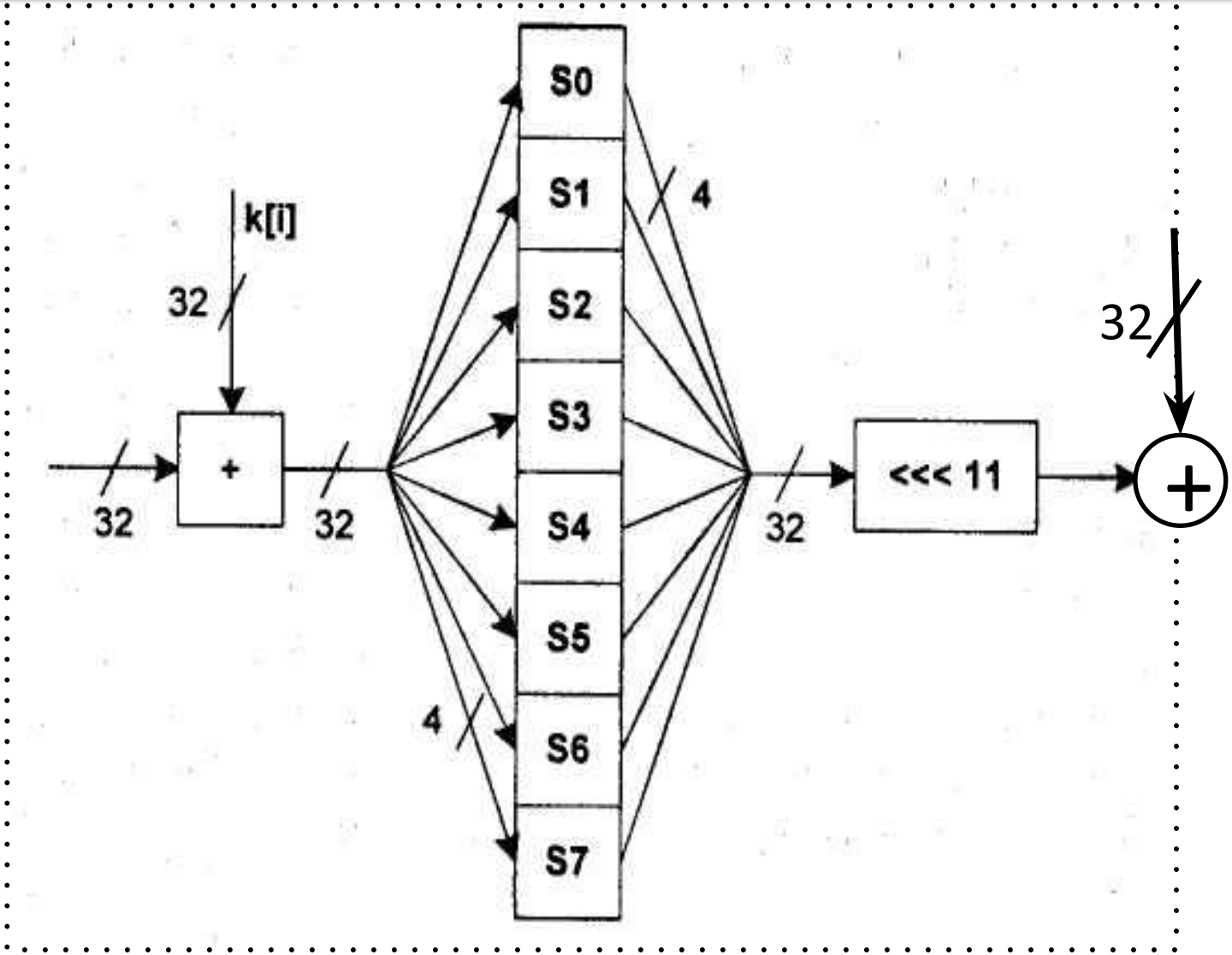
Основной 256-битный ключ делится на 32-битные подключи K0-K7



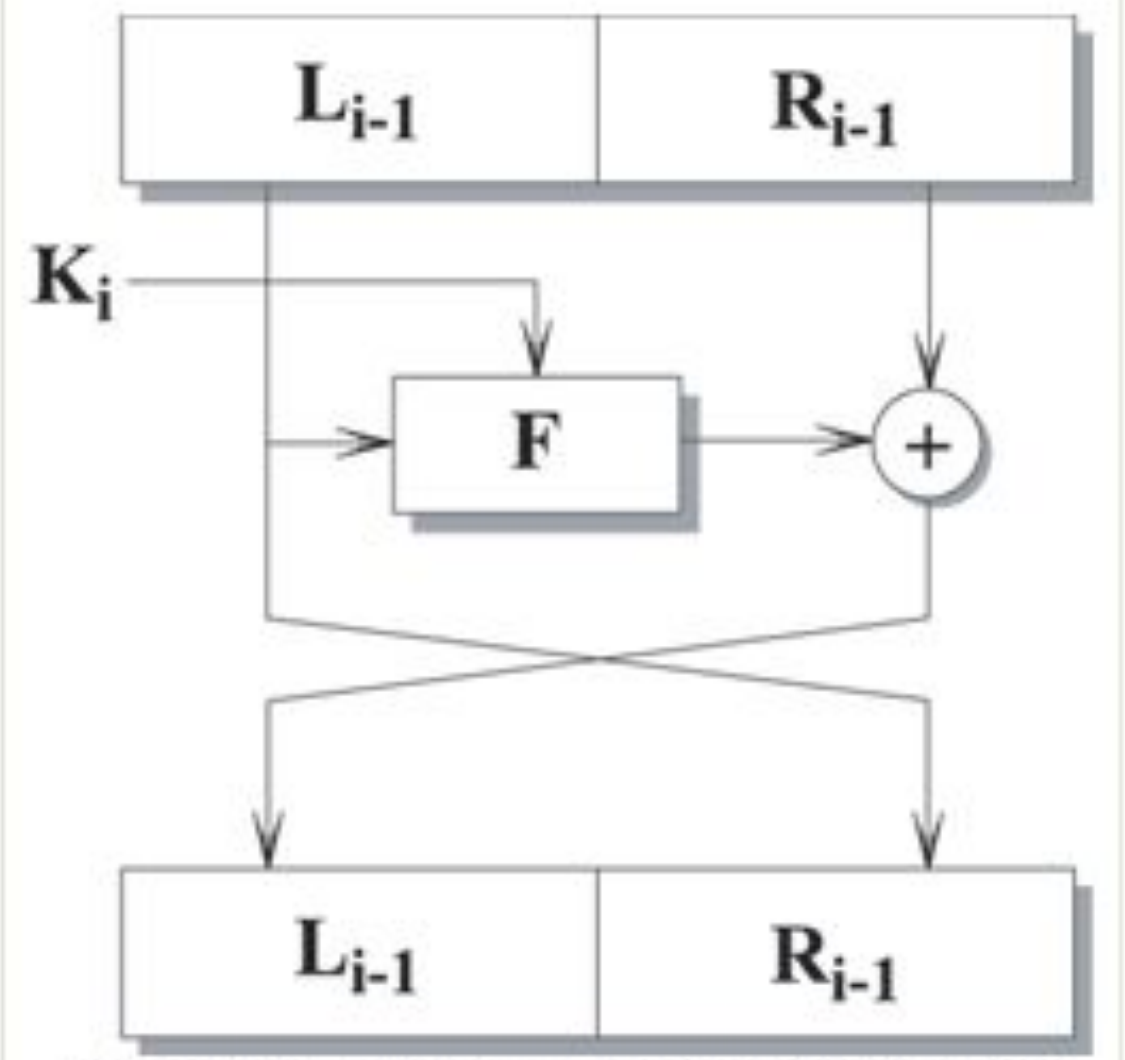
Алгоритм ГОСТ 28147-89. Образующая функция F

- правая половина блока и ***i-ый*** подключ складываются по модулю 2^{32};
- результат разбивается на ***8*** 4-битовых значений, поступающих на узлы замены S0-S7, образующих таблицу замен. Узлы замены имеет 4-битовый вход и выход, содержат числа от 0 до F в разном порядке;
- выходное 32-битное слово циклически сдвигается на 11 битов влево;

Алгоритм ГОСТ 28147-89. Схема образующей функции



Алгоритм ГОСТ 28147-89. Схема i-го раунда



Базовые циклы криптопреобразования по ГОСТ 28147-89

Базовые циклы криптопреобразования

Цикл зашифрования 32-З:

$K_0, \ldots, K_7, K_0, \ldots, K_7, K_0, \ldots, K_7, K_7, \ldots, K_0;$

Цикл выработки имитовставки 16-З:

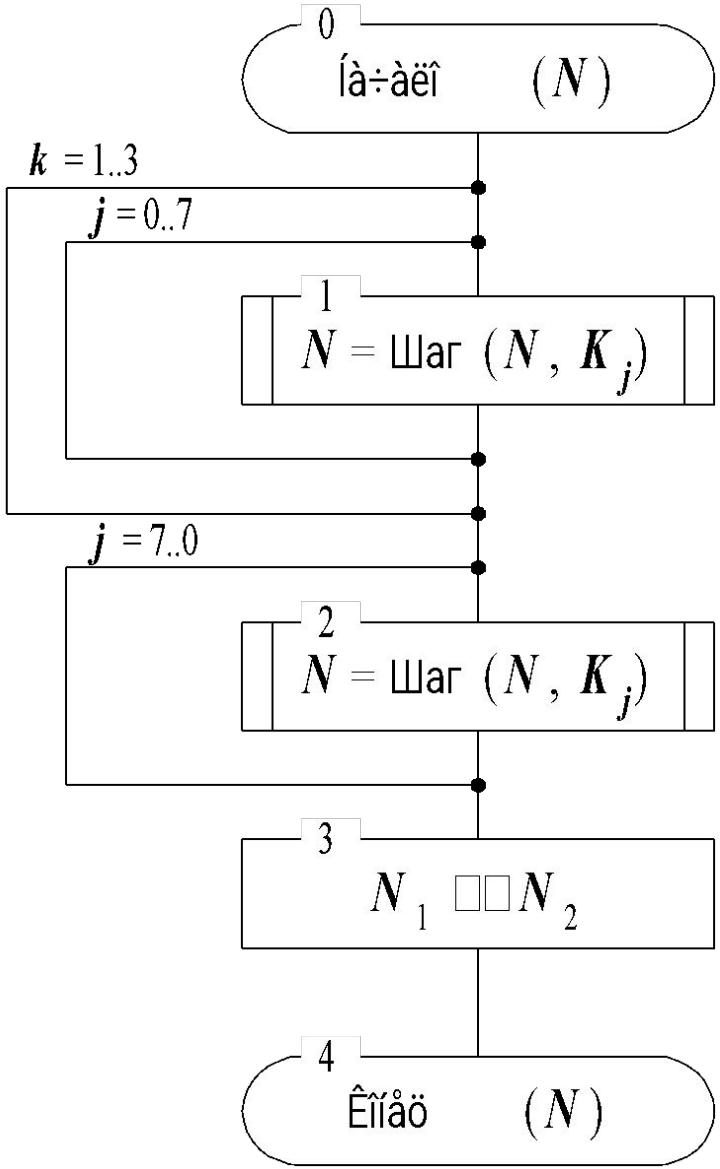
$K_0, \ldots, K_7, K_0, \ldots, K_7.$

Цикл расшифрования 32-Р:

$K_0, \ldots, K_7, K_7, \ldots, K_0, K_7, \ldots, K_0, K_7, \ldots, K_0;$

- это многократное повторение основного шага криптопреобразования.

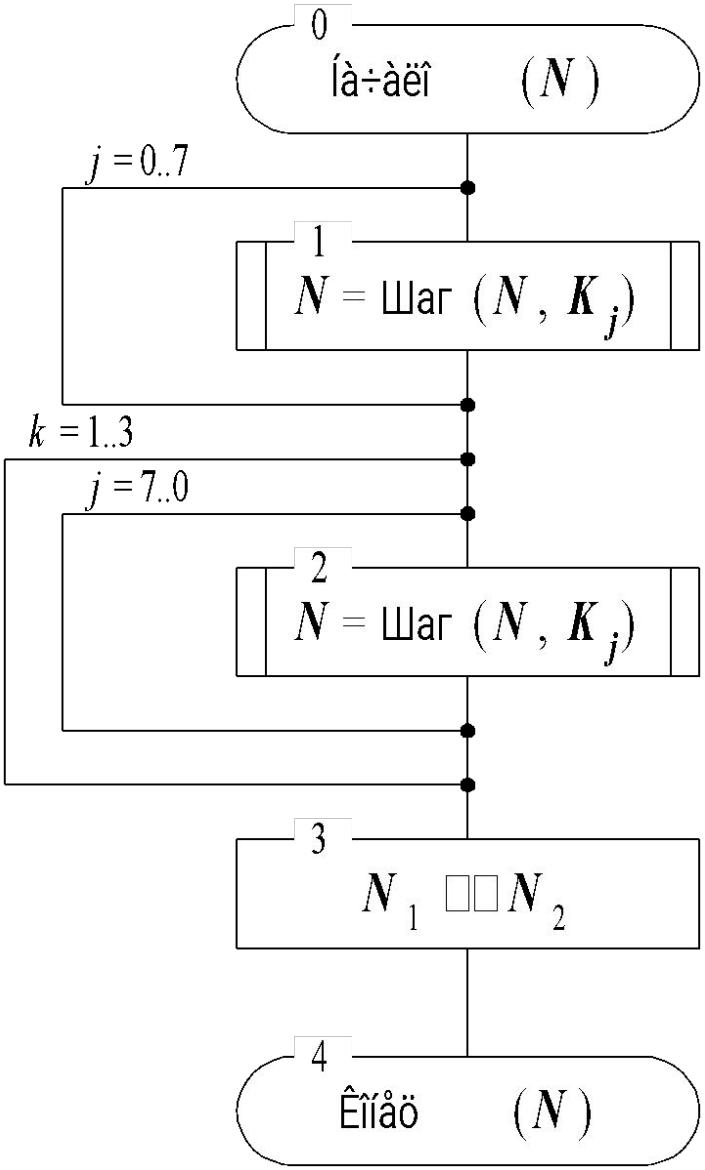
Схема цикла зашифрования 32-3



N- 64 - битный блок данных;

N = Шаг (N,K$_j$) – выполнение основного шага криптопреобразования для блока ***N*** с использованием ключевого элемента ***K$_j$***.

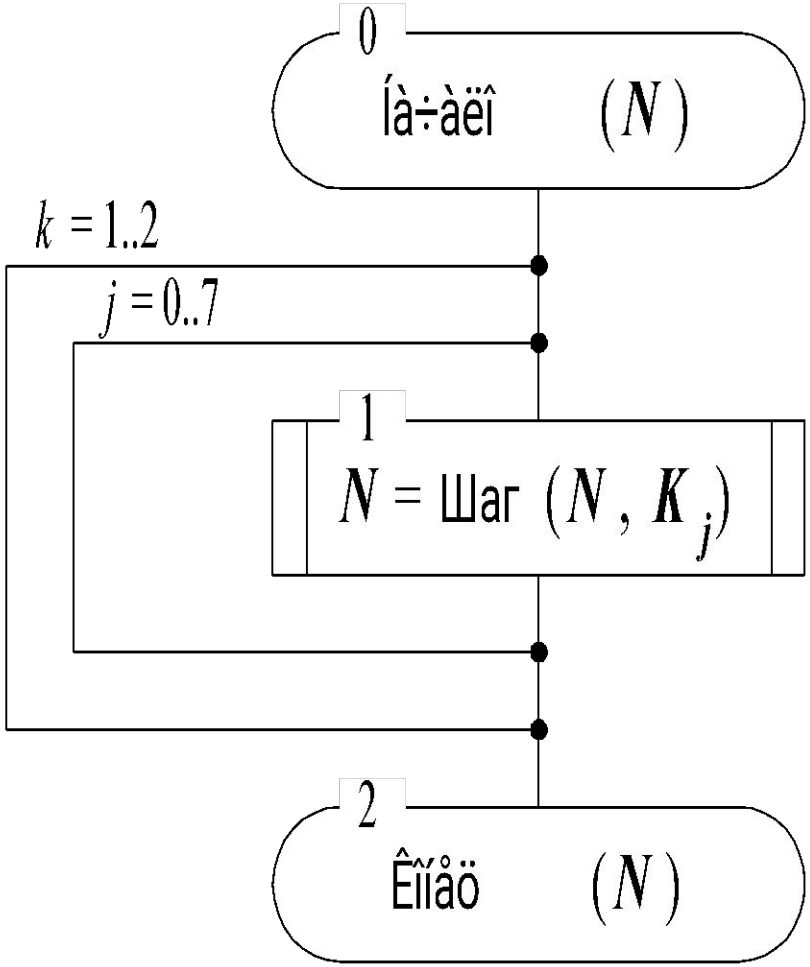
Схема цикла расшифрования 32-Р



***N*- 64 -** битный блок данных;

N = Шаг (N,K$_j$) – выполнение основного шага криптопреобразования для блока ***N*** с использованием ключевого элемента ***K$_j$***.

Схема цикла выработки имитовставки 16-3

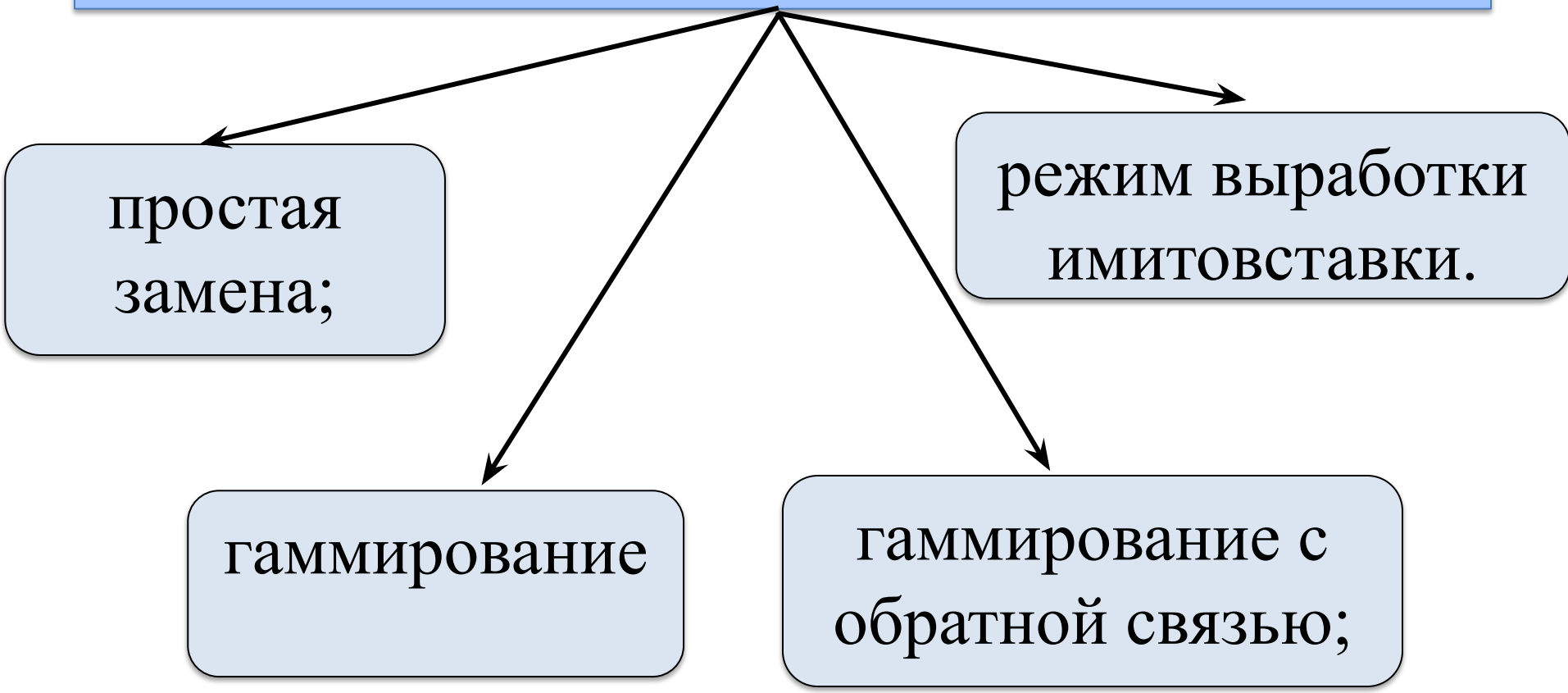


***N*- 64** - битный блок данных;

N = Шаг (N,K$_j$) – выполнение основного шага криптопреобразования для блока *N* с использованием ключевого элемента K_j.

Основные режимы шифрования

Режимы блочного шифрования



Алгоритмы шифрования и дешифрования

Методы блочного шифрования	Алгоритм шифрования	Алгоритм дешифрирования
Простая замена (Электронная кодовая книга (ECB))	$C[n] = E(P[n])$	$P[n] = D(C[n])$
Гаммирование (Обратная связь по выходу (OFB))	$I[0] = IV$ $I[n] = C[n-1]$ $R[n] = E(I[n])$ $C[n] = P[n] \oplus R[n]$	$I[0] = IV$ $I[n] = C[n-1]$ $R[n] = E(I[n])$ $C[n] = P[n] \oplus R[n]$
Гаммирование с обратной связью (Обратная связь по шифротексту (CFB))	$I[0] = IV$ $I[n] = C[n-1]$ $R[n] = E(I[n])$, $C[n] = P[n] \oplus R[n]$	$I[0] = IV$ $I[n] = C[n-1]$ $R[n] = E(I[n])$, $P[n] = C[n] \oplus R[n]$
Имитовставка (Сцепление блоков шифра (CBC))	$C[0] = E(P[0] \oplus IV)$ $C[n] = E(P[n] \oplus C[n-1])$	$P[0] = D(C[0]) \oplus IV$ $P[n] = D(C[n]) \oplus C[n-1]$

Режим простой замены

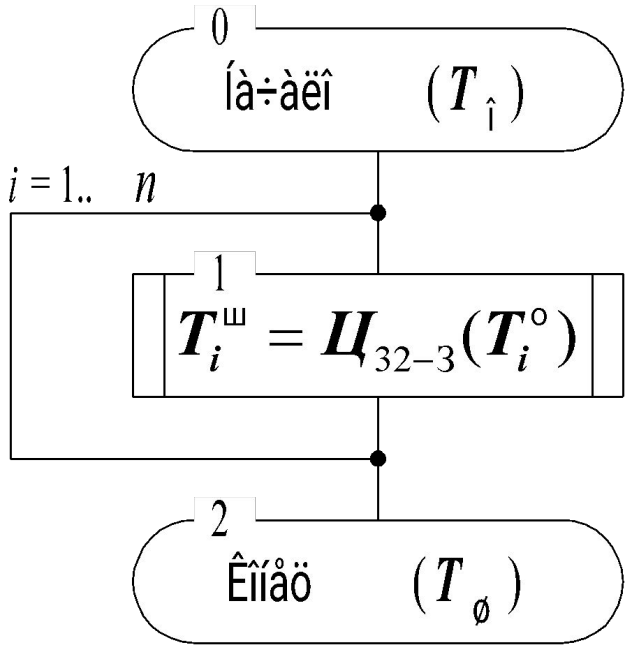
зашифрование - применение цикла **32-З** к блокам открытых данных, **расшифрование** – цикла **32-Р** к блокам зашифрованных данных;

64-битовые блоки обрабатываются независимо друг от друга;

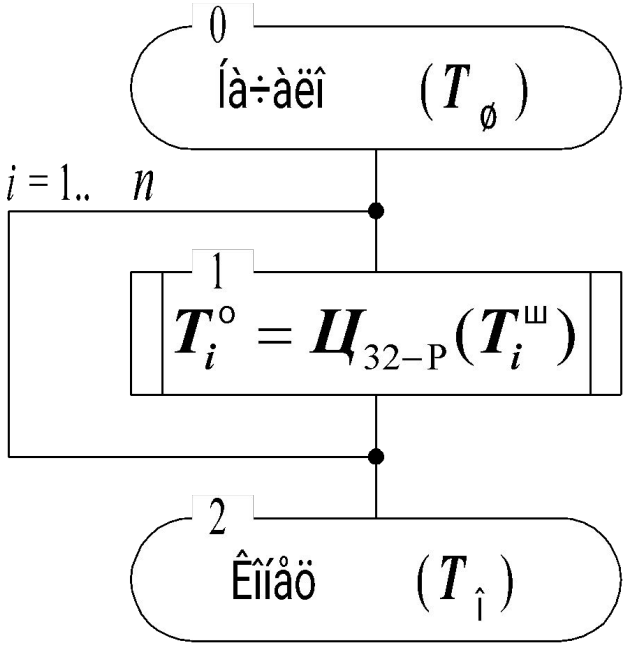
размер обрабатываемых данных должен быть кратен **64 битам**: $|T_{\text{о}}|=|T_{\text{ш}}|=64\cdot n$

Режим простой замены

Шифрование



Расшифрование



Режим простой замены

Особенности режима шифрования простой заменой

- при зашифровании одинаковых блоков получаются одинаковые блоки шифротекста, что позволит криптоаналитику сделать заключение о тождественности блоков исходных данных;
- если длина шифруемого массива данных не кратна 8 байтам или 64 битам, возникает проблема, чем и как дополнять последний неполный блок данных массива до полных 64 бит.
- режим простой замены используется для шифрования ключевой информации. Прочие режимы для этой цели менее удобны, поскольку дополнительно требуют синхропосылки.

Гаммирование

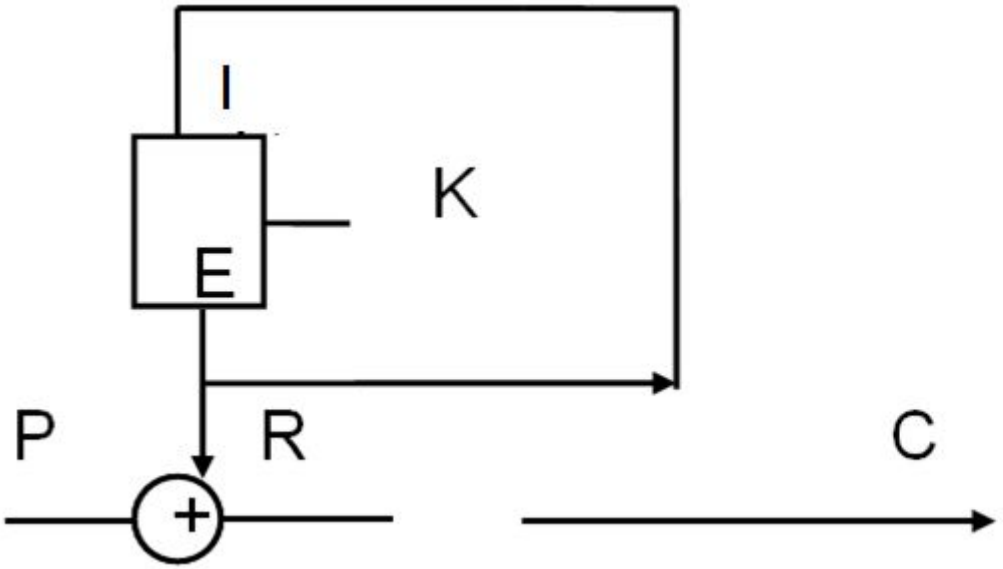
Гаммирование – это наложение на открытые (защифрованные) данные операцией сложения по mod 2 криптографической гаммы

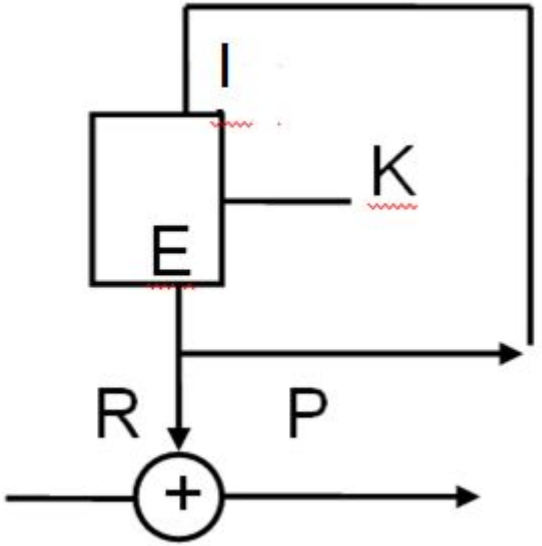
Гамма – псевдослучайная последовательность чисел с рекурсивного генератора последовательности чисел (РГПЧ), дополнительно шифруемая в режиме простой замены (32-З)

Элементы гаммы полностью определяются номером элемента и значением синхропосылки

Режим гаммирования

P - исходный,
C -зашифрованный текст,
E - операция шифрования
K -ключ
IV –синхропосылка





Методы блочного шифрования	Алгоритм шифрования	Алгоритм дешифрования
Гаммирование (обратная связь по выходу (OFB))	I[0]=IV I[n] = R[n-1] R[n] = E(I[n]) C[n]=P[n]+R[n]	I[0]=IV I[n] = R[n-1] R[n] = E(I[n]) C[n]=P[n]+R[n]

Требования к гамме

Период повторения близок к максимально возможному (2^{64})

Соседние значения отличаются в каждом байте

Простота аппаратной и программной реализации

Свойства гаммы

Независимая обработка младшей и старшей части блока

$$\Omega^0_{i+1} = (\Omega^0_i + C_1) \; mod \; 2^{32} \qquad C_1 = 1010101_{16}$$

$$\Omega^1_{i+1} = (\Omega^1_i + C_2 - 1) \; mod \; (2^{32} - 1) + 1$$

где $C_2 = 1010104_{16}$

Период повторения гаммы $2^{32} * (2^{32} - 1)$

Характеристики реккурентного генератора последовательности чисел

В 64-битовом блоке старшая и младшая части обрабатываются независимо друг от друга, существуют ***два независимых РГПЧ*** для старшей и младшей частей блока;

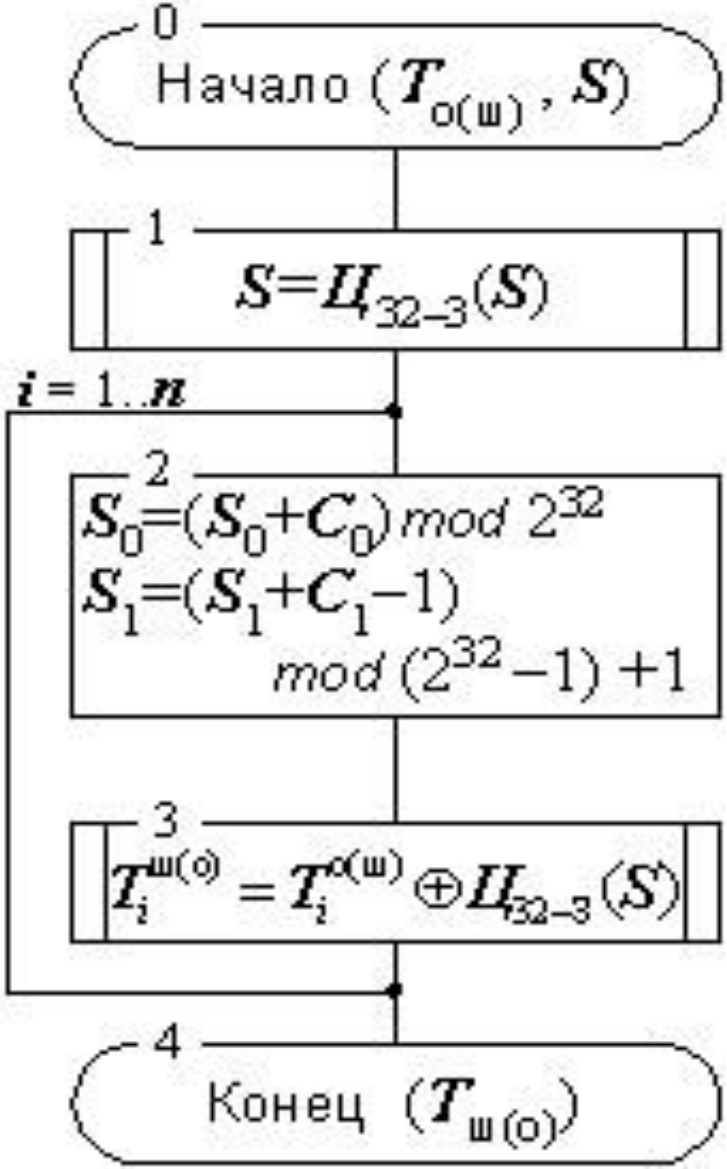
Рекуррентные соотношения для старшей (1) и младшей (2) частей следующие:

$$\Omega_{i+1}^{0} = (\Omega_i^0 + C_1) \bmod(2^{32}) \qquad (1)$$

$$\Omega_{i+1}^{1} = (\Omega_i^1 + C_2 - 1) \bmod(2^{32} - 1) + 1 \qquad (2)$$

Период повторения последовательности ***для младшей части*** составляет 2^{32}, ***для старшей части*** $2^{32}-1$, для ***всей последовательности*** период составляет $2^{32} \times (2^{32}-1)$.

Схема алгоритма шифрования в режиме гаммирования



$T_{о(ш)}$ – массив открытых (зашифрованных) данных произвольного размера, подвергаемый процедуре зашифрования (расшифрования), по ходу процедуры массив подвергается преобразованию порциями по 64 бита;

S – синхропосылка , 64-битовый элемент данных, необходимый для инициализации генератора гаммы;

Режим гаммирования

Особенности гаммирования как режима шифрования

- одинаковые блоки в открытом массиве данных дадут при зашифровании различные блоки шифротекста;
- поскольку наложение гаммы выполняется побитно, шифрование неполного блока данных легко выполнимо;
- синхропосылка, использованная при зашифровании, каким-то образом должна быть передана для использования при расшифровании.

Режим гаммирования

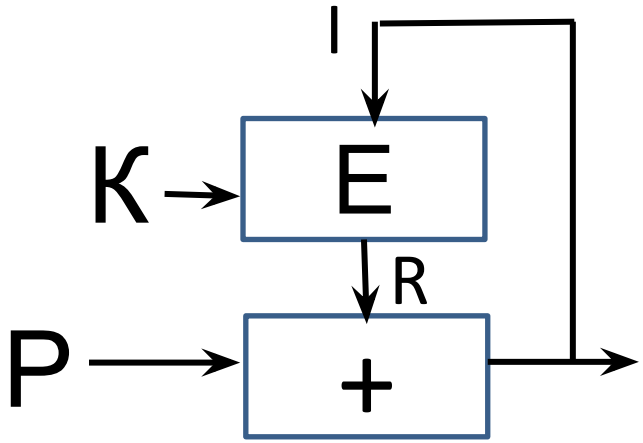
Гаммирование с обратной связью (гаммирование с зацеплением блоков)

очередной элемент гаммы вырабатывается как результат преобразования по циклу ***32-3*** предыдущего блока зашифрованных данных

для зашифрования первого блока массива данных элемент гаммы вырабатывается как результат преобразования по тому же циклу синхропосылки.

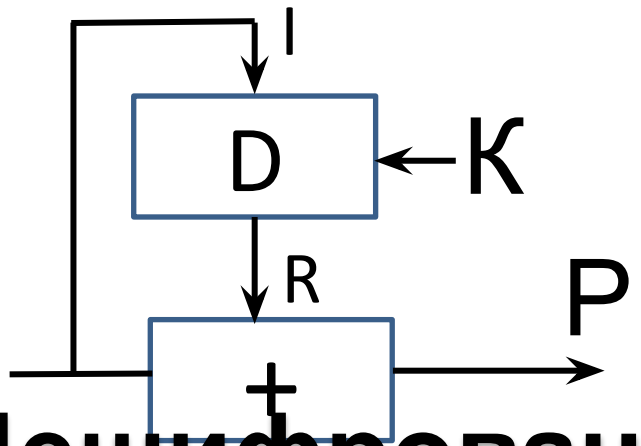
Гаммирование с обратной связью

Р - исходный,
С -зашифрованный текст,
Е - операция шифрования
К -ключ
IV –синхропосылка



Шифрование

С



Дешифрование

Методы блочного шифрования	Алгоритм шифрования	Алгоритм дешифрования
Гаммирование (обратная связь по выходу (OFB))	I[0]=IV I[n] = C[n-1] R[n] = E(I[n]) C[n]=P[n]+R[n]	I[0]=IV I[n] = C[n-1] R[n] = D(I[n]) C[n]=P[n]+R[n]

Алгоритмы шифрования и дешифрования

Методы блочного шифрования	Алгоритм шифрования	Алгоритм дешифрирования
Простая замена (Электронная кодовая книга (ECB))	C[n] = E(P[n])	P[n] = D(C[n])
Гаммирование (Обратная связь по выходу (OFB))	I[0] = IV I[n] = C[n-1] R[n] = E(I[n]) C[n] = P[n] ⊕ R[n]	I[0] = IV I[n] = C[n-1] R[n] = E(I[n]) C[n] = P[n] ⊕ R[n]
Гаммирование с обратной связью (Обратная связь по шифротексту (CFB))	I[0] = IV I[n] = C[n-1] R[n] = E(I[n]), C[n] = P[n] ⊕ R[n]	I[0] = IV I[n] = C[n-1] R[n] = E(I[n]), P[n] = C[n] ⊕ R[n]
Имитовставка (Сцепление	C[0] = E(P[0] ⊕ IV)	P[0] = D(C[0]) ⊕ IV

Гаммирование с обратной связью (гаммирование с зацеплением блоков)

Особенности гаммирования с обратной связью как режима шифрования

- при расшифровании блока данных блок открытых данных зависит от соответствующего и предыдущего блоков зашифрованных данных;
- При искажении зашифрованного блок, после расшифрования в соответствующем блоке открытых данных искаженными окажутся те же биты, что и в блоке шифрованных данных, а следующий блок исказится целиком.

Выработка имитовставки к массиву данных

Имитовставка (Message authentication code(MAC) – это контрольная комбинация, зависящая от открытых данных и секретной ключевой информации;

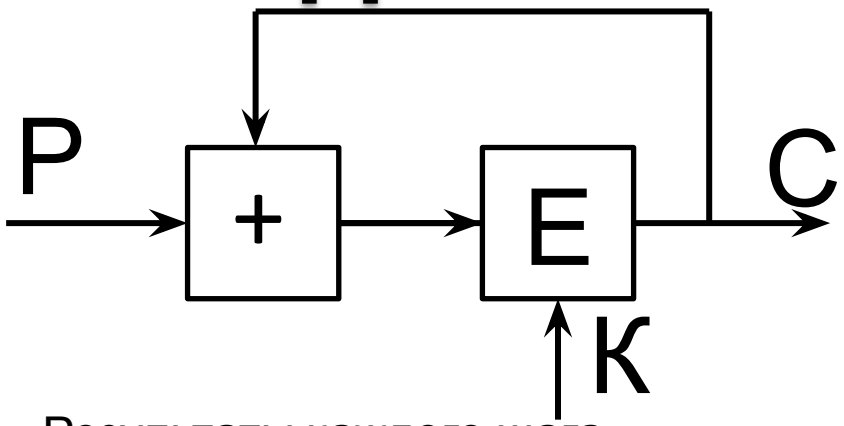
Обеспечивает обнаружение всех случайных или преднамеренных изменений в массиве информации;

В ГОСТ 28147-89 в качестве имитовставки берутся младшие 32 бита последнего блока, полученного на выходе

Выработка имитовставки

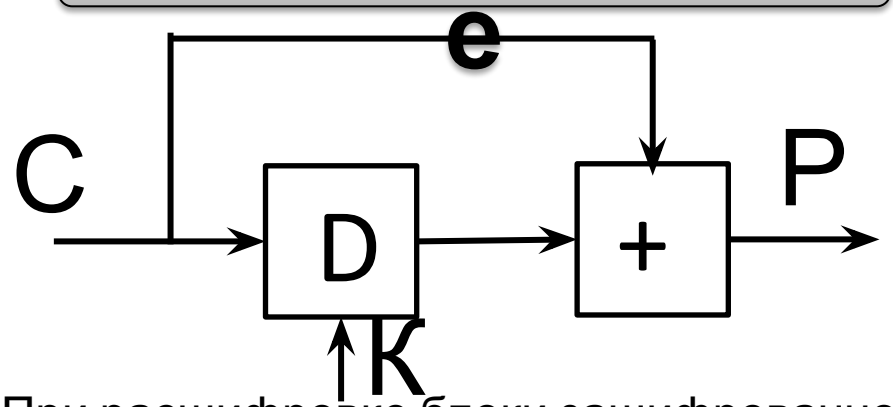
P - исходный,
C -зашифрованный текст,
E - операция шифрования
K -ключ
IV –синхропосылка

Шифрование



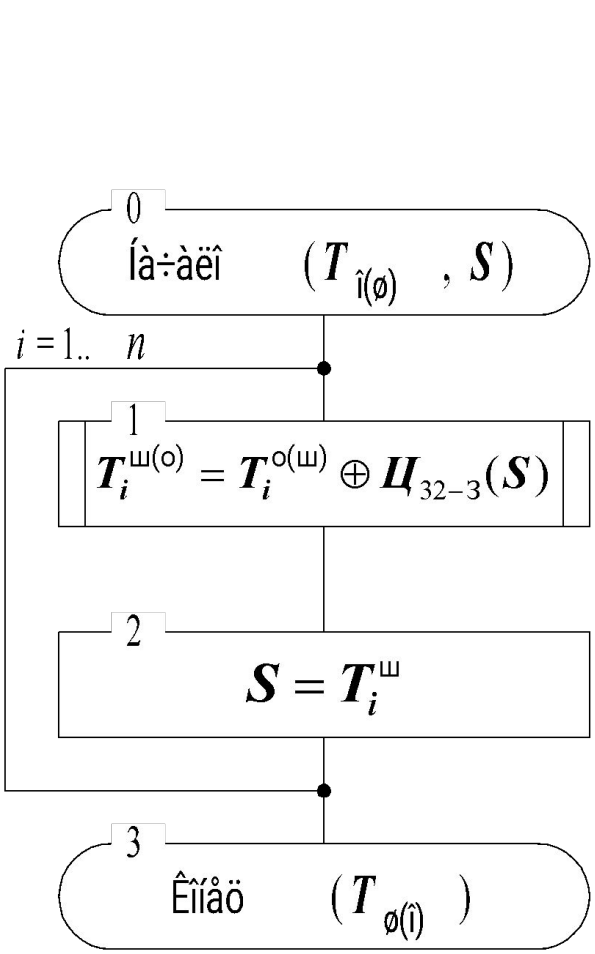
Результаты каждого шага шифрования запоминаются и складываются по модулю 2 со следующим блоком исходного те

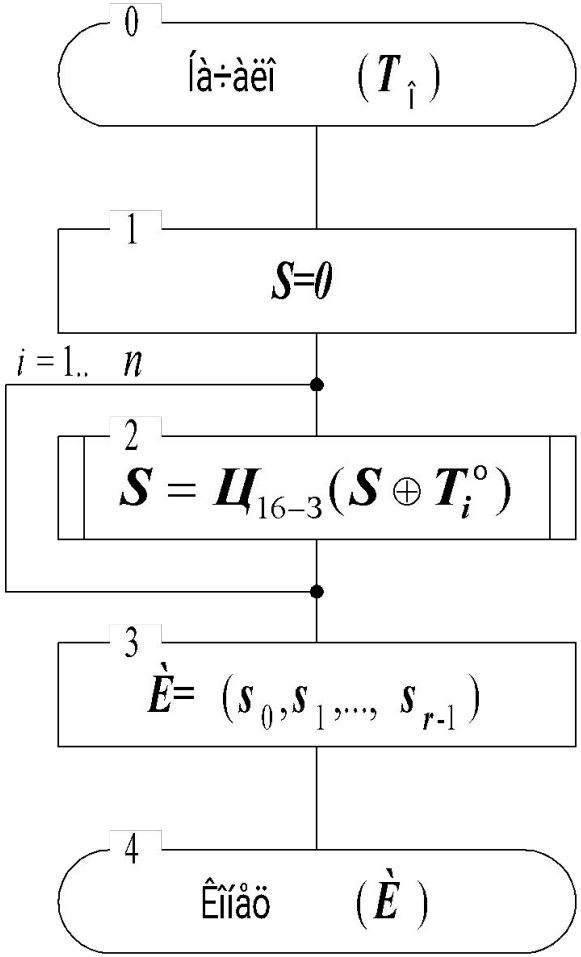
Дешифрование



При расшифровке блоки зашифрованного текста хранятся в течение 1 цикла и складываются по модулю 2 с дешифрованным текстом, полученным в цикле 32-P

Метод блочного шифрования	Алгоритм шифрования	Алгоритм дешифрования
Имитовставка (Сцепление блоков	C[0] = E(P[0] ^ IV) C[n] = E(P[n] ^ C[n-1])	P[0] =D(C[0]) ^ IV P[n] = D(C[n]) ^ C[n-1])


0
Íà÷àëî
$(T_{\text{í(ø)}}, S)$
$i = 1..n$
1
$T_i^{\text{ш(о)}} = T_i^{\text{о(ш)}} \oplus Ц_{32-3}(S)$
2
$S = T_i^{\text{ш}}$
3
Êîíåö
$(T_{\text{ø(í)}})$


0
Íà÷àëî
$(T_{\text{í}})$
1
$S=0$
$i = 1..n$
2
$S = Ц_{16-3}(S \oplus T_i^{\text{о}})$
3
$È = (s_0, s_1, ..., s_{r-1})$
4
Êîíåö
$(È)$

Выработка имитовставки к массиву данных