Американский стандарт блочного шифрования Rijndael

Второго октября 2000 года департамент торговли США подвел итоги конкурса по выработке нового стандарта шифрования США. Победителем стал алгоритм «Rijndael», разработанный бельгийскими криптографами.

Сравнительные характеристики алгоритмов ГОСТ28147-89 и Rijndael

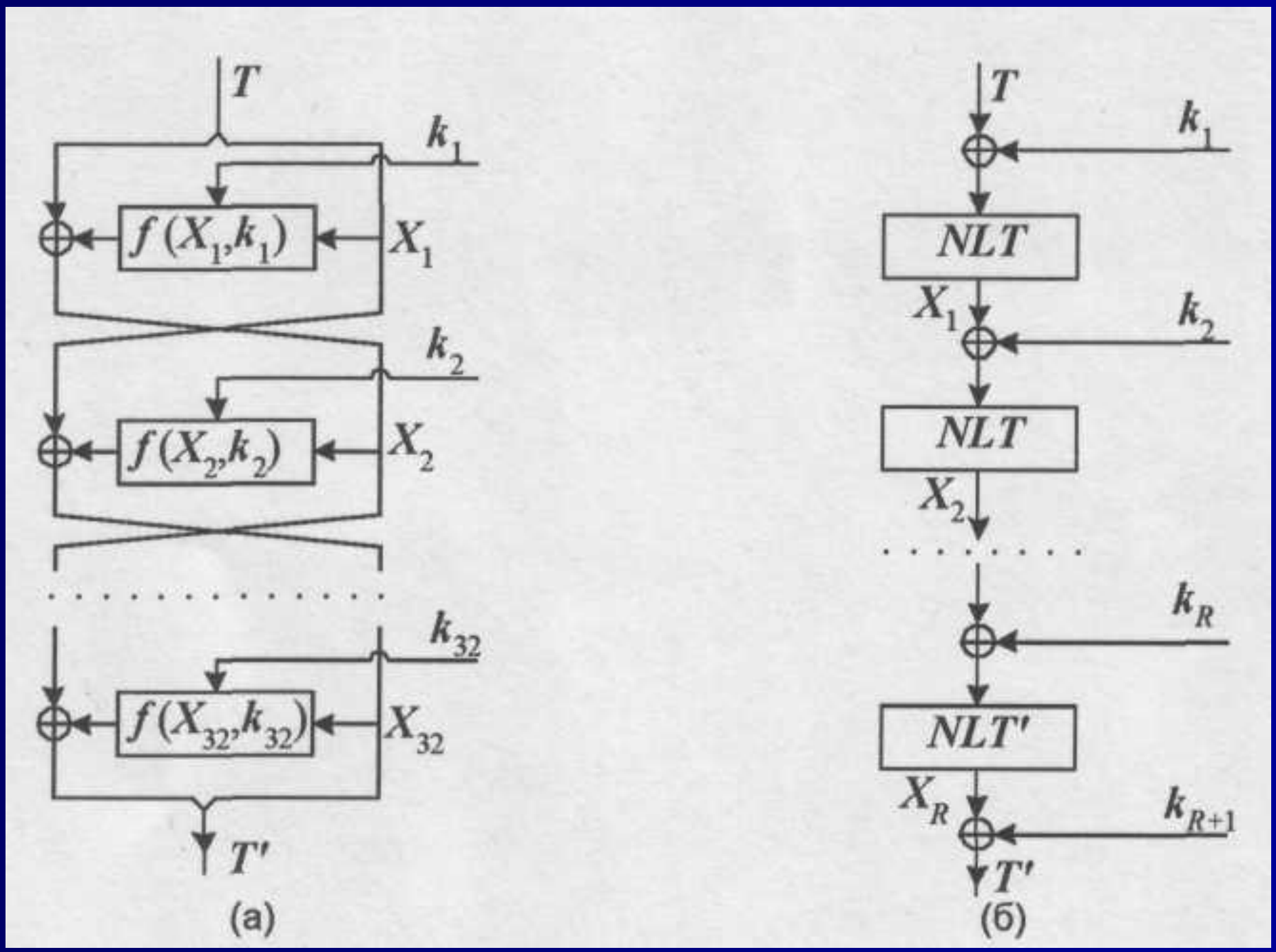
Показатель	ГОСТ28147-89	Rijndael
Размер блока, бит	64	128, 192, 256[1]
Размер ключа, бит	256	128, 192, 256
Архитектура	Однородная сбалансированная сеть Файстеля	«Квадрат» (Square)
Число раундов	32	10, 12, 14[2]

Показатель	ГОСТ28147-89	Rijndael
Часть блока, шифруемая за один раунд, бит	32(полблока)	128, 192, 256 (полный блок)
Размер раундового ключевого элемента, бит	32 (половина размера блока)	128,192, 256(равен размеру блока)
Структура раунда	Простая	Более сложная
Используемые на раунде операции	Только аддитивные операции,подстановки и сдвиги	Широкое использование операций над конечными полями
Эквивалентность прямого и обратного преобразований.	С точностью до порядка следования ключевых элементов	С точностью до вектора ключевых элементов, узла замен и прочих констант алгоритма

Сравнение общих архитектурных принципов

- Криптоалгоритм ГОСТ28147-89, как и большинство шифров «первого поколения», разрабатывавшихся в 70-е годы и в первой половине 80-х, базируется на архитектуре «сбалансированная сеть Фейстеля»
- Шифр Rijndael имеет архитектуру «квадрат» (Square). Эта архитектура базируется на прямых преобразованиях шифруемого блока, который представляется в форме матрицы байтов. Зашифрование также состоит из серии однотипных шагов, раундов, однако на каждом раунде блок преобразуется как единое целое и не остается неизменных частей блока.
  Таким образом, за раунд шифруется полный блок, следовательно, для обеспечения сопоставимой сложности и нелинейности преобразования таких шагов требуется вдвое меньше по сравнению с сетью Файстеля.

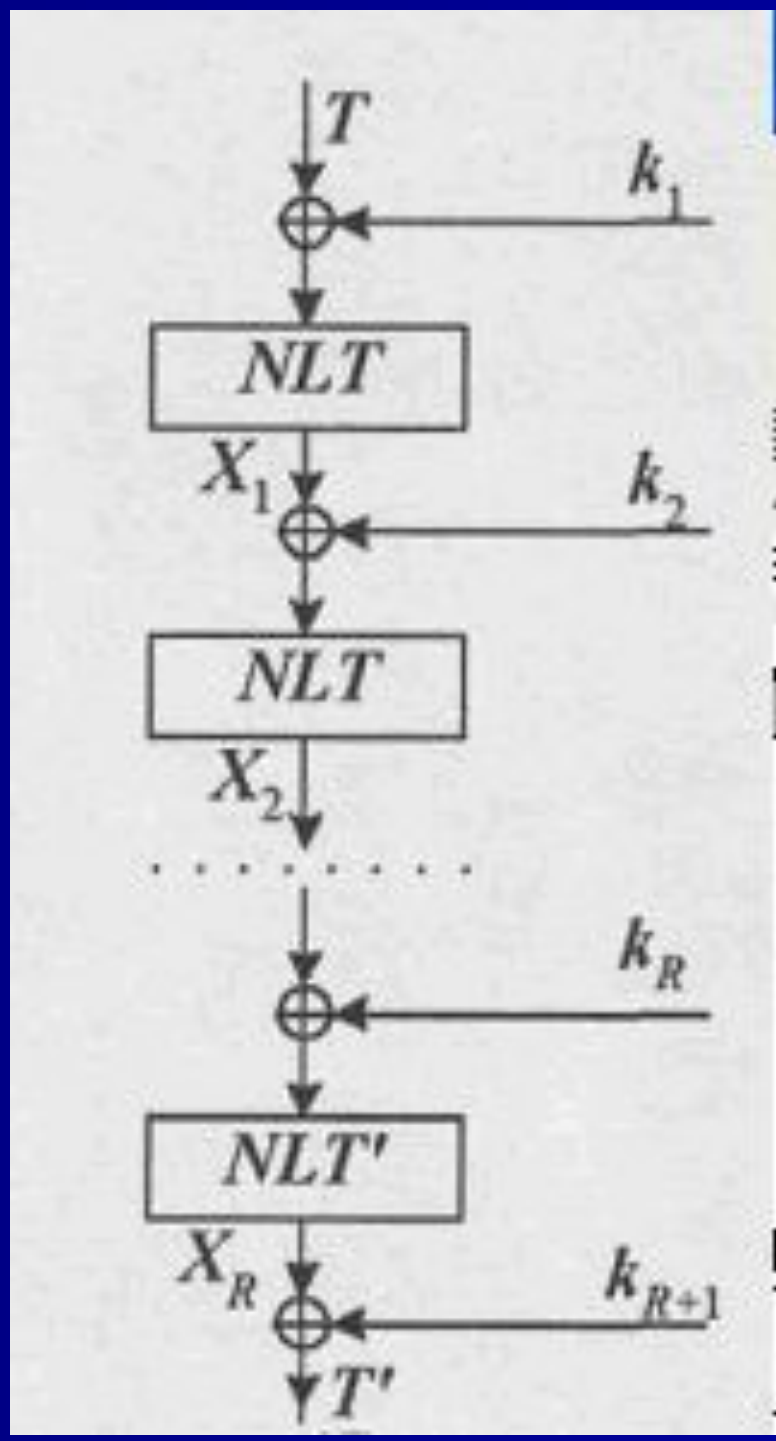
Сравнение общих архитектурных принципов



Общая схема алгоритма

Каждый раунд заключается в побитовом сложении по модулю 2 текущего состояния шифруемого блока и ключевого элемента раунда, за которым следует сложное нелинейное преобразование блока, сконструированное из трех более простых преобразований.

В Rijndael шифруемый блок и его промежуточные состояния в ходе преобразования представляются в виде матрицы байтов 4×n, где n =4, 6, 8 в зависимости от размера блока.



Функция нелинейного преобразования

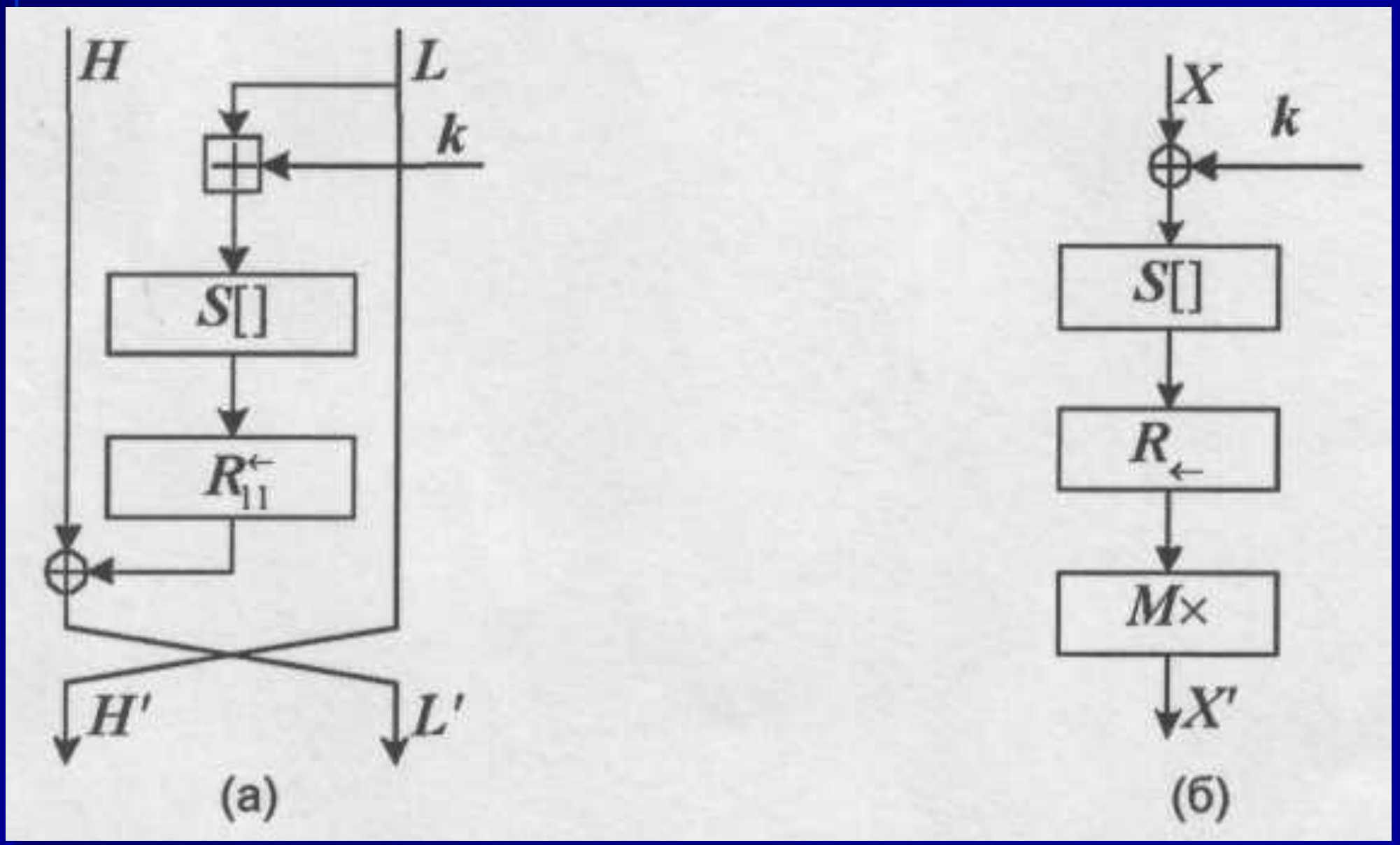
- ✔байтовая подстановка - каждый байт преобразуемого блока заменяется новым значением, извлекаемым из общего для всех байтов матрицы вектора замены;

- ✔побайтовый циклический сдвиг в строках матрицы: первая строка остается неизменной, вторая строка циклически сдвигается влево на один байт, третья и четвертая строка циклически сдвигаются влево соответственно на 2 и 3 байта;

- ✔матричное умножение - полученная на предыдущем шаге матрица умножается слева на матрицу-циркулянт размера 4x4:

$$M = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Сравнение раундов шифрования



Эквивалентность прямого и обратного преобразований

Шифр Rijndael построен на базе прямых преобразований. Как и для всех подобных алгоритмов, обратное преобразование строится из обращений шагов прямого преобразования, применяемых в обратном порядке.

Прямое преобразование	**Обратное преобразование**
$X = X \oplus k_{R-1}$	$X = X \oplus k_{R+1}$
$X = S(X)$	$X = R_{\rightarrow}(X)$
$X = R_{\leftarrow}(X)$	$X = S^{-1}(X)$
$X = M \times X$	$X = X \oplus k_R$
$X = X \oplus k_R$	$X = M^{-1} \times X$
$X = S(X)$	$X = R_{\rightarrow}(X)$
$X = R_{\leftarrow}(X)$	$X = S^{-1}(X)$
$X = X \oplus k_{R+1}$	$X = X \oplus k_{R-1}$

Произведем следующие преобразования:

Операция побайтовой замены (S) коммутативна с процедурой побайтового сдвига строк матрицы:

$$S^{-1}(R_{\rightarrow}(X)) = R_{\rightarrow}(S^{-1}(X)).$$

Кроме того, согласно правилам матричной алгебры по закону ассоциативности можно также поменять порядок побитового прибавления ключа по модулю два и умножения на матрицу:

$$M^{-1} \times (X \oplus k_R) = (M^{-1} \times X) \oplus (M^{-1} \times k_R).$$

После преобразований

Прямое преобразование	Обратное преобразование
$X = X \oplus k_{R-1}$	$X = X \oplus k_{R+1}$
$X = S(X)$	$X = S^{-1}(X)$
$X = R_{\leftarrow}(X)$	$X = R_{\rightarrow}(X)$
$X = M \times X$	$X = M^{-1} \times X$
$X = X \oplus k_R$	$X = X \oplus (M^{-1} \times k_R)$
$X = S(X)$	$X = S^{-1}(X)$
$X = R_{\leftarrow}(X)$	$X = R_{\rightarrow}(X)$
$X = X \oplus k_{R+1}$	$X = X \oplus k_{R-1}$

Алгоритмическая структура прямого и обратного преобразований идентична

Процедуры зашифрования и расшифрования различаются:

- в обратном преобразовании используется вектор замен, обратный в операционном смысле вектору замен прямого преобразования;

- в обратном преобразовании число байтов, на которые сдвигается каждая строка матрицы данных в операции построчного байтового сдвига другое;

- в обратном преобразовании в шаге матричного умножения блок данных умножается слева на матрицу, обратную той, что используется при прямом преобразовании;

- в обратном преобразовании ключевые элементы используются в обратном порядке, и, кроме того, все элементы за исключением первого и последнего, должны быть умножены слева на матрицу M^{-1}.

Выработка ключевых элементов

Существуют два алгоритма генерации последовательности ключевых элементов - для ключа размером 128/192 бита и для ключа размером 256 бит.

Ключ и ключевая последовательность представляются в виде векторов 4-х байтовых слов, и начальный участок последовательности заполняется словами из ключа, точно так же, как в ГОСТе.

Последующие слова ключевой последовательности вырабатываются по рекуррентному соотношению группами, кратными размеру ключа.

Первое 4-байтовое слово вырабатывается с использованием сложного нелинейного преобразования, остальные - по простому линейному соотношению:

$$w_i = \begin{cases} w_{i-N_K} \oplus G(w_{i-1}), & \text{при } i \bmod N_K = 0 \\ w_{i-N_K} \oplus w_{i-1}, & \text{при } i \bmod N_K \neq 0 \end{cases}$$

где N_k - число 32-битовых слов в ключе (4 или 6)
G(w) - нелинейное преобразование 32-битовых слов - включает байтовый сдвиг, побайтовую подстановку по вектору замен и побитовое сложение по модулю 2 с вектором, зависящим от номера вырабатываемой группы элементов:

$$G(x) = S(R_8^{\leftarrow}(x)) \oplus P(i/N_k),$$

P(i/Nk) - 4-байтовое слово, конструируемое особым образом и не зависящее от ключа.

Полученные из описанного выше потока 4-байтовые слова группируются в ключевые элементы необходимого размера, равного размеру шифруемого блока, и используются на раундах шифрования.

Выбор узлов замен и констант

При конструировании узлов замен помимо тривиальных требований обратимости и простоты описания были приняты во внимание следующие соображения:

- минимизация самой большой по величине характеристики корреляции между линейными комбинациями входных и выходных битов (определяет устойчивость к линейному криптоанализу);

- минимизация наибольшего нетривиального значения в таблице EXOR (определяет устойчивость к дифференциальному криптоанализу);
сложность алгебраического выражения, описывающего узел, в $GF(2^8)$.

Операция байтовой замены

Операция байтовой замены в алгоритме Rijndael описывается следующим уравнением:

$$S(X) = (x^7 + x^6 + x^2 + x) + X^{-1} \cdot (x^7 + x^6 + x^5 + x^4 + 1) \bmod (x^8 + 1).$$

Это преобразование начинается с мультипликативной инверсии заменяемого байта в описанном выше конечном поле GF(28), - значение 00 при этом меняется на самого себя, затем результат подвергается аффинному преобразованию.

Полиномы этого преобразования выбраны таким образом, чтобы у итогового отображения отсутствовали точки неподвижности *(S(X)=X)* и «антинеподвижности» *(S(X) = ~X)*. Здесь знаком «~» обозначена операция побитового инвертирования.

Выводы:

При конструировании шифра Rijndael широко использован алгебраический подход.
Это касается главным образом двух основных преобразований шифра - байтовой замены и операции перемешивания столбцов матрицы данных посредством ее умножения слева на матрицу *M*.

По оценкам разработчиков шифра Rijndael, уже на четырех раундах шифрования этот алгоритм приобретает достаточную устойчивость к различным видам криптоанализа.

Теоретической границей, за которой линейный и дифференциальный виды криптоанализа теряют смысл, является рубеж в 6-8 раундов в зависимости от размера блока.

Согласно спецификации, в шифре предусмотрено 10-14 раундов.

Следовательно, шифр Rijndael устойчив к указанным видам криптоанализа с определенным запасом.